Faculty of Informatics, University of Debrecen

Book of Abstracts

21th Central European Conference on Cryptology

CECC 2021

June 23 - 25, 2021, Debrecen, Hungary

Organized by

Faculty of Informatics, University of Debrecen

Supported by

EFOP 3.6.3, a project co-financed by the Hungarian Government and European Union through the European Regional Development Fund.

Program Committee

Andrea Huszti - University of Debrecen (chair)
Nicolas Courtois - University College London
László Csirmaz - Central European University
Andrej Dujella - University of Zagreb
Peter Gaži - IOHK Research
Otokar Grosek - Slovak University of Technology in Bratislava
Jan Hajny - Brno University of Technology
Clemens Heuberger - Alpen-Adria-Universität Klagenfurt
Miroslaw Kutylowski - Wroclaw University of Science and Technology
Vashek Matyáš - Masaryk University
Florian Mendel - Infineon Technologies
Ferenc Molnár – CCLab Ltd.
Karol Nemoga - Slovak Academy of Sciences
Attila Pethő - University of Debrecen
Stefan Porubsky - Czech Academy of Sciences
Havard Raddum - Simula UiB, Norway
Vincent Rijmen - KU Leuven and University of Bergen
Martin Stanek - Comenius University
Rainer Steinwandt - The University of Alabama in Huntsville
Pavol Zajac - Slovak University of Technology in Bratislava
Damian Vizár - CSEM, Switzerland

Organizing Committee

Andrea Huszti (chair)
Tamás Herendi
Zoltán Szabolcs Kovács
Norbert Oláh
Viktória Padányi
Ádám Vécsi

Table of Contents

Abstracts of invited talks

Challenges in Lightweight Cryptography

Maria Eichlseder

Graz University of Technology
maria.eichlseder@iaik.tugraz.at

While our desktop processors grow faster and faster, our data is increasingly often processed elsewhere: by networks of cheap, highly-constrained devices with low computational power and limited power supply. At the same time, these applications are often riddled with additional challenges, such as devices under the physical control of an adversary. Lightweight cryptography is designed to provide security under such difficult conditions. The ongoing NIST Lightweight Crypto (LWC) standardization competition, currently in its final round, is shining a spotlight on this research direction. In this talk, we will discuss how the LWC finalists tackle different challenges in lightweight cryptography. We will also look at directions beyond the scope of LWC: For example, securing the internals of computer systems against microarchitectural attacks requires primitives with very low latency and unusual interfaces.

Breaking and fixing cryptographic systems

Riccardo Focardi

Department of Environmental Sciences, Informatics and Statistics
Ca' Foscari University, Venice

In recent years, we have faced an increasingly pervasive use of cryptography. The expansion of IoT, home automation and industry 4.0 has worryingly increased the attack surface, making it necessary to use cryptographic protocols to protect communications and data. However, cryptography is complex: not all cryptographic mechanisms offer the same level of protection; management and configuration is often the Achilles' heel of cryptographic systems; finally, protocols and implementations may present bugs that weaken or, in some cases, cancel the security guarantees offered by the adopted mechanisms. In this talk we will give an overview of the problems and attacks encountered in real cryptographic systems, discussing their weaknesses and possible remedies. We will present some case studies we have dealt with highlighting how, and in which extent, scientific research can improve the state of the art of real cryptographic systems.

Breaking Historical Ciphers with Modern Means

Klaus Schmeh

Cipherbrain Blog
www.schmeh.org

This presentation introduces a number of ciphers that played an important role in history and explain how they can be broken with modern means. Among other techniques, Hill Climbing has proven especially powerful for this purpose. The current state of research will be demonstrated with original ciphertexts from past centuries, some of which were deciphered only recently. In spite of a number of interesting improvements that have been developed in recent years, there are still surprisingly many historical ciphertexts that are unbroken to date. For instance, nomenclators, short Enigma messages, double column transpositions with long key words, and numerous Cold War ciphers still baffle cryptanalysts. However, research goes on and we might see further improvements in the near future.

Extended abstracts of contributed talks

Cryptanalysis of the quantum public-key cryptosystem OTU under heuristics from Szemerédi-type statements

Shoichi Kamada*

Tokyo Metropolitan University
email: shoichi@tmu.ac.jp

Extended Abstract

The knapsack cryptography is the public-key cryptography whose security depends mainly on the hardness of the following subset sum problem. Here let $\mathbb{N} := \{1, 2, \ldots\}$.

Definition (Subset Sum Problem)**.** For $(a_1, \ldots, a_s) \subseteq \mathbb{N}^s$ and $C \in \mathbb{Z}$, find $(x_1, \ldots, x_s) \in \{0, 1\}^s$ satisfying

$$x_1 a_1 + \ldots + x_s a_s = C.$$

Many of knapsack schemes were broken by low-density attacks [4, 1, 5, 2, 3], which are attack methods to use the situation that a shortest vector or a closest vector in a lattice corresponds to a solution of the subset sum problem. For the case when the Hamming weight of a solution for a random instance of the subset sum problem is arbitrary, if the density is less than 0.9408, then the instance can be solved almost surely by a single call of lattice oracle. The critical value 0.9408 was first appeared in [1].

In Crypto 2000, Okamoto, Tanaka and Uchiyama [6] introduced the concept of quantum public key cryptosystems and proposed a knapsack cryptosystem, so-called OTU cryptosystem. However, no known algorithm breaks the OTU scheme.

For a positive integer k, let $r(k, N)$ denote the cardinality s of a largest set $A = \{a_1, \ldots, a_s\} \subseteq [N] := \{1, \ldots, N\}$ such that the orthogonal lattice

*Supported by JSPS KAKENHI Grant Number 19J00126.

$L(A) := \{(y_1, \ldots, y_s) \in \mathbb{Z}^s : y_1a_1 + \cdots + y_sa_s = 0\}$ does not contain a non-zero lattice vector with Euclidean norm less than $\sqrt{k}$. In this paper, we introduce the following Szemerédi-type assumption.

Assumption (Szemerédi-type assumption)**.** *For $k \geq 5$,*

$$r(k, N) = o(N).$$

Notice that the above assumption is the imitation of the statement of Szemerédi's theorem on arithmetic progressions [7].

For the subset sum problem, we make clear what the average case and the worst case are.

For low density attacks, we give better heuristics for orthogonal lattices than Gaussian heuristics. Consequently, we make clear some extremal problem in a number field related to OTU scheme and we show that the OTU scheme can be broken under some heuristic assumptions.

References

[1] M.J. Coster, A. Joux, B.A. Lamacchia, A.M. Odlyzko, C.P. Schnorr, and J. Stern. "Improved low-density subset sum algorithms". In: *computational complexity* 2 (1992), pp. 111–128.

[2] T. Izu, J. Kogure, T. Koshiba, and T. Shimoyama. "Low-density attack revisited". In: *Designs, Codes and Cryptography* 43.1 (2007), pp. 47–59.

[3] N. Kunihiro. "New Conditions for Secure Knapsack Schemes against Lattice Attack". In: *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences* E93-A.6 (2010), pp. 1058–1065.

[4] J.C. Lagarias and A.M. Odlyzko. "Solving low-density subset sum problems". In: *Journal of the ACM* 32 (1985), pp. 229–246.

[5] P.Q. Nguyen and J. Stern. "Adapting Density Attacks to Low-Weight Knapsacks". In: *Advances in Cryptology – ASIACRYPT 2005*. Springer Berlin Heidelberg, 2005, pp. 41–58.

[6] T. Okamoto, K. Tanaka, and S. Uchiyama. "Quantum Public-Key Cryptosystems". In: *Advances in Cryptology - CRYPTO 2000*. Springer Berlin Heidelberg, 2000, pp. 147–165.

[7] E. Szemerédi. "On sets of integers containing no k elements in arithmetic progression". In: *Acta Arithmetica* 27 (1975), pp. 199–245.

Cryptanalysis of a Special Polybius-Like Cipher

Eugen Antal*

Institute of Computer Science and Mathematics, Slovak University of Technology in Bratislava
eugen.antal@stuba.sk

Polybius (c. 200 - c. 118 BC) was a Greek historian and writer who devised a special signaling system that was later adopted as a cryptographic method [3, 5]. His system is called *Polybius square* (also called as Polybius checkerboard [3]) and consists of a 5×5 square (table) filled with the letters of the alphabet. In the case of the English alphabet, the letters i and j are merged to fit the square. In the original version from Polybius, the rows and columns were labeled with numbers $1, 2, 3, 4, 5$. These numbers serve as a row and column coordinate in the table. The encryption process transforms the letters in the square to their coordinates. Encryption systems with similar characteristics were widely used during the history [3]. Polybius-like cipher from the seventeenth and eighteenth century can be found in the Hessian State Archives in Marburg, Germany. In the twentieth century, some countries like Slovak State and former Czechoslovakia [6–8] also used similar ciphers. Various types of this cipher are described in the first (serious) Czechoslovak crypto manual from J. Růžek [4]. In general, the Polybius checkerboard type cipher can vary in different aspects such as the table labels (numbers, letters, ...), table dimension (any rectangular shape not only a square), and table content (it can contain not only letters but also numbers, common bigrams, and words). It can also contain an element multiple times (homophonic substitution). In this work, we focus on a special Polybius-like checkerboard cipher inspired by three real ciphers used in Czechoslovakia and in the Slovak State. Two were used during WW2 and one right after the war.

The first investigated Polybius-like checkerboard cipher is a 9×9 table. The table contains letters, numbers, and common bigrams/trigrams (from the Slovak language). Numbers $1, 2, \ldots, 9$ were used as row/column labels. It was used during army training in the Slovak State in 1940 [7]. This cipher was called *cipher key*. The row and column labels were permanent, but the order of the columns was changed daily based on an additional permutation. In 1944, a very similar cipher was used by the Czechoslovak resistance army fighting on the Eastern front called 1st Czechoslovak Army Corps in the Soviet Union [8]. The table size was 10×10 (labels $0, 1, \ldots, 9$). It contains letters, numbers, common bigrams/trigrams (from the Czech language), and special characters (e.g. dot, comma, ...). Some letters and bigrams are with a diacritical mark. This cipher was called *encryption table No. 58 C* and was used in radio communication. Both, the row and column labels were changed daily. The third Polybius-like checkerboard cipher was used in newly established Czechoslovakia in 1947 by army units fighting against the Ukrainian nationalist paramilitary and partisan formations. The table size, in this case, was 10×10 and it contains uppercase and lowercase letters, numbers, common bigrams, words, and special characters. This variant also contains elements with a diacritical mark. The row labels were permanent and the column labels were set based on the key.

We investigated the possibility of solving a special Polybius-like cipher (consisting of letters, bigrams/trigrams, and special symbols) with modern heuristic [1, 2] approach. The cryptanalysis (solving) task was defined as a keyspace search, where the daily key is the only unknown parameter. This task can be transformed into an optimization problem. We evaluate the effectiveness (success rate) of the Hill Climbing meta-heuristic methods with restarts. We also investigated several different fitness functions (L1 distance, Jensen-Shannon divergence, weighted sum) and language models (n-gram for $n = \{1, 2, 3, 4\}$). To evaluate how the problem complexity depends on the table dimension, we created several custom Polybius-like ciphers with different sizes (from 5×5 up to 10×10). In the experiments, we used English texts of different lengths and English statistics in fitness functions. The smallest table contains only letters (the classical Polybius variant). By increasing the table size we extended the table by adding numbers, bigrams, and special symbols. To simulate the three real cipher types, we tested a

*This work was supported by grants VEGA 2/0072/20.

variant where only the column labels were changed and a case where both column and row labels were parameters. In the first case (the solution space is small), we obtained a 100% average success rate in almost all cases. Worse results were only in the case of smaller text sizes and large table sizes. For the second case, we were able to reach a 100% success rate for all text lengths and fitness functions only in the case of table size 5 and 6, where the average success rate was around $50 - 60\%$. For table size > 6, the success rate varies based on the used language model and fitness function. For the larger table size, we were also able to solve all tested encrypted text files, but not for all fitness functions. Increasing the table size causes a worse success rate for lower language models. Fitness functions based on statistical distance performed the best and the weighted sum fitness function performed the worst.

References

[1] Antal, E. *Modern Cryptanalysis of Classical Ciphers* (in Slovak). PhD. thesis, STU in Bratislave, 2017.

[2] Antal, E.; Eliáš, M. *Evolutionary Computation in cryptanalysis of classical ciphers.* Tatra Mountains Mathematical Publications, Vol. 70, p. 179–197.

[3] Kahn, D. 1996. The Codebreakers. Scribner.

[4] Růžek, J. 1926-1949. Šifrovací systémy a návod k luštění kryptogramů.

[5] von zur Gathen, J. 2015. CryptoSchool. Springer.

[6] Vojenský Historický Archív Bratislava. f. Banderovci.

[7] Vojenský Historický Archív Bratislava. f. MNO dôverné.

[8] Vojenský Historický Archív Prahe. f. 1. čs. spoj. prapor v SSSR 1944-1945

On the Security of Iterated Block Ciphers with Dependent Round Keys Against Differential and Linear Cryptanalysis

Serhii Yakovliev

Institute of Physics and Technology, National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
yasv@rl.kiev.ua

Introduction

A formal theory of differential and linear cryptanalysis makes a standard assumption that round keys of iterated block cipher are uniform and independent. While the first property is not hard to achieve, the second is not valid for many known ciphers. For example, in AES round keys are generated with deterministic procedure from previous ones; in Kalyna cipher odd round keys are simple bit rotations of even round keys, and so on.

In this paper we research how the assumption of round key independence affects on the security against differential and linear cryptanalysis. We mostly focus on differential cryptanalysis due to limited article size, since presented results can be easily formulated for linear cryptanalysis.

Main results

Let $V_n = \{0,1\}^n$ be a linear space of all n-length binary vectors with bitwise addition $\oplus$. For any mapping $f\colon V_n \to V_n$ a *differential* is an arbitrary pair of vectors $(\alpha, \beta) \in V_n^2$. *A probability of differential* (α, β) (with respect to $\oplus$) is defined as

$$\mathrm{DP}^f(\alpha,\beta) = \frac{1}{2^n} \sum_{x \in V_n} [f(x \oplus \alpha) = f(x) \oplus \beta],$$

where $[\dots]$ denotes an Iverson's brackets: $[P]$ is equal to 1, if P is true, and 0, if not.

For the encryption mapping $F_k\colon V_n \times \mathcal{K} \to V_n$ consider *a probability of differential at point* x DP and *an average probability of differential* EDP:

$$\begin{aligned} \mathrm{DP}^{F_k}(x;\alpha,\beta) &= \frac{1}{|\mathcal{K}|} \sum_{k \in K_n} [F_k(x \oplus \alpha) = F_k(x) \oplus \beta], \\ \mathrm{EDP}^{F_k}(\alpha,\beta) &= \frac{1}{2^n} \sum_{x \in V_n} \frac{1}{|\mathcal{K}|} \sum_{k \in K_n} [F_k(x \oplus \alpha) = F_k(x) \oplus \beta]. \end{aligned}$$

The security against differential cryptanalysis is estimated with maximal values MDP and MEDP of differential probabilities above.

The encryption mapping F_k is *a Markov cipher*, if the probabilities of all its differentials do not depend on points: $\mathrm{DP}^{F_k}(x;\alpha,\beta) = \mathrm{EDP}^{F_k}(\alpha,\beta)$ for any x, α, β. For Markov ciphers there are well-known bounds for both provable and practical security against differential and linear cryptanalysis.

Consider two encryption mappings $F_k, F'_k\colon V_n \times \mathcal{K} \to V_n$ and a bijective mapping $\lambda\colon \mathcal{K} \to \mathcal{K}$. Define two-round cipher $G_k(x)$ as $G_k(x) = F'_{\lambda(k)}(F_k(x))$. Clearly, G_k is a cipher with dependent round keys, even if k selected uniformly from $\mathcal{K}$.

Our main results are stated in two next theorems.

Theorem 1. For the introduced two-round cipher G_k an inequality holds:

$$\forall \alpha, \beta \in V_n\colon \mathrm{EDP}^{G_k}(\alpha,\beta) \le \sum_{\gamma \in V_n} \sqrt{\mathrm{EDP}^{F_k}(\alpha,\gamma)\,\mathrm{EDP}^{F'_k}(\gamma,\beta)}.$$

Theorem 1 says that two-round iterative cipher with fully dependent round keys is not the Markov cipher, even if its round functions are Markov mappings. Thus, the known formal theory of the Markov cipher security against differential (and linear) cryptanalysis cannot be applicable to this case. Moreover, the form of inequality in Theorem 1 statement does not allow extending or generalizing known DP evaluation methods (with so-called differential characteristics) on this class of ciphers.

But for many popular constructions of round functions the statement of Theorem 1 can be strengthened.

Theorem 2. Let $\mathcal{K} \equiv V_n$ and $s\colon V_n \to V_n$ is a bijective mapping (S-box). If one of the next three cases is true:

1) round functions F_k, F'_k have a form $s(x \oplus k)$,

2) round functions F_k, F'_k have a form $s(x) \oplus k$,

3) round functions F_k, F'_k have a form $s(x \oplus k) \oplus \mu(k)$, where μ is some mapping and $k \to \lambda(k) \oplus \mu(k)$ is a bijective mapping,

then an equality holds:

$$\forall \alpha, \beta \in V_n\colon \mathrm{EDP}^{G_k}(\alpha, \beta) = \sum_{\gamma \in V_n} \mathrm{DP}^s(\alpha, \gamma)\,\mathrm{DP}^s(\gamma, \beta).$$

Note, that the similar statement can be obtained for linear approximations and linear potentials of two-round cipher with dependent round keys.

Almost all known block ciphers have round functions of form $s(x \oplus k)$ or $s(x) \oplus k$. It follows from Theorem 2 that the behavior of average differential probabilities looks like these ciphers are Markov, even if their round keys are dependent. One can consider this sufficient to evaluate the security against differential (and linear) cryptanalysis with maximum EDP value, but this is not correct, because in the case of non-Markov cipher the security must be evaluated with maximum DP value.

We conducted some calculations on model ciphers to show the difference. The experimental results presented below were obtained with Bohdan Piasetsky.

Let $n = 8$ and the round function is of the form $F_k(x) = s(x \oplus k)$. We consider as s S-boxes from ciphers AES, ARIA (the second S-box), Kalyna (S-boxes π_0, π_1, π_2, π_3) and Kuznyechik. With this round functions we construct two-round cipher $G_k(x) = F_{\lambda(k)}(F_k(x))$, where $\lambda(k)$ is the identical function or a cyclic shift by 1, 2 or 3 bits. Also, we consider two-round cipher $H_{k_1,k_2}(x) = F_{k_2}(F_{k_1}(x))$ with independent round keys.

For all described ciphers we found maximal EDP and DP value by direct calculation. Maximal EDP values of all G_k's and H_{k_1,k_2} turned out to be equal (as Theorem 2 had predicted). Maximal DP values are given in a Table 1.

Table 1: Values of $2^8 \cdot \mathrm{MDP}(F_k)$, $2^8 \cdot \mathrm{MDP}(G_k)$ and $2^8 \cdot \mathrm{MDP}(H_{k_1,k_2})$ depending on the selected S-box and $\lambda(k)$ function (here $m(f) = 2^8 \cdot \mathrm{MDP}(f)$)

S-box	$m(F_k)$	$m(H_{k_1,k_2})$	$m(G_k)$			
			$\lambda(k) = k$	$\lambda(k) = (k \lll 1)$	$\lambda(k) = (k \lll 2)$	$\lambda(k) = (k \lll 3)$
AES	4	1.297	9	10	9	10
ARIA	4	1.281	10	9	9	10
Kalyna π_0	8	1.453	10	10	10	9
Kalyna π_1	8	1.406	9	10	10	9
Kalyna π_2	8	1.422	9	9	9	11
Kalyna π_3	8	1.422	10	10	9	10
Kuznyechik	8	1.562	10	9	9	10

As we can see, while maximal EDP values (which is equal to MDP of H_{k_1,k_2}) remains pretty low, maximal DP values of model ciphers with dependent round keys are even worse, than the ones of one-round functions. The similar results are valid for other considered forms of round functions. All of this implies that we cannot evaluate the security of ciphers with dependent round keys grounding only on EDP estimations.

Conclusions

In this paper we researched the impact of round key dependency on the security of block ciphers against differential and linear cryptanalysis. We found that the two-round cipher with fully dependent

round keys is not a Markov cipher, even if its round functions are. We obtained analytic upper bounds for differential probabilities of such cipher and showed that average differential probabilities have the same behavior as in Markov cipher, but this is not enough to claim cipher security (which was illustrated on model ciphers).

Round keys cannot be generated from each other with deterministic procedure if we want to avoid such security flaws. One of the possible approach to make round keys statistically independent is to generate them from common source (e.g. master key) with increased amount of entropy. Anyway, the provable and practical security of the ciphers with dependent round keys should be reconsidered.

First Fall Degree and Weil Descent on the Multivariate Quadratic Problem

Yacheng Wang, Takanori Yasuda[1] *and Tsuyoshi Takagi*[2]

[1]Okayama University of Science, Okayama, Japan
[2]Department of Mathematical Informatics, The University of Tokyo, Tokyo, Japan
yacheng.wang@icloud.com

Abstract

The security of multivariate cryptography, one of candidates for post-quantum cryptography, depends on the hardness of solving a multivariate polynomial system over a finite field, which is called multivariate quadratic problem (MQ problem). In this paper, we investigate Weil descent on a polynomial system over a finite field, which transforms it into a new polynomial system over its subfield, and then we analyze the complexity of solving this new system using Gröbner basis techniques through its first fall degree and non-trivial syzygies. As a result, we give a concrete formula for estimating this first fall degree and verify its correctness through some experiments.

Keywords: Weil descent, Multivariate quadratic, First fall degree, Syzygies

1. Introduction

As currently widely used cryptosystems are being threatened by quantum computers, more research on post-quantum cryptography (PQC) is needed. NIST have taken actions on standardizing PQC, and their project has entered 3rd round of screening, where multivariate signature Rainbow is chosen as a finalist and GeMSS is chosen as an alternative candidate. Multivariate cryptography, a candidate for post-quantum cryptography, uses a multivariate polynomial system as its public key and its security is based on the hardness of solving this public key polynomial system, which is called the multivariate quadratic problem (MQ problem). Gröbner basis techniques are used on solving the MQ problem and its complexity is directly related to the degree of regularity of the ideal generated by this polynomial system. And index of regularity and first fall degree of the ideal generated by a polynomial system is often used to approximate degree of regularity when it is intractable.

Weil descent [1], which transforms a polynomial system over a field into a new polynomial system over its subfield, was first proposed to break the discrete logarithm problem on algebraic curve over composite fields, and can also be applied to the MQ problem. However, it is still unclear whether Weil descent makes a difference on solving the MQ problem and we want to fill in this gap in our work.

The main contribution of this paper is giving a complexity analysis on the Weil descent against the MQ problem. More specifically, we analyze its first fall degree by considering its non-trivial syzygies.

2. Multivariate Quadratic Problem

In this section, we review the multivariate quadratic problem, Gröbner bases and complexity for computing a Gröbner basis of a multivariate polynomial system.

2.1. Multivariate Quadratic Problem

Let $\mathbb{F}$ be a finite field of order p^q, $m, n \in \mathbb{N}$, and $R := \mathbb{F}[x_1, \ldots, x_n]$ be the polynomial ring of n variables over $\mathbb{F}$. Given a polynomial system $F = \{f_1, \ldots, f_m\} \subset R$ of degrees $d_1, \ldots, d_m$, let homogeneous component of f_i of degree d_i be $\tilde{f}_i$ for $i = 1, \ldots, m$ and $\tilde{F} = \{\tilde{f}_1, \ldots, \tilde{f}_m\}$. The ideal generated by F and $\tilde{F}$ are denoted by $\langle F \rangle$ and $\langle \tilde{F} \rangle$, individually.

When $d_1 = \cdots = d_m = 2$, given a vector $(y_1, \ldots, y_m) \in \mathbb{F}^m$, the problem of solving $\{f_i - y_i = 0 \mid i = 1, \ldots, m\}$ is called the MQ problem. Let $G = \{f_i - y_i \mid i = 1, \ldots, m\}$, $\langle G \rangle$ be the ideal generated by G and $\tilde{G}$ be the quadratic homogeneous components of G. An effective method for solving G is through Gröbner basis computation. According to Lazard's theorem [2], the row echelon form of the matrix constructed from coefficients of degree d polynomials in $\langle G \rangle$ gives a Gröber basis for any d larger than a certain degree d', which is called *degree of regularity* of $\langle G \rangle$, denoted by $d_{reg}(\langle G \rangle)$. The complexity of computing a Gröbner basis can hence be estimated by $O\left(\binom{n+d_{reg}}{d_{reg}}^{\omega}\right)$, where $2 \leq \omega \leq 3$ is the linear algebra constant. However, d_{reg} of polynomial systems other than regular or semi-regular systems are intractable to be precisely estimated. Its upper bound, *index of regularity*, and lower bound, *first fall degree*, are often used to approximate it.

Index of regularity of $\langle G \rangle$, denoted by $i_{reg}(\langle G \rangle)$, is defined as the degree, at which the Hilbert function $HF_{R/\langle \tilde{G} \rangle}(i) := \dim_{\mathbb{F}}(R_i/\langle \tilde{G} \rangle_i)$ stabilizes, where R_i and $\langle \tilde{G} \rangle_i$ represent homogeneous polynomials of degree i in R and $\langle \tilde{G} \rangle$, respectively.

First fall degree of $\langle G \rangle$, denoted by $d_{ff}(\langle G \rangle)$ is defined to be the smallest degree of non-trivial syzygies of $\tilde{G} = (\tilde{g}_1, \ldots, \tilde{g}_m)$, where syzygies are m-tuples $\mathbf{s} = (s_1, \ldots, s_m) \in R^m$ such that $\sum_{i=1}^{m} s_i \tilde{g}_i = 0$ and non-trivial syzygies are syzygies that are not linear combinations of the following syzygies:

$$(0 \cdots 0 \underset{\substack{i\text{-th}\\ \downarrow}}{-f_j} 0 \cdots 0 \underset{\substack{j\text{-th}\\ \downarrow}}{f_i} 0 \cdots 0), \quad (0 \cdots 0 \underset{\substack{i\text{-th}\\ \downarrow}}{f_i^{p^q-1}} 0 \cdots 0).$$

The degree of a syzygy $\mathbf{s}$ is defined as $\max_{1 \leq i \leq m} \deg(s_i \tilde{g}_i)$. We have $d_{ff}(\langle G \rangle) \leq d_{reg}(\langle G \rangle) \leq i_{reg}(\langle G \rangle)$, the equality holds for regular and semi-regular systems. Many results in multivariate cryptography are based on analyzing first fall degree when degree of regularity is intractable, and they have shown in some cases these two values are very close.

2.2. Computing Syzygies Using Linear Algebra

Given degree d homogeneous polynomials $f_1, \ldots, f_m \in R$, its degree d syzygies $\mathbf{s}_0 = (s_1^{(0)}, \ldots, s_m^{(0)})$ satisfy $(f_1, \ldots, f_m) \cdot \mathbf{s}_0^{\top} = 0$. Let $\mathbf{m}_0$ be the set of all monomials appeared in $f_1, \ldots, f_m$, and $\mathbf{c}_i \in \mathbb{F}^{|\mathbf{m}_0|}$ for $i = 1, \ldots, m$ be coefficients of

f_i with respect to $\mathbf{m}_0$. Then we have

$$\mathbf{m}_0 \cdot \begin{pmatrix} \mathbf{c}_1^\top & \mathbf{c}_2^\top & \cdots & \mathbf{c}_1^\top \end{pmatrix} \cdot \begin{pmatrix} s_1^{(0)} & \cdots & s_m^{(0)} \end{pmatrix}^\top = 0.$$

Therefore, $(s_1^{(0)}, \ldots, s_m^{(0)})$ can be obtained from the right kernel of the matrix $\begin{pmatrix} \mathbf{c}_1^\top & \mathbf{c}_2^\top & \cdots & \mathbf{c}_1^\top \end{pmatrix}$. Similarly, for degree $d+r$ syzygies $(s_1^{(r)}, \ldots, s_m^{(r)})$, we first find the set of degree r monomials $\mathbf{b} = (b_1, \ldots, b_t)$ in R. Then consider polynomials $b_i f_j$. Let $\mathbf{m}_r$ be all monomials appeared in $b_i f_j$ and $\mathbf{c}_{k,j} \in \mathbb{F}^{|\mathbf{m}_d|}$ be coefficients of $b_k f_l$. Then $(s_1^{(r)}, \ldots, s_m^{(r)})$ can be obtained from the left kernel of the matrix $\begin{pmatrix} \mathbf{c}_{1,1}^\top & \mathbf{c}_{2,1}^\top & \cdots & \mathbf{c}_{t,m}^\top \end{pmatrix}$.

3. Weil Descent on the MQ Problem

In this section, we specify $\mathbb{F}_{p^q}$ to be $\mathbb{F}_{2^q}$.

3.1. Weil Descent on the MQ Problem

Let $\{\theta_1, \ldots, \theta_q\} \subset \mathbb{F}_{2^q}$ be a basis for $\mathbb{F}_{2^q}/\mathbb{F}_2$, then there exists $y_{1,1}, \ldots, y_{1,q}, \ldots, y_{n,q}$ such that $x_i = \sum_{j=1}^{q} y_{i,j}\theta_j$ holds for $i = 1, \ldots, n$. Let $\hat{R} := \mathbb{F}_2[y_{1,1}, \ldots, y_{n,q}]$ be the polynomial ring over $\mathbb{F}_2$.

$F = \{f_1, \ldots, f_m\}$ is asked to be solved in the MQ problem, by substituting $\sum_{j=1}^{q} y_{i,j}\theta_j$ for x_i in F, we obtain a new polynomial system

$$\{f'_{1,1}, \cdots, f'_{1,q}, \cdots, f'_{m,q}, y_{1,1}^2 - y_{1,1}, \cdots, y_{n,q}^2 - y_{n,q}\}. \quad (1)$$

Note that equations $\{y_{1,1}^2 - y_{1,1} = 0, \cdots, y_{n,q}^2 - y_{n,q} = 0\}$ are trivial relations over $\mathbb{F}_2$.

3.2. Complexity Analysis

We will investigate the complexity of solving (1) using Gröbner bases computation by analyzing its d_{ff}. It is the smallest degree of non-trivial syzygies of its homogeneous components of highest degrees, which we denote by

$$\{\tilde{f}'_{1,1}, \ldots, \tilde{f}'_{m,q}, y_{1,1}^2, \ldots, y_{n,q}^2\}. \quad (2)$$

In (2), all $y_{i,j}^2$ for $i = 1, \ldots, n, j = 1, \ldots, q$ vanish, which leads to vanishing of x_i^2 for $i = 1, \ldots, n$. Moreover, non-trivial syzygies of (2) can be derived from non-trivial syzygies of $\tilde{f}_1, \ldots, \tilde{f}_m$. Therefore, non-trivial syzygies of (2) can be obtained from non-trivial syzygies of $\tilde{f}_1, \ldots, \tilde{f}_m$ coupling with $x_i^2 = 0$ for $i = 1, \ldots, n$ using linear algebra techniques introduced in section 2.2. Eventually, we can obtain a formula for d_{ff} of (2) under different m, n shown in (3).

3.3. Experiments

We run some experiments on the correctness of our formula using random polynomial systems. Fig. 1 shows the results. Moreover, we compare complexity of solving a random polynomial system of $n = m = 11, q = 2, \ldots, 8$ with direct Gröbner basis solving and Weil descent and plot the results in Fig. 2.

4. Conclusion

We theoretically investigated the complexity of Weil descent on a multivariate polynomial system by analyzing its first fall degree. We gave a concrete formula for estimating this first fall degree and testified it via experiments. Moreover, our experiments showed the difference between first fall degree and degree of regularity was no larger than 1, but this was not yet clarified in our research and left for future investigation.

$$\begin{cases} \min\left\{d \;\middle|\; m\binom{n}{d-2} > \binom{n}{d}\right\} \cap \{2,3\} \\ \min\left\{d \;\middle|\; m\binom{n}{d-2} > \binom{n}{d} + \binom{m}{2} + m\right\} \cap \{4\} \\ \min\left\{d \;\middle|\; m\binom{n}{d-2} > \binom{n}{d} + n\left(\binom{m}{2} + m\right)\right\} \cap \{5\} \\ \min\left\{d \;\middle|\; m\binom{n}{d-2} > \binom{n}{d} + \binom{n}{2}\left(\binom{m}{2} + m\right) - \frac{n(n+1)(n+2)}{6}\right\} \cap \{6\} \\ \min\left\{d \;\middle|\; m\binom{n}{d-2} > \binom{n}{d} + \binom{n}{3}\left(\binom{m}{2} + m\right) - \frac{n^2(n+1)(n+2)}{6}\right\} \cap \{7\} \\ \vdots \end{cases} \quad (3)$$

Figure 1: *Comparison of the estimated first fall degree (est. d_{ff}), experimental first fall degree (exp. d_{ff}) and experimental degree of regularity (exp. d_{reg}) of polynomial systems derived from Weil descent. It shows exp. d_{ff} (green line) and est. d_{ff} (blue line) match perfectly for the chosen parameters and the difference between exp. d_{reg} (red line) and est. d_{ff} (blue line) is no larger than 1*

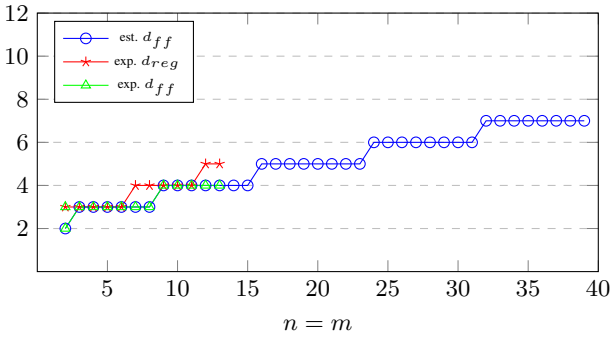
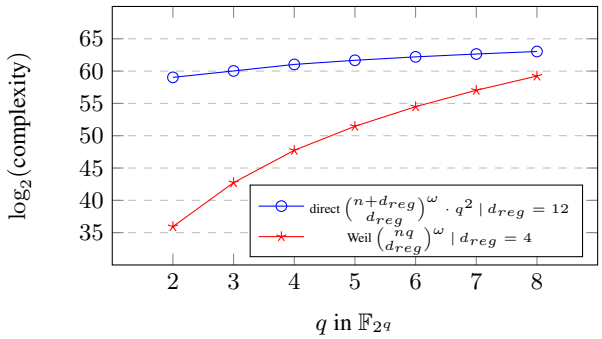


Figure 2: *Comparison between the complexity of directly solving $f_1, \ldots, f_m \in R$ using Gröbner basis techniques and Weil descent with $n = m = 11, \omega = 2.8$ and q ranging from 2 to 8*



5. References

[1] G. Frey and H.-G. Ruck. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[2] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *European Conference on Computer Algebra - EUROCAL 1983*, volume 162 of *LNCS*, pages 146–156. Springer, 1983.

Searching for row complete latin squares (a new benchmark for SAT solvers)*

Daniel Janči , Viliam Hromada , and Milan Vojvoda[1]

Slovak University of Technology in Bratislava, Slovaki
[1]milan.vojvoda@stuba.sk

Several designs of various cryptographic algorithms and primitives (stream cipher Edon80, hash function NaSHA, S-boxes [2], etc. [5]) in the past years used quasigroups. Usually quasigroups with some special properties were used. Quasigroups are tightly connected with latin squares since Caley table of a quasigroup is a latin square and for each latin square the is a quasigroup that has the given latin square as its Caley table.

A latin square of order n is an $n \times n$ array filled with n distinct symbols (e.g. $0, 1, \ldots, n-1$) with the property that each row and each column contains a permutation of these n symbols [1].

One way of finding a special quasigroup (latin square) is to find an algorithm for its construction. In our approach we transformed the problem of the existence of a special latin square to the famous SAT problem. Instances of a SAT problem can be solved using a SAT solver. SAT solvers are also used for cryptanalysis and also in attacks on logic locking of logical circuits. Each year a SAT solver competition [4] takes place. Properly chosen formulas (solvable within one hour, but not in a negligible time) can be also used as a new benchmark for the SAT solver competition [4].

In our contribution we show how to create a CNF formula using boolean variables that is satisfiable iff the special latin square exists. We focused our attention on the so called row complete latin squares.

A latin square L is said to be row-complete [1], if for all pairs (α, β), $\alpha \neq \beta$, $\alpha, \beta \in \{0, 1, \ldots, n-1\}$ there is a row i of L, $0 \leq i < n$ such that $L(i, j) = \alpha$ and $L(i, j+1) = \beta$, $0 \leq j < n-1$.

The construction of row-complete latin squares of even order is known for years [6]. Later Higham proved that row complete latin squares of any composite order do exist [3]. It is not known if there are any row-complete latin squares of some prime order. By exhaustive search it was shown that there are no row-complete latin squares of prime orders n=3,5,7.

We will present the results of our experiments, the running times of the CaDiCaL SAT solver needed to find row complete latin squares (of non prime order yet :)), including the impact of the order of clauses in the CNF formulas.

*This project is supported by NATO Science for Peace and Security Programme under Grant G5448

8 s p	8 1c s p	rand	1c rand
39.7	0.36	15.04	4.29
39.43	0.36	110.29	5.16
39.53	0.36	3	13.07
39.55	0.36	10.81	0.93
40.55	0.36	153.82	16.87
39.45	0.36	0.26	20.76
39.54	0.36	171.81	5.11
39.53	0.36	0.25	4.71
40.65	0.36	7.02	2.47
39.42	0.36	5.15	1.41

Table 1: Running times in seconds (as were stated by the CaDiCaL SAT solver itself) needed to find a row complete latin square of order 8 with various order of clauses in formula. Rand = random order of clauses in formula, 1c = first column forced to be 1, 2, ..., 8, s p = firstly clauses that ensure that an item cannot occur more than once in a row/column and then clauses that ensure that each item has to appear in each row/column. The SAT solver was running on a PC with Linux Ubuntu, Intel i5-6400, 2.7GHz, 4 cores, 8GB DDR4 2133MHz memory.

References

[1] Dénes, J., Keedwell, A.D.: Latin Squares and Their Applications, Academic Press, NY, 1974.

[2] Grošek, O., Satko, L., Nemoga, K.: Ideal difference tables from an algebraic point of view, Cryptology and Information Security, Proceedings of VI RECSI, ammendment to CRIPTOLOGÍA y SEGURIDAD de la INFORMACIÓN, RA-MA, Madrid, 2000, pp. 453-454.

[3] Higham, J.: Row-complete Latin squares of every composite order exist, J. Combin. Des. 6 (1998) 63–77.

[4] The International SAT Competition Web Page, `http://www.satcompetition.org/`.

[5] Shcherbacov, V.: Elements of quasigroup theory and applications. CRC Press 2017.

[6] Williams, E.J.: Experimental Designs Balanced for Pairs of Residual Effects, Australian J. Sci. Research, Ser. A, 3(1950), pp. 351–363.

COMBINATORIAL PROPERTIES OF THE SYSTEM OF LINEAR RESTRICTIONS OVER A FINITE FIELD

Oleh Kurinnyi
Institute of Physics and Technology
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»
ol.kurinnoy@gmail.com

ABSTRACT

In this work we formulated a problem of recovering unknown vector by partial information given in the form of linear dependencies. We proposed formalization of this problem by introducing a notation of the system of linear restrictions over a finite field. We proved several claims about a cardinality of a solution set of the system of linear restrictions with zero/non-zero right-hand sides generated by an unknown fixed vector.

***K*eywords** System of linear restrictions · Algebraic cryptanalysis · Finite field · Stream ciphers · Saturation point

1 Introduction

Standard models of algebraic cryptanalysis search dependencies between plaintexts, ciphertexts and keys in a form of a system of polynomial equations over a finite field [1]. But we can consider an alternative problem when only some restriction on possible values of dependencies with an unknown vector are known. Research of such problem is expedient because there are many methods that allows to get partial information about intermediate values of some parameters of encryption process. These methods can indicate that some dependencies with unknown parameters can't get specific finite range of values. Such information can be obtained from a side channel or weaknesses of a cryptosystem implementation. So we can formulate the problem of unknown vector recovering with information given in the form of linear dependencies. As a formalization of this problem, we introduced a notation of the system of linear restrictions over a finite field. In practice, the system of linear restrictions is generated with fixed but unknown vector, so we'll mainly consider this case. Obtained in this paper results can be applied to algebraic cryptanalysis of stream ciphers and cryptosystems based on linear codes [2].

2 Results

Let's define a notation of the system of linear restrictions with analogy to the system of linear equations.

The system of linear restrictions over a field $\mathbb{F}$ is a system of expressions of the form

$$\begin{cases} a_1^{(1)}x_1 + a_2^{(1)}x_2 + \ldots + a_n^{(1)}x_n \neq a_0^{(1)} \\ \cdots \\ a_1^{(m)}x_1 + a_2^{(m)}x_2 + \ldots + a_n^{(m)}x_n \neq a_0^{(m)} \end{cases},$$

where $a_i^{(j)} \in \mathbb{F}$ for $i = \overline{0,n}, j = \overline{1,m}$, $x_i \in \mathbb{F}$ for $i = \overline{1,n}$ and $m > 1$. Shortly we can denote the system as $A \cdot x \neq a_0$, where A and a_0 are, respectively, matrix and vector of coefficients. Also the symbol «$\neq$» is used in untypical context and stands for «not equal in all components». If the constants $a_0^{(j)} = 0$ for $j = \overline{1,m}$, then we can write $A \cdot x \neq \overline{0}$.

Solution of the system is a vector $x_0 \in \mathbb{F}^n$ that satisfies every restriction in the system. *Solution set* is a set of all solutions: $\{x \in \mathbb{F}^n | A \cdot x \neq a_0\}$.

Commonly used on practice case is $\mathbb{F} = \mathbb{F}_{2^k}$, so we'll consider binary fields, but all results can be easily generalized to arbitrary finite fields. Also, we'll consider systems, generated with fixed vector $z^{(tr)} \in \mathbb{F}_{2^k}^n$, $n \geq 2$, because on practice we usually know that cryptosystem works with such fixed parameter (for example, key or initial vector) for a while. Let A_{true} is the set $\{a \in \mathbb{F}_{2^k}^n | (a, z^{(tr)}) \neq 0\}$, where $(a, z^{(tr)})$ is the inner product of vectors a and $z^{(tr)}$.

Proposition. *The number of vectors in A_{true} is $2^{kn} - 2^{k(n-1)}$.*

Now we can form the system of linear restrictions from all vectors in A_{true}. We'll denote solution set of this system as D_{true}. Such a system is the most *complete*, because it includes all possible restrictions for $z^{(tr)}$. Now the question arises whether we can find the vector that was used for a generation of A_{true}. The answer is positive, so we can restore $z^{(tr)}$ accurate to proportionality coefficient for a system $A \cdot x \neq \overline{0}$.

Theorem. *For the system of linear restrictions $A_{true} \cdot x \neq \overline{0}$ the cardinality of the solution set D_{true} is equal to $2^k - 1$.*

This theorem claims that it's possible to restore $z^{(tr)}$ or it's multiples for the complete system of restrictions. But the size of A_{true} tends to $|\mathbb{F}_{2^k}^n|$ with growth of k. That's why we should look for smaller systems, whose solution set is D_{true}. To formalize this problem we need one more notation. *The saturation point* is a number $\min_{A'} |A'|$, where minimum is taken over all A', such that $A' \subseteq A_{true}$ and $A' \cdot x \neq 0$ has solution set D_{true}. In fact, such set, on which minimum is reached, has all properties of A_{true}, but smaller size. Now let's consider the case of a non-zero right side.

As earlier, vector $z^{(tr)} \in \mathbb{F}_{2^k}^n$ is fixed (also assume that $z^{(tr)}$ is non-zero). For an arbitrary $b \in \mathbb{F}_{2^k}$ we can define the set

$$A_{true}^{(b)} = \{\langle a, b\rangle, a \in \mathbb{F}_{2^k}^n | (a, z^{(tr)}) \neq b\}.$$

Notice, that $A_{true}^{(0)}$ is equal to A_{true} accurate to a first component of each pair. Also, we can fix a non-zero element g and corresponding set $A_{true}^{(g)}$. Let's introduce a modified set $\widehat{A}_{true}$ as the union of sets $A_{true}^{(0)}$ and $A_{true}^{(g)}$. We also denote the solution set of this system as $\widehat{D}_{true}$.

Theorem. *For the system of linear restrictions $\widehat{A}_{true}$ the number of solutions $|\widehat{D}_{true}| = 1$.*

So, in the case of a non-zero right-hand side an unknown fixed vector can be recovered completely. The proof on this fact is constructive and it used a redundant number of vectors to eliminate all unnecessary candidates, expect of $z^{(tr)}$. That's why it's possible to propose more explicit construction of a matrix that will also have one solution.

Proposition. *Let $\widehat{A}_{expl} \subseteq \widehat{A}_{true}$ is a system of linear restrictions, which includes all possible restrictions of two types: a) restrictions, in which one component is equal to 1, all other components are zero and right side is also zero; b) restrictions, in which one component is non-zero, all other components is zero and right side is equal to g. Then such system has only one solution $z^{(tr)}$. Also, the cardinality of $\widehat{A}_{expl}$ is $(2^k - 1) \cdot n$.*

Now it's possible to give an upper bound for the saturation point (which defined similarly for a non-zero case).

Consequence. *For the system of linear restrictions with an unknown fixed vector and restrictions, in which right-hand sides are equal to zero or fixed element $g \neq 0$, the saturation point is upper bounded by $(2^k - 1) \cdot n$.*

In fact, such construction isn't so redundant as $\widehat{A}_{true}$, but still «brute force» for an unknown vector.

3 Conclusion

In this paper we formalized a problem of recovering an unknown vector by partial information with a notation of the system of linear restrictions. We proved several results about the cardinality of the solution set in cases of zero and non-zero right sides. These results show that in such cases an unknown fixed vector can be fully or partially recovered. Also, we introduced an explicit construction of matrix that gives an upper bound on the saturation point. It claims that on practice in some cases we can gather much less restrictions than all possible to fully recover unknown vector.

References

[1] Bard G.V. Algebraic Cryptanalysis / Gregory V. Bard., 2009. – Springer Science+Business Media, LLC, 2009. – 368 pp. – ISBN 978-0-387-88756-2.

[2] Menezes A. Handbook of Applied Cryptography / A. Menezes, S. Vanstone, P. Oorschot. – Boca Raton: CRC Press, Inc., 1996. – 816 pp. – (Discrete Mathematics and Its Applications).

Experimental Enumeration of Bent Functions with Binary Decision Diagrams

Reni Banov

University of Applied Sciences Zagreb
reni.banov@tvz.hr

Keywords: Bent functions, Binary Decision Diagrams, Cryptography

Since their introduction by Rothaus in 1976 [4], bent functions played an important role in the security of cryptographic systems. As functions which have a maximum Hamming distance from the set of affine functions, they are extensively used to achieve nonlinearity of S-boxes for block and stream ciphers. While the theory behind bent functions is substantially developed [3],[5], their enumeration is difficult even for a small number of variables (listed for $n \leq 6$). Bent functions are rare and they are found by sieving on a large number of prospective Boolean functions or constructed by various methods, such as the iterative Maiorana-McFarland method. This work observes the use of the novel sieving technique based on the Binary Decision Diagram (BDD) representation of Boolean functions.

The BDD structure was introduced by Akers [1], and gained true popularity with Bryant's work [2]. It is distinguished for compact representation of Boolean functions and for efficient manipulation with them. The BDD stands as a variant of the *directed acyclic graph* with two terminal vertices and efficiently represents a *truth table* of Boolean functions by encoding their values as paths from the top vertex to terminal vertices. Many variations of BDDs are developed for different purposes, for example, the Zero Decision Diagram (ZDD) to represent combinatorial sets. Herein we use the *Reduced Ordered BDD* (ROBDD) structure which is a canonical representation of Boolean functions, i.e. under certain conditions the Boolean function has only one representation with the ROBDD graph.

It is an established fact that the total number of Boolean functions with n-variables is 2^{2^n}, thereby imposing an extremely large search space of prospective functions to sieve for bentness. Such a large search space must be reduced and partitioned to make a sieving possible even for Boolean functions defined on small number of variables. The main steps of the approach are based on the compactness of ROBDD representation of Boolean functions and a *divide-and-conguer* implementation of algorithms on them, let us

- build the ROBDD graph for the *characteristic* function $1_{\mathbb{B}_n}$ of a set $\mathbb{B}_n$ of **all** Boolean functions with n-variables excluding the affine functions. The cardinality of such a set is known to be equal to $2^{2^n} - 2^{n+1}$,
- partition a *characteristic* function according to its *minterm* representation,
- based on certain properties of bent functions, eliminate *minterms* which cannot identify a bent function, and
- sieve through remaining *minterms* of a *characteristic function* $1_{\mathbb{B}_n}$ and select bent functions.

As a result of the ROBDD compactness the approach can be applied to enumerate bent functions for $n \leq 6$ variables. For example, the ROBDD graph for the *characteristic* function $1_{\mathbb{B}_6}$ has only 670 vertices, while the ROBDD graph encoding the full set of Bent functions $\mathcal{B}_6$ out of six variables contains approximately $12.7M$ vertices. Despite its hugeness, logical operations with such a graph are feasible by using the ROBDD diagram, though it appears unnecessary to utilize them on the whole graph. This paper reveals the idea of the graph reduction by the restriction of a characteristic function to a variable values, which actually brings on considerable graph reduction.

For the above mentioned characteristic function $1_{\mathbb{B}_n}$ of a set of all Boolean functions without the affine functions, restriction to the values of some variable $x_i \in \{0, 1\}$ will produce two disjunctive sets

characterized by restriction functions

$$1_{\mathbb{B}_{n-1}}(\ldots,0_i,\ldots),\ 1_{\mathbb{B}_{n-1}}(\ldots,1_i,\ldots)$$

This step can be further applied to these functions by selecting values for another variable

$$x_j \in \{0,1\} : j \neq i$$

thereby further reducing the sets. Having applied the steps repeatedly, we were able to confirm the number of Bent functions for $n = 8$ and even improve the upper bound on a number of Bent functions for $n = 10$. Since promising results have so far been obtained, we expect that such a technique can be further improved and thereby allow a better estimation of upper bounds for number of Bent function with $n \geq 10$ variables.

References

[1] Akers, S.B., *Binary Decision Diagrams*, IEEE Transaction on Computers, C-27 (6), 1978.

[2] Bryant, R.M., *Graph-Based Algorithms for Boolean Function Manipulation*, IEEE Transaction on Computers, 35 (8), 1986.

[3] Cusick, T.W., Stanica, P., *Cryptographic Boolean Functions and Applications*, Academic Press, 2nd Edition, 2017.

[4] Rothaus, O.S., *On "bent" functions*, Journal of Combinatorial Theory, Series A, 20 (3), 1976.

[5] Tokareva, N., *Bent Functions: Results and Applications to Cryptography*, Academic Press, 2015.

Arithmetic on generalized Hessian curves using compression function and its applications to the isogeny-based cryptography

Michał Wroński, Tomasz Kijko, Military University of Technology in Warsaw

In our work, we present formulas for differential-addition and doubling using a compression function $f_{GH,2}(P) = x_P + y_P$ of degree 2 on a generalized Hessian curve $E_{GH} : x^3 + y^3 + a = dxy$, where $P = (x_P, y_P)$, using elementary algebra methods. Moreover, we also present formulas for 2, 3-isogeny, and general ℓ-isogeny evaluation, using this function. It is worth noting that for compression function $f_{GH,2}$ such formulas have not been presented before. On the other hand, we also use elementary algebra methods for obtaining differential-addition and doubling formulas using compression function $f_{GH,6}(P) = x_P y_P$ of degree 6, as well as we present formulas for 2 and general ℓ-isogeny evaluation using this function.

Differential addition and doubling formula for the compression function of degree 2 and 6 on generalized Hessian curves. This time has been obtained using elementary algebra methods, not the Gröbner basis mechanism as in [1] and [2]. The most important part of this paper is presenting formulas for computing 2,3, and ℓ-isogenies on generalized Hessian curves using compression function of degree 2 and formulas for computing general ℓ-isogenies, for $\ell \neq 3$. In the case of the compression function of degree 6, it is worth noting that computing 3-isogenies, in this case, is impossible because it is impossible to distinguish compression of different points of order 3.

We also show that the compression function of degree 6 is much more convenient for using the isogeny-based cryptography because computation and evaluation of ℓ-isogeny are, in this case, much more efficient than similar computations for the compression function of degree 2. This situation holds because the compression function of degree 6 has a multiplicative character, and the compression function of degree 2 has an additive character.

Isogeny-based cryptography is one of the most promising fields in post-quantum cryptography. In the SIKE algorithm (Supersingular Isogeny Key Encapsulation) specification, x-line arithmetic on the Montgomery curve is used. However, it is also possible to use other alternative models of elliptic curves in this context, for example, Edwards, twisted Edwards curves, Huff's curves, Hessian curves, generalized Hessian curves, and twisted Hessian curves. We mainly focus on applying x-line arithmetic to the Hessian curves family. We consider compression function on generalized Hessian curves, given by $f_{GH,2}(P) = x_P + y_P$, where $P = (x_P, y_P)$. This compression function may be easily obtained from compression function $f_{TH,2}(P) = \frac{y_P+1}{x_P}$ on twisted Hessian curve E_{TH} and isomorphism between E_{GH} and E_{TH}, which is simple coordinates swapping.

Unfortunately, it seems that using compression function $f_{GH,2}$ in isogeny-based cryptography is reasonable only in the context of SIDH and SIKE protocols, where consecutive computations of 2 and 3-isogenies are required. In the case, when it is necessary to compute isogenies of larger degree, like, e.g., in CRS [3] and CSIDH [4], application of compression function $f_{GH,2}$ is challenging and inefficient because isogeny evaluation formula for twisted Hessian curves given in [5] (and thus for generalized Hessian curves) has multiplicative character. Unfortunately, the compression function $f_{GH,2}$ has an additive character.

A method for computing an odd general ℓ-isogeny on a generalized Hessian curve using the compression function $f_{GH,6}(x, y) = xy$ will be shortly described below.

For a generalized Hessian curve given by the equation

$$E_{GH} \ : \ x^3 + y^3 + a = dxy \tag{1}$$

and an ℓ-isogeny $\phi \ : \ E_{GH} \to E'_{GH}$, where $\ell = 2s + 1$, with a kernel $F = \{(1 : -1 : 0)\} \cup \sum_{i=1}^{s} \{(u_i, v_i), (v_i, u_i)\}$ one may obtain the isogenous generalized Hessian curve equation:

$$E'_{GH} \ : \ x^3 + y^3 + a' = d'xy, \tag{2}$$

where

$$\begin{aligned} a' &= a^\ell, \\ d' &= \left((1-2n)d + 6\sum_{i=1}^{s}\left(\frac{dr_i - a}{r_i}\right)\right)\prod_{i=1}^{s} r_i, \end{aligned} \tag{3}$$

and $r_i = f_{GH,6}(u_i, v_i) = u_i v_i$.

Finally, for $P = (x_P, y_P) \in E_{GH}$ one obtains that

$$\begin{aligned} f_{GH,6}(\phi(P)) = \ & \prod_{Q \neq (1:-1:0) \in F} x_{P+Q} y_{P+Q} = \prod_{Q \neq (1:-1:0) \in F} f_{GH,6}(P+Q) = \\ & \prod_{i=1}^{s} f_{GH,6}(P+Q) f_{GH,6}(P-Q), \end{aligned} \tag{4}$$

which may be easily computed using formula for differential-addition formula for compression function $f_{GH,6}$.

In conclusion, we believe that our methods may be helpful in isogeny-based cryptography algorithms and can be used in practice.

References

[1] R. Dryło, T. Kijko, and M. Wroński, "Determining formulas related to point compression on alternative models of elliptic curves," *Fundamenta Informaticae*, vol. 169, no. 4, pp. 285–294, 2019.

[2] M. Wroński, T. Kijko, and R. Dryło, "High-degree compression functions on alternative models of elliptic curves and their applications," *Submitted to Fundamenta Informaticae*, 2021.

[3] A. Rostovtsev and A. Stolbunov, "Public-key cryptosystem based on isogenies.," *IACR Cryptol. ePrint Arch.*, vol. 2006, p. 145, 2006.

[4] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "Csidh: an efficient post-quantum commutative group action," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 395–427, Springer, 2018.

[5] T. Dang and D. Moody, "Twisted hessian isogenies," tech. rep., IACR Cryptology ePrint Archive, 2019: 1003, 2019.

Linear complexity of some sequences derived from hyperelliptic curves of genus 2

Vishnupriya Anupindi[1] and László Mérai[2]

Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences
[1]vishnupriya.anupindi@oeaw.ac.at
[2]laszlo.merai@oeaw.ac.at

Pseudorandom sequences, i.e. sequences which are generated with deterministic algorithms but look random, have many applications, for example in cryptography, in wireless communication or in numerical methods. Based on the particular application, many different approaches for pseudorandomness have been proposed.

In this work, we are interested in studying the properties of pseudorandomness of sequences derived from hyperelliptic curves of genus 2. In particular, we want to study the linear complexity of these sequences.

The *N-th linear complexity* $L(s_n, N)$ of a sequence (s_n) over the finite field $\mathbb{F}_q$ is defined as the smallest non-negative integer L such that the first N terms of the sequence (s_n) can be generated by a linear recurrence relation over $\mathbb{F}_q$ of order L, that is, there exist $c_0, c_1, \ldots, c_{L-1} \in \mathbb{F}_q$ such that

$$s_{n+L} = c_0 s_n + c_1 s_{n+1} + \cdots + c_{L-1} s_{n+L-1}, \quad 0 \leqslant n \leqslant N - L - 1.$$

Linear complexity is a figure of merit of pseudorandom sequences introduced to capture undesirable linear structure in a sequence. It provides a test of randomness and is a standard tool to eliminate sequences with non-randomness properties. This test is implemented in many test suites such as NIST [2] and TestU01 [1].

Let C be a hyperelliptic curve of genus 2 defined by

$$C: \ y^2 = f(x)$$

with $f(x) = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$ over a finite field $\mathbb{F}_q$ of odd characteristic. Contrary to the elliptic case, hyperelliptic curves with higher genus ($g \geqslant 2$) do not form an additive group. However, one can define a group operation by introducing the *Jacobian* J_C of the curve C, which is a 2 dimensional abelian variety for genus 2 curves, that is, the Jacobian is a surface for genus $g = 2$.

The elements of the Jacobian can be represented by the Mumford representation, that is, for each $D \in J_C$ there is a one-to-one map

$$D \mapsto (u, v),$$

such that

1. u is monic,
2. u divides $f - v^2$,
3. $\deg(v) < \deg(u) \leqslant g$.

The addition of elements, given in Mumford representation, can be evaluated using Cantor's algorithm.

Our aim is to study the pseudorandomness properties of walks on the Jacobian $J_C(\mathbb{F}_q)$ defined by

$$W_n = D + W_{n-1} = nD + W_0, \quad n = 1, 2, \ldots,$$

with $D \in J_C(\mathbb{F}_q)$ and some initial value $W_0 \in J_C(\mathbb{F}_q)$.

We estimate the N-th linear complexity of the Mumford coordinates of the sequence (W_n). More precisely, for $D \in J_C(\mathbb{F}_q)$, let $[u_D(x), v_D(x)]$ be its Mumford representation, where for most elements,

$u_D(x) = x^2 + u_1(D)x + u_0(D)$ and $v_D(x) = v_1(D)x + v_0(D) \in \mathbb{F}_q[x]$. For the coordinate function $u_0(D)$, our result implies the following lower bound for the linear complexity

$$L(u_0(W_n), N) \geqslant \left\lfloor c\frac{\min\{t, N\}}{q} \right\rfloor, \quad \text{for } N \geqslant 1$$

for some absolute and explicit constant $c > 0$, where t is the order of D. A similar bound holds for the other coefficients. The most promising case is when the $\mathbb{F}_q$-rational elements of the Jacobian J_C is close to being a cyclic group, and D has order $t = q^{2+o(1)}$.

Our proof uses an embedding of the Jacobian J_C into $\mathbb{P}^8$ provided by Grant [3], for which he gave explicit addition formulas for points on the Jacobian. After tailoring these formulas for the Jacobian over finite fields, we are able to prove the required degree estimates in order to use Stepanov's method.

References

[1] P. L'Ecuyer, R. Simard, TestU01: *A C Library for Empirical Testing of Random Number Generators ACM Transactions on Mathematical Software*, Vol. 33, article 22, 2007.

[2] A. Rukhin et al., NIST Special Publication 800-22, Revision 1.a, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, https://www.nist.gov/publications/ statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic

[3] David Grant, *Formal groups in genus two*, Journal für die Reine und Angewandte Mathematik., Vol. 411, pages 96–121, 1990.

Application of Velusqrt algorithm to Huff's and general Huff's curves

Michał Wroński, Military University of Technology in Warsaw

This paper presents the Velusqrt method's application to the Huff's and general Huff's curve models. Although the formula for the computation of ℓ-isogeny using kernel polynomial for general Huff's curves is known and was given in [1], we found a similar formula for the case of Huff's curves. What is more, we presented many different compression functions suitable for such applications. Presented by us, the compression functions of degree 4 seem to be efficient for evaluating ℓ-isogeny. They seem to be also reasonable for computation of the ℓ-isogenous curves.

Huff's curve over K is provided by the equation [2]

$$H_{a,b} \ : \ ax(y^2-1) = by(x^2-1), \tag{1}$$

where $a^2 \neq b^2$ and $a, b \neq 0$. The neutral element is the point $O = (0,0)$ and for any point $P = (x_P, y_P)$ the opposite point is equal to $-P = -(x_P, y_P) = (-x_P, -y_P)$. Similarly, general Huff's curve over K is provided by the equation [3]

$$G_{\overline{a},\overline{b}} \ : \ \overline{x}(\overline{a}\overline{y}^2-1) = \overline{y}(\overline{b}\overline{x}^2-1), \tag{2}$$

where $\overline{a} \neq \overline{b}$ and $\overline{a}, \overline{b} \neq 0$. The neutral element is the point $\overline{O} = (0,0)$, and for any point $\overline{P} = (\overline{x}_P, \overline{y}_P)$ the opposite point $-\overline{P} = -(\overline{x}_P, \overline{y}_P) = (-\overline{x}_P, -\overline{y}_P)$.

The Velusqrt method was firstly showed in 2020. In [4] Bernstein, De Feo, Leroux, and Smith presented an odd-degree isogeny computation method called Velusqrt. They modified the algorithm for the evaluation of polynomials whose roots are powers $h_S(\alpha) = \prod_{s\in S}(\alpha - \zeta^s)$, with complexity $\tilde{O}(\sqrt{\#S})$, to use a similar technique with x-line arithmetic for points on an elliptic curve to evaluate $h_S(\alpha) = \prod_{s\in S}(\alpha - f([s]P))$, where $f : E \to \mathbb{F}_q$ is compression function (in the case of Weierstrass and Montgomery curve $f(P) = x$, where $P = (x,y)$, is compression function of degree 2). Such an algorithm has complexity $\tilde{O}(\sqrt{\ell})$, where ℓ is the degree of the isogeny.

As was shown in [4], the Velusqrt algorithm can be applied to the practical implementations of CSIDH and CSURF, obtaining faster solutions for $\ell \gtrapprox 110$ (it depends on many factors).

Other authors also analyzed the application of the Velusqrt method. For example, in [5] it was considered the constant-time implementation of CSIDH using the Velusqrt method. What is more, in [6] applications of Velusqrt algorithm to CSIDH and B-SIDH constant-time implementations were analyzed.

Application of compression functions of degree 2 for Huff's and general Huff's curves to the isogeny-based cryptography was presented in [7], but only in the case of traditional Vélu formulas. This paper extends presented in [7] applications of Huff's and general Huff's curves to the isogeny-based cryptography by adding new compression functions of degree 4 and their application to the Velusqrt method.

To find compression functions of degree 4, we used the method of Kohel. In [8], Kohel studied symmetric quartic models over binary fields with a rational 4-torsion point T. He showed that a genus one curve which admits translations by rational points and translation morphism $\tau_T = P + T$ on curve E is projectively linear (induced by a linear transformation of the ambient projective space), iff E is a degree n model determined by a complete linear system in $\mathbb{P}^{n-1}$ and T is in the n-torsion subgroup. Such a method was used in [9] to obtain high-degree compression functions on many alternative models of elliptic curves.

This paper uses his ideas to find new compression functions of high degree (degree 4) for Huff's curves and general Huff's curves. The compression functions for which we are looking for are invariant on the action of involution and translation by specific point T, in this case of order 2, which means that for the compression function of degree 4 it holds that $f_4(P) = f_4(Q)$ iff $Q = \pm P + [k]T$, for $k = \overline{0,1}$.

Finally, we used the formula by Moody and Shumow [1] for obtaining ℓ-isogeny on general Huff's curves using kernel polynomials, which is given by

$$\overline{\psi} = \left(\frac{\overline{x}\overline{g}(\overline{x})}{\overline{g}(0)(b\overline{x})^{2s}\overline{g}\left(\frac{1}{b\overline{x}}\right)}, \frac{\overline{y}\overline{h}(\overline{y})}{\overline{h}(0)(\overline{a}\overline{y})^{2s}\overline{h}\left(\frac{1}{\overline{a}\overline{y}}\right)} \right), \tag{3}$$

where $\overline{a}' = \overline{a}^{\ell}\overline{h}(0)^2$ and $\overline{b}' = \overline{b}^{\ell}\overline{g}(0)^2$. Let $\overline{F} = \{(0,0), (\overline{\alpha}_i, \overline{\beta}_i), (-\overline{\alpha}_i, -\overline{\beta}_i) : i = 1 \dots s\}$, where $-(\overline{\alpha}_i, \overline{\beta}_i) = (-\overline{\alpha}_i, -\overline{\beta}_i)$, is the kernel of an isogeny $\overline{\psi}$ of degree ℓ, where $\ell = 2s+1$. Functions $\overline{g}(\overline{x})$ and $\overline{h}(\overline{x})$ are therefore given by

$$\begin{array}{l} \overline{g}(x) = \prod_{i=1}^{s}\left(x^2 - \overline{\alpha_i}^2\right), \\ \overline{h}(y) = \prod_{i=1}^{s}\left(y^2 - \overline{\beta_i}^2\right). \end{array} \tag{4}$$

Using formula (3) and isomorphism between Huff's and general Huff's curves, we found formula for obtaining ℓ-isogeny on Huff's curves using kernel polynomials, which is given by

$$\psi(P) = \left(\frac{(-1)^s x g(x)}{x^{2s} g\left(\frac{1}{x}\right)}, \frac{(-1)^s y h(y)}{y^{2s} h\left(\frac{1}{y}\right)} \right). \tag{5}$$

Let $F = \{(0,0), (\alpha_i, \beta_i), (-\alpha_i, -\beta_i) : i = 1 \dots s\}$, where $-(\alpha_i, \beta_i) = (-\alpha_i, -\beta_i)$, is the kernel of an isogeny ψ of degree ℓ, where $\ell = 2s+1$. Functions $g(x)$ and $h(x)$ are therefore given by

$$\begin{array}{c} g(x) = \prod_{i=1}^{s} \left(x^2 - \alpha_i^2\right), \\ h(y) = \prod_{i=1}^{s} \left(y^2 - \beta_i^2\right). \end{array} \tag{6}$$

Using formula (3) we obtained formula for compression function of degree 2 on general Huff's curve which is given by Theorem 1.

Theorem 1 *Let us note that using the compression function $f_2(\overline{P}) = \overline{xy} = \overline{r}$ one obtains that*

$$f_2\left(\psi(\overline{P})\right) = \left(\frac{\overline{r}\,\overline{g}_2\left(\frac{\overline{r}(\overline{a}\overline{r}+1)}{\overline{b}\overline{r}+1}\right)\overline{h}_2\left(\frac{\overline{r}(\overline{b}\overline{r}+1)}{\overline{a}\overline{r}+1}\right)}{\overline{g}_2(0)\overline{h}_2(0)\left(\overline{a}\overline{b}\overline{r}\right)^{2s}\overline{g}_2\left(\frac{\overline{b}\overline{r}+1}{\overline{b}^2\overline{r}(\overline{a}\overline{r}+1)}\right)\overline{h}_2\left(\frac{\overline{a}\overline{r}+1}{\overline{a}^2\overline{r}(\overline{b}\overline{r}+1)}\right)} \right), \tag{7}$$

where $\overline{r}_i = \overline{\alpha}_i^2, \overline{g}_2(z) = \prod_{i=1}^{s}\left(z - \frac{\overline{r}_i(\overline{a}\overline{r}_i+1)}{\overline{b}\overline{r}_i+1}\right), \overline{h}_2(z) = \prod_{i=1}^{s}\left(z - \frac{\overline{r}_i(\overline{b}\overline{r}_i+1)}{\overline{a}\overline{r}_i+1}\right)$ and $\overline{a}' = \overline{a}^{\ell}\overline{h}_2(0)^2$ and $\overline{b}' = \overline{b}^{\ell}\overline{g}_2(0)^2$.

Similarly, using formula (5) we obtained formula for compression function of degree 2 on Huff's curve which is given by Theorem 2.

Theorem 2 *Let us note that using the compression function $f_2(P) = xy = r$ one obtains that*

$$f_2\left(\psi(P)\right) = \left(\frac{r g_2\left(\frac{r(ar+b)}{br+a}\right) h_2\left(\frac{r(br+a)}{ar+b}\right)}{r^{2s} g_2\left(\frac{br+a}{r(ar+b)}\right) h_2\left(\frac{ar+b}{r(br+a)}\right)} \right), \tag{8}$$

where $r_i = \alpha_i\beta_i, g_2(z) = \prod_{i=1}^{s}\left(z - \frac{r_i(ar_i+b)}{br_i+a}\right)$ and $h_2(z) = \prod_{i=1}^{s}\left(z - \frac{r_i(br_i+a)}{ar_i+b}\right)$ and $a' = (-1)^s\frac{a}{g_2(0)}$ and $b' = (-1)^s\frac{b}{h_2(0)}$.

We also showed similar formulas for some compression function of degree 4 on both general Huff's and Huff's curve.

Formulas presented in the paper may be easily applied to the postquantum isogeny-based algorithms like B-SIDH, CSIDH, and CSURF.

References

[1] D. Moody and D. Shumow, "Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves," *Mathematics of Computation*, vol. 85, no. 300, pp. 1929–1951, 2016.

[2] M. Joye, M. Tibouchi, and D. Vergnaud, "Huff's model for elliptic curves," in *International Algorithmic Number Theory Symposium*, pp. 234–250, Springer, 2010.

[3] H. Wu and R. Feng, "Elliptic curves in Huff's model," *Wuhan University Journal of Natural Sciences*, vol. 17, no. 6, pp. 473–480, 2012.

[4] D. Bernstein, L. De Feo, A. Leroux, and B. Smith, "Faster computation of isogenies of large prime degree," *arXiv preprint arXiv:2003.10118*, 2020.

[5] J. Chávez-Saab, J.-J. Chi-Domínguez, S. Jaques, and F. Rodríguez-Henríquez, "The sqale of csidh: Square-root vélu quantum-resistant isogeny action with low exponents." Cryptology ePrint Archive, Report 2020/1520, 2020. `https://eprint.iacr.org/2020/1520`.

[6] G. Adj, J.-J. Chi-Domínguez, and F. Rodríguez-Henríquez, "On new vélu's formulae and their applications to csidh and b-sidh constant-time implementations." Cryptology ePrint Archive, Report 2020/1109, 2020. `https://eprint.iacr.org/2020/1109`.

[7] R. Dryło, T. Kijko, and M. Wroński, "Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography." Cryptology ePrint Archive, Report 2020/526, 2020. `https://eprint.iacr.org/2020/526`.

[8] D. Kohel, "Efficient arithmetic on elliptic curves in characteristic 2," in *International Conference on Cryptology in India*, pp. 378–398, Springer, 2012.

[9] M. Wroński, T. Kijko, and R. Dryło, "High-degree compression functions on alternative models of elliptic curves and their applications," *Submitted to: Fundamenta Informaticae.*

A Provable 2-Signatures Scheme Based on a Certain BDHI-type Assumption in the Random Oracle Model

Mariusz Jurkiewicz

Military University of Technology, 2 Gen. S. Kaliski St., Warsaw, Poland
mariusz.jurkiewicz@wat.edu.pl

Extended abstract

This abstract is a brief description of our research that pertain to construction of a certain 2-signature scheme, which in turn is intended to be exploited in crypto-protocols requiring two independent credentials, as in cryptocurrencies for instance. The high level idea of the scheme is such that there are two signers with two independent keys $(\mathsf{sk}_1, \mathsf{pk}_1)$ and $(\mathsf{sk}_2, \mathsf{pk}_2)$, that sign the same message. Unlike the regular digital signature schemes (DSS), the signing algorithm here is split into two separated phases. Namely, within the first stage both signers independently make so-called pre-signatures with their secret keys and send them to the second phase. It must be highlighted that none of the signers has already control of signature generation process. Eventually, both the pre-signatures became a seed for creating a value of the proper signature.

Since the scheme itself exploits Type 3 pairings, the setup algorithm $\mathscr{G}(1^n)$ generates parameters of the following form $\mathsf{params} := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_{i,j}, \hat{e}, \mathsf{Hashes})$, where $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are three multiplicative cyclic groups of prime order p, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a pairing of Type 3 and $g_{i,j} \in \mathbb{G}_i$ with $i, j \in \{1, 2\}$. It is obvious that according to the definition, $\mathbb{G}_1 \neq \mathbb{G}_2$ and no efficiently computable isomorphism is known between $\mathbb{G}_1$ and $\mathbb{G}_2$, in either direction. The component Hashes consists of three hash functions $H_1 : \{0,1\}^* \to \mathbb{F}_p^*$, $H_2 : \mathbb{G}_T \times \mathbb{G}_T \to \{0,1\}^n$, $H_3 : \{0,1\}^* \to \mathbb{F}_p^* \times \mathbb{F}_p^*$. Below we describe some details of the scheme

$\mathsf{Gen}(1^n, \mathsf{params})$

1 : $s_1, s_2 \xleftarrow{\$} \mathbb{F}_p^*$
2 : $u_1 \leftarrow g_{1,1}^{s_1}, u_2 \leftarrow g_{2,1}^{s_2}$
3 : $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2) = (s_1, s_2),\ \mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2) = (u_1, u_2)$
4 : **return** $(\mathsf{sk}, \mathsf{pk})$

$\mathsf{Sign.Stage1\text{-}Signer1}_{\mathsf{sk}_1, \mathsf{params}}(M)$

1 : $t_1 \leftarrow g_{1,2}^{\frac{1}{s_1 + H_1(M)}}$
2 : **return** t_1

$\mathsf{Sign.Stage1\text{-}Signer2}_{\mathsf{sk}_2, \mathsf{params}}(M)$

1 : $t_2 \leftarrow g_{2,2}^{\frac{1}{s_2 + H_1(M)}}$
2 : **return** t_2

Even though DLP protects each of the pre-signatures against being forged, they are raw data and none of them ought to be sent via a publicly available canal. In case if at least one of the signing sites is outside a local network the protocols like VPN (IPSec) have to be used to provide secure data traffic.

$\mathsf{Sign.Stage2}_{\mathsf{params}}(M, t_1, t_2)$

1 : $\mathsf{nonce} \xleftarrow{\$} \{0,1\}^n$
2 : $(r_1, r_2) \leftarrow H_3(\mathsf{nonce} \| M)$
3 : $\sigma = (\sigma_1, \sigma_2, \sigma_3) \leftarrow (t_1^{r_1}, t_2^{r_2}, \mathsf{nonce}\ \oplus H_2\left(\hat{e}(g_{1,1}, g_{1,2})^{r_1} \| \hat{e}(g_{2,1}, g_{2,2})^{r_2}\right))$
4 : **return** σ

$\mathsf{Vrfy}_{\mathsf{pk},\mathsf{params}}(M,\sigma)$

1 : $\lambda_1 \leftarrow \hat{e}\left(u_1 \cdot g_{1,1,}^{H_1(M)}, \sigma_1\right),\ \lambda_2 \leftarrow \hat{e}\left(u_2 \cdot g_{1,2,}^{H_1(M)}, \sigma_2\right)$

2 : $\eta \leftarrow H_2(\lambda_1 \| \lambda_2) \oplus \sigma_3$

3 : $(\tau_1, \tau_2) \leftarrow H_3(\eta \| M)$

4 : **if** $\lambda_1 = \hat{e}(g_{1,1}, g_{1,2})^{\tau_1}$ **and** $\lambda_2 = \hat{e}(g_{2,1}, g_{2,2})^{\tau_2}$

5 : **return** 1

6 : **else**

7 : **return** 0

The security proof is conducted in the random oracle model, where the hash function H_1 is modeled as a random oracle. To be more precise we show that making a forgery is at least as hard as solving a two-bilinear inversion problem that we denote ℓ-2BDHI$_3$ and define in the following way

$$\begin{aligned} \ell\text{-2BDHI}_3: \quad & \text{given} \quad \{g_{1,j}, g_{1,j}^{\alpha}, \ldots, g_{1,j}^{(\alpha^{\ell})}; g_{2,j}, g_{2,j}^{\beta}, \ldots, g_{2,j}^{(\beta^{\ell})};\},\ j \in \{1,2\} \\ & \text{compute} \quad \hat{e}(g_{1,1}, g_{1,2})^{\frac{1}{\alpha}} \text{ and } \hat{e}(g_{2,1}, g_{2,2})^{\frac{1}{\beta}}. \end{aligned}$$

Moreover, we indicate that solving stronger version of ℓ-2BDHI$_3$ enables us to solve the classical bilinear Diffie-Hellman inversion problem $(\ell+1)$-BDHI$_3$. This strengthen means that except the above input data there has been also given an access to a certain decision oracle.

Formal Verification of Confidentiality in Attribute-Based Encryption through ProVerif

Baasansuren Bat-Erdene[1], Yuping Yan[1], and Mohammed B. M. Kamel[1,2,3]

[1]Faculty of Informatics, Eötvös Loránd University, Budapest, Hungary
[2]Institute of Data Science, Cloud Computing and IT Security, Hochschule Furtwangen University, Furtwangen, Germany
[3]Department of Computer Science, University of Kufa, Najaf, Iraq

Abstract

Attribute-based encryption (ABE) is an extension scheme of identity-based encryption and public-key encryption. It is able to achieve fine-grain access control and one-to-many encryption mode that makes it suitable in the practical applications. In addition to mathematical proofs, it is important to formally verify its security properties using different protocols. ProVerif as an automatic cryptographic protocol verifier that we have used to prove the protocol security in a formal way. In our paper, we use ProVerif to prove the confidentiality property of ABE secret key exchange in different protocols.

1 Attribute Based Encryption

Sahai and Waters [4] firstly proposed the ABE scheme in 2005 as the first one-to-many cryptosystem. In the ABE schemes, both the ciphertext and the key are related to a set of attributes. According to the characteristics of information and the attributes of receivers, the encryptor can customize an encryption strategy, and the generated ciphertext can be decrypted only by the users whose attribute satisfies the encryption policy [5]. ABE can be divided into two main versions: key-policy attribute-based encryption (KP-ABE) [3] and ciphertext-policy attribute-based encryption (CP-ABE) [1]. These two version differ in the phase where the access policies are settled. Due to its outstanding performances on practical applications, it is important to formally verify the security properties of ABE in different protocols.

2 ProVerif

ProVerif [2] is an automatic cryptographic protocol verifier, which has been used and developed since 2001. It is able to prove the security properties of secrecy, authentication and observational equivalences. ProVerif takes a model of the protocol in an extension of the pi calculus with cryptography and the security properties that we want to prove as inputs. Then, it automatically translates this information into an internal representation, and uses an algorithm based on resolution with free selection to determine whether a fact is derivable from the clauses or not. The goal of our paper is to proof the confidentiality property of ABE as part of different protocols using ProVerif protocol verification tool.

3 Formal Verification

Confidentiality means that legitimate users get access to the encrypted data or files by verifying their attributes. Only when the members meet the requirements of access control polices, the plaintext can be retrieved. On the other hand, every PPT adversary should be able to learn the plaintext without proper attributes with negligible probability only. Using ProVerif, first we defined the different algorithms of ABE. Then, we defined two different protocols and the required property, and specified the behavior of attacks and output the results based on attacks to prove the confidentiality property of ABE in various manifestations. We specifically discussed the security of ABE secret key exchange in different protocols.

4 Our contribution

In this paper, we will verify confidentiality property of ABE secret key exchange in two different protocols using ProVerif and show that without proper signing and asymmetrically encrypting the user secret key, an adversary can intrude and decrypt the ciphertext. A first protocol is through the use of Public Key Infrastructure (PKI), while the second protocol is based on the use of Key Distribution Center (KDC) as a trusted entity to check the public key and send the corresponding keys for signing and encryption.

References

[1] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." 2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007.

[2] Blanchet, Bruno. "An efficient cryptographic protocol verifier based on prolog rules." csfw. Vol. 1. 2001.

[3] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. 2006.

[4] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2005.

[5] Yan, Yuping, Mohammed BM Kamel, and Peter Ligeti. "Attribute-based Encryption in Cloud Computing Environment." 2020 International Conference on Computing, Electronics and Communications Engineering (iCCECE). IEEE, 2020.

On bipartite secret sharing

Máté Gyarmati*

Department of Computeralgebra
Eötvös Loránd University
gyarmati93mate@gmail.com

Abstract: Secret sharing is a method to distribute a sensitive information amongst the participants of the protocol. The secret can only be restored by some predefined coalitions of the participants called qualified subsets and the unqualified coalitions cannot determine anything about the secret. The system of qualified sets is called access structure. Secret sharing is used in many cryptographic protocols, e.g. multi-signatures, secure aggregations, secure shuffling, and other secure MPC protocols.

The most used secret sharing method the Shamir secret sharing assumes that the role of the participants is symmetric. In some applications where there is a hierarchy amongst participants for example business, companies, governments, we don't want to make such restrictions. Bipartite structures are a specific family of access structures where the participants are partitioned into two groups and a set is qualified if it consist enough participants from both groups. Within this work we prove a lower bound for information ratio, more precisely the Shannon-complexity of regular bipartite structures.

Keywords: Secret sharing, biparite access structures, Shannon-complexity

1 Introduction

An access structure Γ on P participants is bipartite, if $P = P_1 \cup P_2$, $P_1 \cap P_2 = \emptyset$ and $A \in \Gamma$ depends only on the cardinalities $A \cap P_1$ and $A \cap P_2$. More precisely if $n_1 = |P_1|$ and $n_2 = |P_2|$, Γ is given by an integer ℓ and two monotone sequences of integers

$$0 \leq a_1 < a_2 < ... < a_\ell \leq n_1 \text{ and } n_2 \geq b_1 > b_2 > ... > b_\ell \geq 0$$

such that $A \in \Gamma$ is equivalent to $|A \cap P_1| \geq a_k$ and $|A \cap P_2| \geq b_k$ for some $1 \leq k \leq \ell$. $(a_1, b_1), (a_2, b_2), ..., (a_\ell, b_\ell)$ is a staircase in the non-negative grid, having steps of width $w_k = a_{k+1} - a_k$ and heights $h_k = b_{k+1} - b_k$. We call a staircase regular if all heights and weights are the same.

We measure the complexity of an access structure with the information ratio, that is the amount of information the participants have to store related to the size of the secret. If the value is 1, then the structure called ideal. Computing the information ratio of an access structure is

*Research has been supported by the ÚNKP-30-3 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

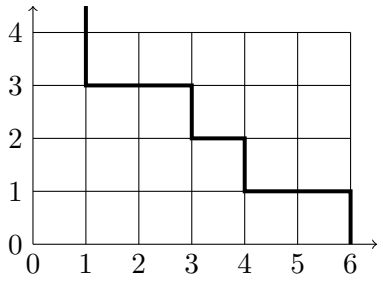


Figure 1: A staircase of length $\ell_\Gamma = 4$ for bipartite Γ with $n_1 = 6$, $n_2 = 4$. The widths of the steps are $2, 1, 2$, and the heights are $1, 1, 1$

usually a hard problem. The exact value is known only for small structures and specific families: for example access structures on at most 5 participants, most graph based access structures on at most 6 participants, tree represented access structures, D-dimensional cubes, D-dimensional cube with leaves, and some ideal structures.

Padro et. al. [1] proved that every regular bipartite with height and weight 1 is an ideal structure. Csirmaz et al. [2] computed the value of information ratio of some regular bipartite structures. Let denote w and h the weight and height respectively.

- If $w = h$ then the information ratio of the structure is $2 - 1/w$
- If $h = 1$ then the information ratio of the structure is $1 + \frac{(\ell-1)(w-1)}{\ell+w-2}$

Our work is a generalisation of these results. We proved a lower bound for every regular staircase.

The only known method to compute lower bound for information ratio is the entropy method. The properties and the definition of information ratio yields a linear programming problem. The solution of this LP is called Shannon-complexity denoted by κ and is a smaller bound for the information ratio.

I determined the Shannon-complexity for regular bipartite access structures by solving the corresponding LP problem. On one hand I proved a lower bound using combinatorial properties on the other hand I constructed a solution satisfying the constraints of the LP.

Theorem 1 *Consider the regular staircase of width w, height h and length ℓ where the points a_1, b_1 are not on the axis and $w \geq h$. Then the value of κ is*

$$\kappa = \frac{(\ell w - 1)(2w - 1)}{2w^2 + (h\ell + \ell - 2h - 3)w - h\ell + 2h}$$

In the cases of $w = h$ and $h = 1$ our formula yields the results mentioned above.

References

[1] Carles Padró and Germán Sáez. Secret sharing schemes with bipartite access structure. IEEE Transactions on Information Theory, 46(7):2596–2604, 2000.

[2] László Csirmaz, Frantisek Matus and Carles Pedró. Bipartite secret sharing and staircases. (Unpublished)

Multilevel secret sharing by finite geometry*

Máté Gyarmati

Department of Computeralgebra
Eötvös Loránd University
gyarmati93mate@gmail.com

Péter Ligeti

Department of Computeralgebra
Eötvös Loránd University
turul@cs.elte.hu

Peter Sziklai

Department of Computer Science
Eötvös Loránd University
sziklai@cs.elte.hu

Marcella Takáts

MTA-ELTE Geometric and Algebraic
Combinatorics Research Group
marcella.takats@ttk.elte.hu

Abstract:

Secret sharing refers to methods for distributing some secret information amongst a finite set of participants holding a partial information of the secret called share. The goal is to distribute these shares in such a way that only predefined coalitions of users are able to compute the secret.

Several secret sharing constructions are based on geometric objects. In this talk we investigate multilevel schemes, where the participants are partitioned into groups of the same role. Especially, we propose finite geometric constructions for compartmented and conjunctive hierarchical secret sharing schemes.

Keywords: Secret sharing, finite geometry, projective space

1 Introduction

Within this talk we consider secret sharing schemes from an algorithmic point of view. Assume that some secret information s is distributed amongst a group of participants $\mathcal{P}$ by a special additional entity called dealer. The dealer participates in this distribution step only. The secret s can be reconstructed from the respective share only when a sufficient number of shares are combined together. The collection of possible "reconstructers" is described by the so-called access structure $\mathcal{A}$, i.e. a monotone increasing set of subsets of the participants.

In this talk we use the following useful linear algebraic method introduced by Blakley and Kabatianskii [1] and van Dijk [2]. Let us assume that the dealer and the participants are assigned vectors $d, v_i \in \mathbb{F}_q^k$ for $i \in \mathcal{P}$. The proposed constructions are based on the following result:

*This research has been partially supported by Application Domain Specific Highly Reliable IT Solutions project which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme, by project K-120154 and project 132625 of the National Research, Development and Innovation Fund of Hungary, by the ÚNKP-30-3 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund and by the Lendület programme of the HAS.

Theorem 1 (Blakley and Kabatianskii [1]) *A linear secret sharing generated by* $G = (d, v_1, \ldots, v_{|\mathcal{P}|})$ *represents an ideal perfect secret sharing scheme realizing* $\mathcal{A}$ *if and only if the following conditions hold:*

1. $\forall X \in \mathcal{A}$ *the vector* d *is a linear combination of the vectors* $v_x, x \in X$*;*
2. $\forall Y \notin \mathcal{A}$ *the vector* d *is disjoint from the subspace generated by vectors* $v_y, y \in Y$*.*

Multilevel secret sharing is one straightforward generalization of the widely used t-threshold schemes, where, apart from some threshold value(s), the set of participants is partitioned into smaller subsets (called groups or levels) such that the users within any given level are equivalent from the secret sharing point of view. We are focusing on two special cases, namely on compartmented access structures with upper bounds and on hierarchical threshold access structures as a generalization of results [3]. Further general multilevel constructions based on bivariate interpolation techniques are introduced by Tassa and Dyn [4].

In *compartmented access structures with upper bounds* the goal is to avoid a given percentage of members from all (disjoint) groups in qualified subsets. More precisely, let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{G}_i$ and let $t \in \mathbb{N}, t_i \in \mathbb{N}, i = 1, \ldots, m$ be thresholds with $t \leq \sum_{i=1}^{m} t_i$. Then the access structure is the following:

$$\mathcal{A} = \{A \subseteq \mathcal{P} : \exists B \subseteq A \text{ such that } |B \cap \mathcal{G}_i| \leq t_i, \forall 1 \leq i \leq m \text{ and } |B| = t\}$$

We propose geometric constructions for the special case of $t_1 = \cdots = t_m = t - 1$ and show the limits of this method as well.

In *hierarchical* threshold access structures with m disjoint levels, let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{L}_i$ and let $t_1 < t_2 < \cdots < t_m$ be a sequence of thresholds. In *conjunctive* $(t_1, \ldots, t_m)$*-hierarchical schemes* the access structure is the following:

$$\mathcal{A} = \Big\{ A \subseteq \mathcal{P} : \big|A \cap \big(\bigcup_{j=1}^{i} \mathcal{L}_j\big)\big| \geq t_i, \text{ for all } 1 \leq i \leq m \Big\}.$$

We suggest ideal constructions for special cases of hierarchical access structures, in particular a 2-level conjunctive $(1, n+1)-$hierarchical scheme and 3-level conjunctive $(1, 2, n+1)$ scheme using finite geometry arguments. We propose ideas for generalization of these constructions for any number of levels.

References

[1] E.F. Blakley, G.A. Kabatianskii, Linear algebra approach to secret sharing schemes, *Error Control, Cryptology, and Speech Compression* **LNCS 829** (1994) 33–40.

[2] M. van Dijk, A linear construction of secret sharing schemes, *Des. Codes Cryptogr.* **12** (1997) 161–201.

[3] P. Ligeti, P. Sziklai, M. Takats, Generalized threshold secret sharing and finite geometry, *Des. Codes Cryptogr.*, to appear

[4] T. Tassa, N. Dyn, Multipartite secret sharing by bivariate interpolation, *J. Cryptology* **22** (2009), 227–258.

Control Flow Obfuscation with Irreducible Loops and Self-Modifying Code

Gregory Morse morse@inf.elte.hu[1],
Midya Alqaradaghi alqaradaghi.midya@inf.elte.hu[1], and
Tamás Kozsik kto@elte.hu[1]

[1]Eötvös Loránd Tudományegyetem/University (ELTE), Budapest, Hungary

April 10, 2021

Keywords: x86, x86-64, Assembly language, Self-modifying code, Obfuscation, Software protection, Control-flow graph, Irreducible loops

Protection mechanisms in recent times have focused on virtualization mechanisms as a form of securing software from prying eyes of reverse engineers. Some of the more successful implementations such as VMProtect have been largely defeated [1]. Other protections focus on anti-tamper capabilities and tend to rely on encryption such as Denuvo have similarly been defeated [2].

One area of protection which has not been extensively studied is the use of self-modifying code (SMC). Introducing it into binaries is possible with some special memory access modification whether in a static binary file or in memory created on-the-fly at runtime through operating system dependent procedures and based on the processor's memory access enforcement mechanisms. We will study an approach where loop transformations obfuscate the protected code, and dynamically generated SMC provides an effective solution to allow decisions in the transformed loops.

The idea that dynamically generated SMC has a blueprint that is used to generate custom "stamped" SMC on the fly has also not been studied. We will show that a graph algorithm such as depth-first search (DFS) based identification of strongly-connected components (SCCs) and topological sorting can be implemented by a SMC control-flow graph (CFG) representing the actual graph being queried. The ideas allow for an optimization geared towards simplification of the stack and are generalizable to largely any graph algorithm. The algorithms mentioned are those that make up an efficient linear Boolean 2-satisfiability (2-SAT) instance solver [3].

As for CFG obfuscation, the hardest structure for most static analysis tools to properly understand semantically is an irreducible loop, which is, informally speak-

ing, a loop with multiple entries. Nesting of irreducible loops can cause quadratic behavior where the loop nesting forest is constructed [4], and the only resolution to structuring them into an abstract syntax tree (AST) involves introduction of variables and conditional expressions [5]. Although almost linear time algorithms exist for building loop nesting forests of irreducible loops by various strategies which combine them, translation to the AST does not necessarily allow for the same reductions as identification.

This study will take a look at specifically a case study where every control flow construct, be it a conditional or loop, will be further embedded or converted into an irreducible loop nest designed to cause quadratic behavior in identification. These loops however will be largely fictitious allowing the original looping behavior, or a simple single iteration. The 2-SAT solver will be used to determine the exit conditions for all of the loops in question, and given that it uses dynamic SMC, will be beyond the scope of any state-of-the-art static analysis tools. The function which will be protected will be a security critical function such as a white-box AES or RSA implementation. Performance measurements and a look at how powerful tools such as IDA Pro and Ghidra disassemblers and decompilers will process them will be presented under Windows and Linux on the modern x86 and x86-64 platforms.

De-obfuscation techniques will continue to get stronger against complex virtualization schemes. Inevitably, the power of dynamic SMC would ensure more advanced capabilities be developed in static analysis frameworks. Currently, they largely do not consider it, making it one very open practical technique which causes theoretical problems that have not yet received attention.

References

[1] Anatoli Kalysch, Johannes Götzfried, and Tilo Müller. Vmattack: Deobfuscating virtualization-based packed binaries. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, New York, NY, USA, 2017. Association for Computing Machinery.

[2] J. Karthik, P. P. Amritha, and M. Sethumadhavan. Video game drm: Analysis and paradigm solution. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–4, 2020.

[3] Bengt Aspvall, Michael F. Plass, and Robert Endre Tarjan. A linear-time algorithm for testing the truth of certain quantified boolean formulas. *Information Processing Letters*, 8(3):121–123, 1979.

[4] G. Ramalingam. Identifying loops in almost linear time. *ACM Trans. Program. Lang. Syst.*, 21(2):175–188, March 1999.

[5] K. Yakdan, S. Dechand, E. Gerhards-Padilla, and M. Smith. Helping johnny to analyze malware: A usability-optimized decompiler and malware analysis user study. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 158–177, 2016.

DiSSECT: Distinguisher of Standard & Simulated Elliptic Curves via Traits

Vladimir Sedlacek[1,2], Vojtech Suchanek[1], and Antonin Dufka[1]

[1]Masaryk University
[2]Ca' Foscari University of Venice
{vlada.sedlacek, vojtechsu, dufkan}@mail.muni.cz

Abstract

It is hard to trust elliptic curves standardized in a non-transparent way. We present a new methodology and a tool to help spot any unexpected behaviour of these curves and potentially find a problem.

Keywords: elliptic curves, standards, simulations, testing tool

1 Introduction

The selection of elliptic curves suitable for cryptographic applications is a difficult task. There are widely used standards [3, 1, 4], defining elliptic curves with specific parameters and usually also describing how these parameters were generated. Unfortunately, the parameter selection is often unsatisfactorily explained, and there are documented instances of standards being manipulated [2].

According to the publicly known research, it is easy to detect weak elliptic curves (in the sense of ECDLP) based only on their order [3]. However, it is plausible that unknown vulnerabilities exist in some of the curves. A thorough analysis of the standard parameters is therefore needed to re-establish the trust, especially if the standards are not transparent enough.

2 Methodology and simulations

Instead of looking for some new specific vulnerability, we mimic the generation process as closely as possible to create a large set of simulated curves. It should not be possible to distinguish them from the corresponding standard ones in any way. Yet we try to do exactly that, using any means necessary. Any deviations found might reveal problems with the standards.

Following two specifications from two major standards X9.62 [1] and Brainpool [4], we have generated over 200 000 simulated curves[1]. At a few points, the standards were a little ambiguous (e.g., the class number computation in the Brainpool standard or the precise choice of curve parameters in the x9.62 standard), so we filled the gaps to reflect the choices made for the actual standard curves whenever possible. We plan to implement other standards where the parameter selection is explicit enough to allow reasonable simulations.

Both X9.62 and Brainpool deterministically generate each elliptic curve by hashing an initial seed and then check the specified security conditions. The actual seeds are claimed to be random, but their choice is not explained. In our simulations, we iterated over several millions of seeds and applied the same process. Thus our curves should be indistinguishable from the standardized ones.

3 Our tool DiSSECT

DiSSECT is, to the best of our knowledge, the largest publicly available database of standardized elliptic curves and offers generation of simulated curves according to the mentioned standards. The tool contains

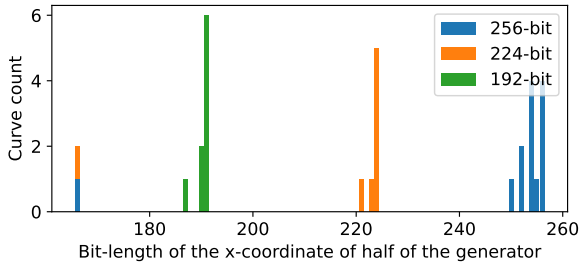
[1]This took up to a week per standard on 20-core cluster of Intel® Xeon® Gold 5218.

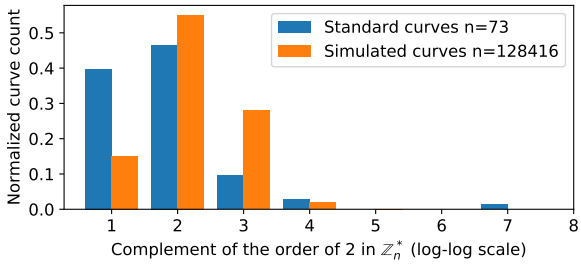
over 20 tests (which we call traits), each computing curve properties, ranging from classical algebraic ones to unconventional ones and those connected to implementations. After obtaining their empirical distributions, the traits allow us to compare the simulated curves to the standard ones. Finally, DiSSECT provides an easy-to-use interface for implementations of custom traits and their interactive visualization. We will make DiSSECT open-source in the near future and invite any collaborators. DiSSECT is written in Python 3 and imports the SageMath library. The database of the standardized elliptic curves as well as the simulated ones with the results of the traits, including the visualization, can be found at https://dissect.crocs.fi.muni.cz/.

4 First results

Here we highlight two discoveries made with DiSSECT. A trait inspecting the bit-length of the x-coordinate of half of the generator (in the left figure) revealed two curves (`secp256k1` and `secp224k1`) with only 166 significant bits. Further inspection showed that those values *are identical*. This property has been known before, but the ability to find it demonstrates the usefulness of our approach.

The right figure displays a single curve (`BLS12-381`) appearing as an outlier for a trait computing multiplicative orders of low primes modulo the curve order – pointing us to another property of the curve that we were not aware of.





Acknowledgements. Computational resources were supplied by the project "e-Infrastruktura CZ" (e-INFRA LM2018140) provided within the program Projects of Large Research, Development and Innovations Infrastructures. V. Sedlacek and A. Dufka were supported by Czech Science Foundation project GA20-03426S. V. Suchanek was supported by a grant from the Cisco University Research Program Fund, an advised fund of Silicon Valley Community Foundation. V. Sedlacek and V. Suchanek were also supported by the Ph.D. Talent Scholarship - funded by the Brno City Municipality.

References

[1] *American National Standard X9.62-1998, Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA)*. Preliminary draft. Accredited Standards Committee X9, 1998.

[2] D. J. Bernstein et al. "How to Manipulate Curve Standards: A White Paper for the Black Hat". In: *International Conference on Research in Security Standardisation*. Springer. 2015, pp. 109–139.

[3] D. J. Bernstein and T. Lange. *SafeCurves: choosing safe curves for elliptic-curve cryptography*. 2017. URL: `https://safecurves.cr.yp.to/`.

[4] *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. Tech. rep. IETF RFC 5639, 2010.

Fortification of OSP, a payload-agnostic IoT protocol

Roland Nagy, Zoltán L. Németh

Abstract

Optin Sensor Protocol (OSP) is a payload-agnostic, connection oriented Client-Server protocol aiming to minimize overhead for IoT applications. It has many features useful for IoT devices, but version 1.2 lacks any security features, thus it's not suitable for use cases, where confidentiality or the authentication of both parties is required. In this work, we identify the weaknesses of OSP 1.2, set the requirements for version 2.0 and design a more secure successor. We also implemented and tested this new protocol, formally and informally as well.

1 Introduction

OSP has features to eliminate transmission problems of unreliable connections and it's capable of updating, controlling and configuring devices, besides data transmission. Version 1.2[1] however lacks any security features: data is sent as plain text, the server is not authenticated and the client authentication has many flaws as well.

Our goal was to fortify OSP, design, implement and verify version 2.0. This version relies on cryptographic primitives to satisfy the requirements we determined by threat modelling. Our design respects the resource constraints of IoT environments. We provided a reference implementation, an informal test suit, and for formal validation, we created a model of the protocol for the Tamarin Prover[2] and used it to prove how the requirements are satisfied.

2 Threat modelling & requirements

Threat modelling is a process to identify and correct vulnerabilities and weaknesses of applications. To do so, we examine the application at an architectural level, rather then by inspecting the implementation itself. At the time we performed threat modelling of OSP 1.2, we couldn't find any framework suitable for protocol design. So we examined three threat modelling frameworks (ASF[3], STRIDE[4], and DREAD[5]), and tried to combine their essence in a threat modelling cheat-sheet we could use on protocols.

We identified several vulnerabilities and weaknesses, which led us to our requirements for the new version. These requirements include the authentication of the client and server as well, the integrity and authentication of messages, session integrity, the ability of confidential data transmission and the prevention of a possible DoS attack we discovered in version 1.2.

[1] https://optin.hu/static/www/OSP_spec_en.pdf
[2] https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf
[3] www.omtp.org/OMTP_Application_Security_Framework_v2_2.pdf
[4] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
[5] https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model

3 Design

For the purpose of authenticating the communicating parties, we introduced the a 4-way handshake, where both the client and the server can authenticate each other in a challenge-response manner, using symmetric encryption only. Message integrity, authentication and confidentiality is achieved by using the EAX[6] cipher operation mode. This way our packets can contain non-confidential, but authenticated parts (the fixed header) and encrypted data (the packet payload). A MAC is appended to each message, and only AES is needed, which is a suitable cipher for our low-resource environment. To achieve session integrity, we generate a 2-byte random session ID on the server side, at session establishment. Message IDs are also changed, to fix the following denial of service vulnerability. In OSP v1.2, a device can be tricked to request re-send of K messages, where K is the maximal message ID, by sending it two messages with the same ID. This issue can cause denial of service easily.

4 Implementation & evaluation

We implemented a reference client and server application. The client implementation was tested on Atmega328P and ESP8266 microcontrollers, and the overhead of the EAX operation was found to be acceptable (3 and 0.27 ms, respectively). The server can be considered to have infinite capacity, so testing its performance didn't seem to be relevant. We also implemented a simple domain specific language to generate client behavior from textual commands and implemented many test cases to check if the server handles errors as expect.

We created a Tamarin model as well for formal verification. In the model, we implemented a setup rule to generate keys, the 4-way handshake and simple data transmission. We checked if the handshake can be completed and we proved that the key can not be acquired by an attacker.

5 Conclusion

OSP 1.2 suffered from several security-related weaknesses. We corrected these in the new version while extended its functionality by confidential data transmission and integrity features. We implemented and tested the new protocol: the overhead of the used EAX primitive is acceptable, while the server implementation reacts to edge cases as expected. We also performed formal validation to prove the correctness of the handshake and to make sure that keys cannot be acquired by an attacker.

Acknowledgment

This research was supported by the project "Deepening the activities of the Hungarian Industrial Innovation Mathematical Service Network HU-MATHS-IN", no. EFOP-3.6.2-16-2017-00015. The project has been supported by the European Union and co-funded by the European Social Fund.

We would like to thank the contribution of Tamás Bitó (former MSc student of SZTE), Tamás Dékány (former employee of Optin Kft.) and Tamás Lautner (former employee of Optin Kft.)

[6] https://en.wikipedia.org/wiki/EAX_mode

Identity-based anonymous authentication for VANETs

Andrea Huszti, Norbert Oláh and Szabolcs Kovács
Faculty of Informatics, University of Debrecen
huszti.andrea@inf.unideb.hu, olah.norbert@inf.unideb.hu, kovacs.szabolcs@inf.unideb.hu

Nowadays, the number of cars is increasing rapidly. To increase the efficiency of transport and the safety of vehicles and pedestrians, there is an increasing need for participants to be able to communicate with each other. The ITS (Intelligent Transportation System) recommends the use of VANET (Vehicular Ad-hoc networks) for this. With the help of VANET V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) communication can be implemented.

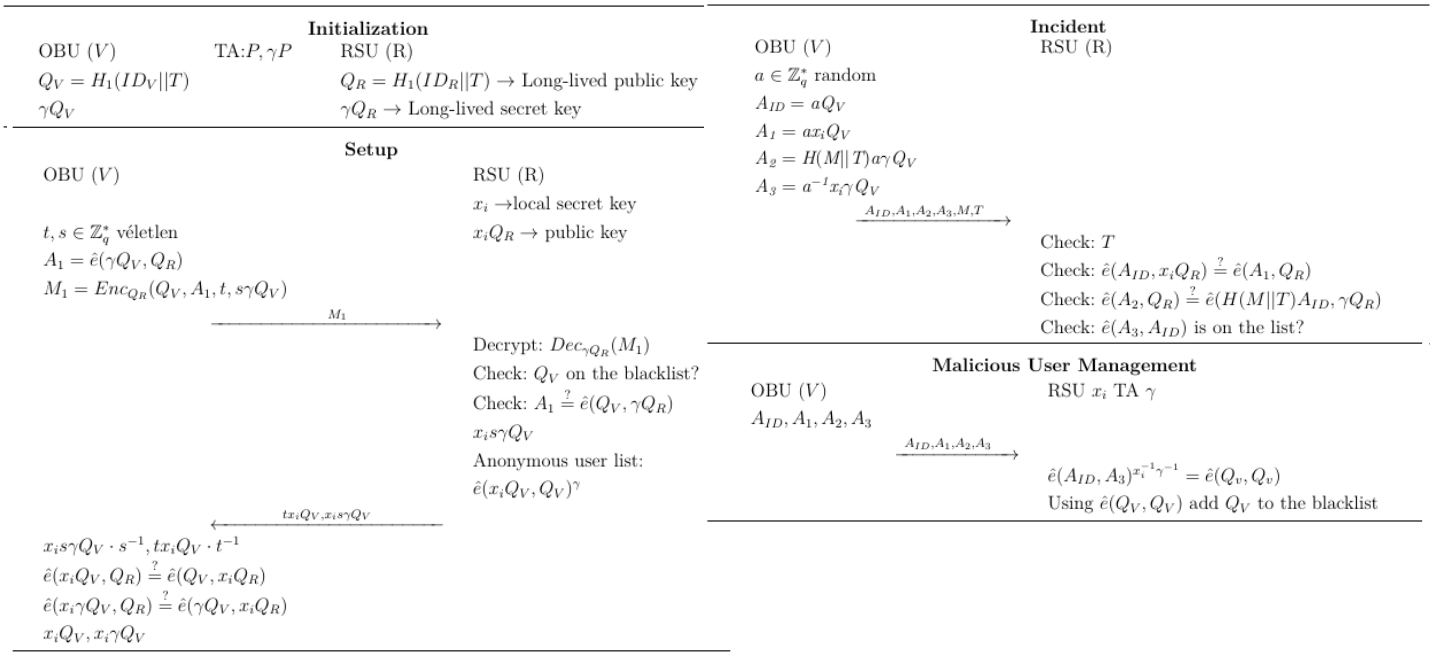
Identity-based cryptography (IBC) is proposed to replace Public Key Infrastructure. IBC does not require certificates because public keys are computed from identifiers. Thus, the relationship between the entity and the public key is in clear contrast to the Public Key Infrastructure, where a certificate is required for this. This can be a significant benefit in terms of saving on communication costs. Results show that operating costs are one-fifth of the cost of public key systems, and IBC users are three times more efficient than users of public key cryptography. In the identity-based model, each wireless node only needs to store public parameters, their own ID, and their secret keys. The device does not need to contact the recipient in advance to get its certificate, so the cost of managing and storing certificates is avoided.

Several proposals have been made in the scientific literature to secure the communication of self-driving vehicles. In the solution proposed by Zhaojun Lu et al. [3], the traditional public key infrastructure is combined with blockchains to ensure the protection of personal data. However, this solution is more complex and complicated than identity-based systems. In addition, the process execution requires more resources if certificates are applied. To initialize the system, entities must generate keys and communicate with leading organizations, which requires a secure channel. Due to the finite validity period of the certificates, they need to be updated from time to time. In addition, each device must store three lists (blockchains): a blockchain containing valid certificates, sent messages, and revoked public keys. Debiao He et al. proposed a scheme [1] that implements identity-based conditional authentication using elliptic curve cryptography on VANET systems. Their solution does not involve bilinear pairing, citing its high resource requirements. The disadvantage of this system is that if a car is compromised, the whole system is, as all parameters, including the master secret key, are stored on all devices.

We present a cryptographic protocol, where eligible vehicles can authentically and anonymously report road conditions (e.g. traffic jam, accident etc.). Our proposed solution is based on identity-based cryptography. To eliminate weaknesses of the previously mentioned solutions, our protocol takes advantage of bilinear pairing, so the devices do not store the master secret key, do not store certificates, revocation lists, moreover the anonymity of the sender can be revoked.

Our system consists of the following participants: a trusted third-party (TTP), roadside units (RSU) and vehicles with the on-board units (OBUs). Each roadside unit has its own domain. Within this, vehicles can communicate with each other and with the local roadside unit, but not directly with devices in other domains. RSUs are also connected to each other to form their own communication ring, through which they can share information about global traffic. There are advantages of applying bilinear mappings, a common secret master key can be easily used to authenticate participants due to bilinearity, moreover devices do not have to store the master secret key. The results of the performance analysis prove that using bilinear pairing our proposed system is practical as well. Another advantage of our solution is that the vehicles do not store a revocation list, only the roadside units check the list at the moment of registration to their domain. This relieves the on-board unit of less resources from storing any revocation list and constantly check it, yet the receiver can verify the authenticity of the senders of the received messages using bilinear mapping.

The protocol consists of four main phases. The first phase is **Initialization**, during which system parameters, public IDs, and secret keys are generated. The second phase is the **Setup of Communication**, where vehicles



entering the domain of a given RSU register, i.e., if they are eligible to send a message, they receive a pseudonym. The third phase is called **Incident,** where vehicles report road conditions, accident, traffic jam, etc.. The vehicle broadcasts its announcement to surrounding participants, which can be vehicles or the RSUs. The final phase is the **Malicious User Management** phase. In this phase, the anonymity of the malicious messengers is revoked, and their ID is added to the revocation list.

The proposed protocol meets the basic security requirements of VANET systems. The protocol implements authentic and anonymous messaging so that anonymity can be revoked by the RSU and TTP together. The identification and location data of the vehicles involved in the communication remain confidential, however, only an authorized vehicle can send a message. Also, at least one reliable authority is required for VANETs, which is responsible for allocating keys and controlling processes. However, the activities of this organizational unit must be transparent to all participants in the network. We have formalized the security analysis in AVISPA, which offers various tools to check security goals. One of these goals is providing mutual authentication of participants. In AVISPA, we apply witness and request pair for the verification of the authentication goal facts. We have also formalized the protocol and security goals, applied OFMC and CL-AtSe, and performed the attacker simulation. In the case of authentication, the result of the security analysis shows that the attacker is not able to impersonate the legal participants.

We have also implemented our protocol in Python (cPy) and also in MicroPython (uPy) for IoT devices. The computational costs were analyzed on three tools: a PC with an AMD Ryzen 5 3600 3.6 – 4.2 GHz 6-core/12 threads processor running the Python3 implementation; an ESP32 DevKit1 with a 240 MHz clock processor and a Raspberry Pi 4 b, which has a Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz processor, so it has much more computing capacity than an ESP32. We show our protocol is suitable for practice.

References

[1] D. He – S. Zeadally – B. Xu – X. Huang: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 10. (2015) 12., 2681–2691. p

[2] Z. Lu – W. Liu – Q. Wang – G. Qu – Z. Liu: A privacy-preserving trust model based on blockchain for VANETs. IEEE Access, 6. (2018), 45655–45664. p.

Scalix mix network

Ádám Vécsi[1] and Attila Pethő[2]

Department of Computer Science, Faculty of Informatics, University of Debrecen
[1]vecsi.adam@inf.unideb.hu
[2]petho.attila@inf.unideb.hu

By secure communication, most commonly we mean that the message sent between the communicating parties is encrypted with a cryptographic method since the message is considered to be the sensitive information. However, the communication includes several metadata, which might also be valuable for the observers. The metadata is basically the data about the data. It records the what, when, where, and whom of the communication. The focus of this work is the protection of the communicating parties' identity by providing anonymity with a mix network.

A mix network is a system designed by Chaum [1] that includes multiple stages of mixes, where every stage receives multiple messages, performs some cryptographic transformation for each message and permutes them. After every mix, tracking the path of the messages gets more and more difficult, achieving untraceability. The most important property of this protocol family is that it provides message untraceability against strong adversaries, which can observe the entire network. Of course, it comes with a cost, most of the protocols deliver messages with high latency. However, recent studies are focusing on solutions for low-latency mix networks, and some are achieving promising results. The Loopix [4] protocol, built on the Sphinx [2] mix format was able to narrow the delay to milliseconds. Loopix gives us a well-thought solution for cover traffic generation and network topology, which guarantees bi-directional sender and receiver anonymity. Although the paper gives promising benchmarks, we believe there are two bottlenecks of the protocol. One is the load balancing between the mixes in each stage, which is based on theoretical random generation, which in practice might result in overloaded and underloaded mixes. The other one is that the senders must pick the full path of the message, so the protocol requires a shared database with the information of every mix server, which could become costly to maintain if there are lots of mix servers.

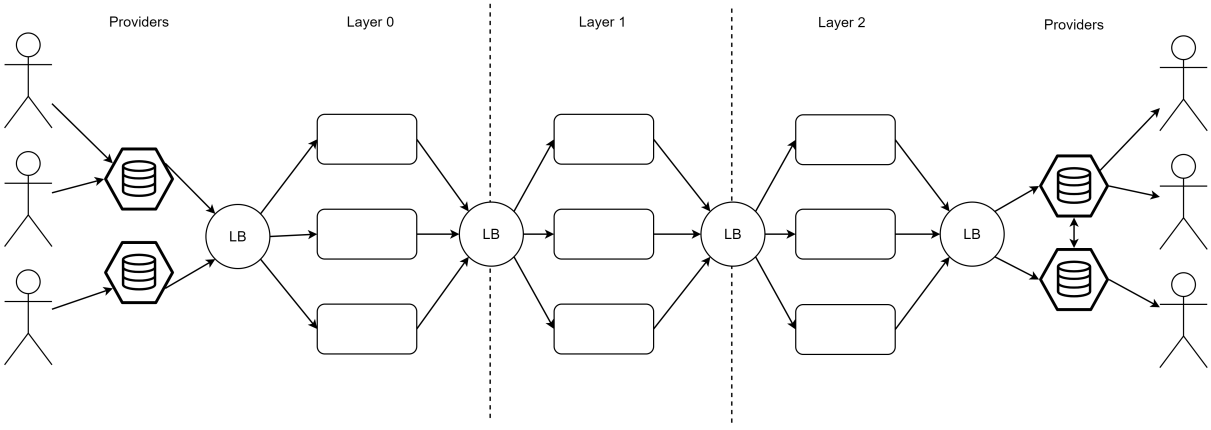


Figure 1: The topology of the Scalix mixnet

Our protocol is intended to fix those issues with the application of identity- and attribute-based cryptographic methods, maintaining the advantages of the Loopix protocol. The main idea, to achieve our goal is to share the number of layers in the mix networks (which is usually a small number), with their group ID, instead of every mix server's identity. With that, the senders can encrypt the required information for each layer (not for a specified mix server) and the load balancer's task to provide a more practical load balancing service than a random generator. Figure 1 shows the full topology of our

protocol, where the participants have the same task as in the Loopix. The main difference comes from the structure of the packet. We designed our packet format, meanwhile, Loopix uses the Sphinx packet.

To build a packet, the sender uses AES, secure identity-based encryption (IBE), and secure attribute-based encryption (ABE). First, he generates an AES key and he encrypts the message using that key. After that, the sender encrypts the AES key using IBE targeting the receiver's identity. Since the receiver's identity should only be known by its provider, the sender encrypts the receiver's identity with the IBE targeting its provider. As Figure 1 shows, there is a load balancer before the provider layer. This helps to hide the information from the mix servers, that they are in the last layer since they will do the same process as any other layer. Because of that any of the providers could receive the message and they will have to route it to the receiver's provider, so the sender will be required to encrypt the identity of the receiver's provider with ABE targeting the provider's layer group. Furthermore, our protocol is inheriting the same stop-and-go mixnet [3] delay mechanism used in the Loopix, so the sender has to generate the amount of delay for every layer the mix server is required to wait before it is allowed to forward the packet. Once all the delays are generated, he will encrypt each amount with ABE targeting the correct layer group. The final touch before the packet is ready to go is the encrypt with ABE the whole bunch of blocks targeting the first layer to give a uniform look to the packet, because once it is sent, the mix servers will decrypt the packet, gather the delay amount and encrypt it for the next layer. With that, they will all do the same operation. This only gives the idea of the packet; the full packet is also required to hold additional information to be verifiable about its correctness in every phase during its path.

Using the previous structure, the sender is easily able to create a reusable anonymous return channel, where the receiver will not find out his identity. It only requires to encrypt with IBE the AES key targeting his own and encrypt his identity targeting his provider. Also, encrypt with ABE his provider's identity targeting the provider layer group. After these, he will concatenate these blocks to the message and then he uses the AES key to encrypt this extended message. With the additional blocks, the receiver will be able to without knowing the sender's identity.

In conclusion, we were able to create a protocol, which supports high scalability and besides that provides similar security as the Loopix anonymity system.

References

[1] D. L. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". In: *Communications of the ACM* 24.2 (Feb. 1981), pp. 84–90. DOI: 10.1145/358549.358563. URL: https://doi.org/10.1145/358549.358563.

[2] G. Danezis and I. Goldberg. "Sphinx: A Compact and Provably Secure Mix Format". In: *2009 30th IEEE Symposium on Security and Privacy*. IEEE, May 2009. DOI: 10.1109/sp.2009.15. URL: https://doi.org/10.1109/sp.2009.15.

[3] D. Kesdogan, J. Egner, and R. Büschkes. "Stop- and- Go-MIXes Providing Probabilistic Anonymity in an Open System". In: *Information Hiding*. Springer Berlin Heidelberg, 1998, pp. 83–98. DOI: 10.1007/3-540-49380-8_7. URL: https://doi.org/10.1007/3-540-49380-8_7.

[4] A. M. Piotrowska et al. "The Loopix Anonymity System". In: *26th USENIX Security Symposium*. 2017, pp. 1199–1216. URL: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-piotrowska.pdf.

Scalable, password-based and threshold authentication for Smart Homes

Andrea Huszti, Szabolcs Kovács and Norbert Oláh
Faculty of Informatics, University of Debrecen, CCLab Ltd.
huszti.andrea@inf.unideb.hu, szabolcs.kovacs@cclab.com, olah.norbert@inf.unideb.hu

Introduction

Smart homes constitute a special field of the IoT paradigm, which is becoming more and more important in our lives. Sensors, devices and applications make our daily lives easier and collect our sensitive data, which may lead to security problems and incidents (e.g. hacked devices, botnets, etc.). In several cases devices lack proper security mechanisms. Therefore, security measures and the appropriate protections have become a central topic in the field of IoT. The most essential requirements include secure user-device authentication and confidentiality of the transferred sensitive data. Today, passwords are still the most widely used factors in certain areas, such as user authentication, key establishment, and secret sharing. An area of usage for passwords is the password-based protocols, which are resistant to most common threats, such as offline dictionary, man-in-the-middle and phishing attacks. The major aim of these solutions is to guarantee high level of security even if a user applies a single low-entropy human memorable password for all her/his accounts. Our goal is to propose a password-based multi-device authentication scheme for smart homes to reduce security vulnerabilities.

Our proposed protocol is designed typically for smart home environments. We assume that a typical smart home contains several IoT devices and at least one central node or edge. We reject the centralized authentication approach (e.g. Kerberos) and we propose a multi-device authentication. The central node or edge is called the *device manager*. If one or more devices break down or become compromised, the system will still be able to authenticate the user in a secure way. Hence, we thoroughly utilize the capabilities of these systems like *robustness* and *greater availability*. The scheme is an authenticated key exchange protocol with key confirmation (AKC) which takes advantage of the distributed IoT system. The client's password is shared among the smart home devices. Thus, several sensors and devices verify together the correctness of the user password. Attackers need to attack multiple devices simultaneously in order to impersonate a user successfully. Distributed storage of the passwords provides resistance against offline attacks as well. We accomplish the *password-only setting*, hence a user needs to know only a password. Since smart home devices (e.g. cameras) generate a lot of sensitive data, *confidentiality of data* needs to be ensured during the communication between the parties, and besides the identity verification of the user and the smart home a session key is also generated. Our scheme is designed to be an AKC between the user and the device manager. However, if the user would like to connect to an IoT device directly, the proposed protocol provides end-to-end security as well. Since there are resource constrained devices, we put a great emphasis on *efficiency* during the design. The session key is generated by Elliptic Curve Diffie-Hellman key exchange, moreover hash, MAC, xor operations and raising to a power are applied. We checked and compared the various properties of our proposed protocol (scalability, robust, passed, distributed authentication, etc.) with other suggestions in the scientific literature (e.g. [2, 3]) and these properties do not appear together in any of these suggestions.

The protocol consists of two phases: setup and authentication. During the setup phase a password is chosen by the user and split among the devices. Whenever the user logs in to the smart home system the authentication phase is run. The devices verify the password specified by the user. The number of devices in a smart home system is changing, therefore the proposed protocol is *scalable* in an efficient way. The password is not necessarily changed every time the number of devices is increased, hence the shares already set for the installed devices are not changed. For the newly registered devices new shares of the same password are set. To provide higher security level, during the authentication phase the user chooses a random value called *authentication value*, which is securely split among the devices. For the authentication value a threshold based on the number of devices, called *authentication threshold* is set. At least threshold number of devices are necessary to construct the authentication value from its shares. The authentication threshold is greater than or equal to the password threshold. A device calculates its authentication share with the help of its symmetric key based on its password share. Consequently, the smart home system authenticates the user successfully only if the authentication value is calculated, *i.e.* only if at least authentication threshold number of devices participate. Increasing the number of devices results in a larger authentication threshold, hence greater security level is achieved. Similarly, the number of devices can be decreased. Reregistration is required only if it goes below the threshold of the password secret sharing. The smart home is also authenticated and the user checks whether the devices are able to correctly calculate the password and the authentication value. Valid verification value is constructed

Preprint submitted to Central European Conference on Cryptology *April 18, 2021*

only if the devices possess valid password shares. Secret sharing algorithm and bilinear map are adopted to provide resistance against offline attacks. To construct the password at least threshold number of shares are necessary. Let l denote the password threshold and assume that $l-1$ devices are compromitted. With the knowledge of $l-1$ password shares the adversary can launch a dictionary attack. For each possible password the authentication value should be constructed from its shares for the verification. Besides the hash, these calculations are also required for each dictionary element that slows down the attack. We apply a bilinear map for storing the hash value of the password and the salt. A hash and a bilinear map calculation should be carried out together for each possible password that also slows down the attack.

Security analysis

Formal methods have been proved to be a good choice for uncovering flaws of incorrectly designed security protocols. There are many tools available that can analyse and identify attacks against protocols, such as Automated Validation of Internet Security Protocols and Applications (AVISPA) [1]. We have validated the security properties of the proposed protocol by using AVISPA. We formalize the protocol in HLPSL and also define the above security goals for the analysis. With the use of HLPSL correct protocol behavior described in the specification is achieved. This language is based on roles: basic roles for representing each participant role, and composition roles for representing scenarios of basic roles. Each role is independent from the others, getting some initial information by parameters, communicating with the other roles by channels. The intruder is modeled using the DolevYao model. AVISPA supports four types of goal predicates:witness (for weak authentication), request (for strong authentication), and secret. AVISPA also contains four different formal verification approaches (i.e. On-the-fly Model-Checker, Constraint-Logic-based Attack Searcher, SAT based Model-Checker and Tree Automata-based Protocol Analyser), which can formally validate security properties of a protocol.

Our main goal besides mutual authentication of participants is providing that at the end of the protocol the attacker is not able to gain any information about the exchanged new session key. After formalizing the protocol and the security goals, we apply the OFMC and CL-AtSe then execute the attacker simulation. The results of the security analysis show that the attacker is not able to impersonate the legal participants or get the session key. In AVISPA we can apply the secret, witness and request goal facts. We use these facts to demonstrate that our protocol is secure and we verify the m_0, h, SSK values in the AVISPA model . The secret is used to show that the session key (SSK) is secret and witness and request serve to prove authentication of participants (m_0, h). At the end, parties should be able to verify that the other party knows and is able to use the new session key. We also consider known-key security and forward secrecy properties. Known-key security preserves the security of session keys after disclosure of a session key. Disclosure of a session key should not jeopardize the security of other session keys. Forward secrecy holds if long-term secrets of one or more entities are compromised and the secrecy of previous session keys is not affected.

Appendix

```
role role_U(U:agent, DM:agent, D:agent, G:text,  H:hash_func, P:text,  Psw:text, Kab,Kac :symmetric_key,  SND,RCV:channel(dy))
played_by U
def=
        local
                State:nat,
                R1,R2 :text, %random
                W1,W2,C2, Secret :text, %authentication challenge
                X:text, Y:text, %session key parameter
                W:message,
                M1: hash(message),
                HE: hash(message.hash(message).message),
                SSK: hash(message),
                M3: hash(hash(message).message.message),
                Mac1: hash(symmetric_key.text),
                Mac2: hash(symmetric_key.text.message)
        init
                State := 0
        transition
                1. State=0 ∧ RCV(start)   =|>
                   State':=2 ∧  R1':=new() ∧  R2':= new() ∧ X':=new() ∧ W1':=new() ∧ W2':=new() ∧
                             Mac1':= H(Kac.R1') ∧ Mac2':= H(Kab.R2'.exp(G,X')) ∧
                             W' := exp(exp(exp(P,Psw),W1'),W2') ∧
                             M1' :=H(W') ∧
                             SND(xor(Mac2',W2').R2'.exp(G,X').H(W')) ∧   SND(xor(Mac1',W1').R1') ∧
                             witness(U,DM, user_dm_w, W')
                5. State=2   ∧ RCV(exp(G,Y')) =|>
                   State':=7 ∧  SSK' := H(exp(exp(G,Y'),X))
                6. State=7  ∧ RCV(HE') ∧ H(W.SSK.exp(G,Y))=HE' =|>
                   State':= 9 ∧ Secret':=new() ∧  M3':=H(SSK.exp(G,Y).exp(G,X)) ∧
                                secret(Secret',sec_1,{U,DM})  ∧ SND(M3'.{Secret'}_SSK) ∧ request(U,DM, user_dm_SSK, SSK)
end role
```

Figure 1: HLPSL specification of user's role

References

[1] A. Armando, Basin D, Boichut Y, Chevalier Y, Compagna L, Cullar J, Drielsma PH, Ham PC, Kouchnarenko O, Mantovani J, et al. *The avispa tool for the automated validation of internet security protocols and applications.* International conference on computer aided verification (Springer), , pp 281285. (2005)

[2] Işler, D., & Küpçü, A. *Distributed Single Password Protocol Framework.* IACR Cryptol. ePrint Arch., 2018, 976.

[3] Rathore, M. Mazhar; BENTAFAT, Elmahdi; BAKIRAS, Spiridon. *Smart Home Security: A Distributed Identity-Based Security Protocol for Authentication and Key Exchange.* In: 2019 28th International Conference on Computer Communication and Networks (ICCCN). IEEE, pp. 1-9., 2019.

Probability of double spend attack for network with non-zero synchronization time

Lyudmila Kovalchuk[1,2], Mariia Rodinko[1,3], Roman Oliynykov[1,3], Dmytro Kaidalov[1], and Andrii Nastenko[1]

[1]Input Output HK
[2]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
[3]V.N. Karazin Kharkiv National University

Introduction. In this paper, we obtained for the first time mathematically substantiated formulas for probability of a double spend attack on blockchain that is based upon Proof-of-Work consensus protocol and longest chain rule, for a network with a non-zero time of block propagation in the model with continuous time. Also, for the first time, it was shown that probability of such attack depends on the value equal to the product of the block propagation time and of the block generation intensity. The larger is this value, the larger is the attack success probability. Formulas obtained allow not only calculating of the attack success probability at various network parameters, but also to determine the number of confirmation blocks allowing reduction of the attack probability below some given small threshold, e.g. 10^{-3}.

Related work. The idea of the double spend attack appeared at the same time when the idea of the blockchain itself – for the first time this attack was described in the paper by Nakamoto [4]. The same paper proposed a method to withstand such attack, namely, generation of a certain number of confirmation blocks. Probability of the attack success was also calculated, depending on the network parameters and the number of confirmation blocks. Unfortunately, these calculations were made with serious probabilistic mistakes, one of which was replacement of a random variable by its mathematical expectation. As a result of this and other mistakes, the attack success probability appeared to be significantly underestimated.

In the papers [6, 5] and in some others, the authors also pointed out that the attack probability in the Nakamoto paper was underestimated, but failed to propose any alternative options having comprehensive mathematical substantiation. The paper [2] became the first where probability attack formulas were strictly proved. However, this paper also had certain drawbacks related not to strictness of presentation but to the model itself in the framework of which the results were obtained. The authors considered a simplified model of the network operation at assumption that the block delivery time is zero. Note that even at this simplifying assumption proofs of the obtained results appeared to be quite cumbersome.

The paper [1] presents estimation of the security threshold for the Bitcoin protocol in the model with discrete time, taking into account network delays.

The paper [3] was the first on to state how exactly the block propagation time affects security of the consensus protocol against the double spend attack. In particular, one of results of this paper were formulas for calculation of the security threshold — the minimal ratio of an adversary allowing completion of such attack with probability 1. Note that the larger the block propagation time in the network, the larger the security threshold differs (downward) from 50%.

This paper is a logical continuation of the paper [3]. We obtained strictly substantiated formulas for attack probability calculation that allowed not only explicit obtaining of attack success probability, but also calculating the number of confirmation blocks would be sufficient to ensure security against such attack. Using obtained analytical expressions for attack probability, we obtained the relevant numerical results that also appeared to be quite interesting.

Main results. Further we need the following notations. Let p_H, p_M be the hashrates of honest and malicious miners (full nodes), respectively, $p_H + p_M = 1$. Also define D_H block delivery time for honest miners (here we make an assumption to the benefit of a malicious miner, and consider that such malicious miner is well-synchronized). Then define α_H, α_M as block generation intensities (average numbers of blocks per second, generated by honest and malicious miner, respectively) for honest

and malicious miners, $\alpha = \alpha_H + \alpha_M$. In these designations block creation times have exponential distributions with parameters α_H, α_M respectively. Also define values

$$p'_M = 1 - e^{-\alpha_M D_H} \cdot p_H;\ p'_H = e^{-\alpha_M D_H} \cdot p_H.$$

Next, define an auxiliary value

$$P_z(k) = \frac{p_H^n}{(z-1)!} \cdot \frac{e^{-\alpha_M z D_H} \cdot (\alpha_M z D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(z-i+1)! \cdot C_k^i}{(\alpha z D_H)^i}, \text{for } z \in \mathbb{N}.$$

Theorem 1: the success probability of double spend attack after confirmation blocks is

$$P(z) = \begin{cases} 1, & \text{if } p'_M \geq p'_H; \\ 1 - \sum_{k=0}^{z} P_z(k) \left(1 - \left(\frac{p'_M}{p'_H}\right)^{z-k}\right), & \text{else.} \end{cases}$$

Calculation results. Table 1 presents the results obtained using Theorem 1. We calculate the minimal number z of confirmation blocks sufficient to make probability of success less than 10^{-3}.

Table 1: The results for $\alpha = 0.00167\ \text{sec}^{-1}$ (as for BTC) and various values of the block delivery times (measured in seconds) and malicious hashrate, and results from Nakamoto article [4], for comparison

p_H	$D_H = 0$ (Nakamoto)	$D_H = 15$	$D_H = 30$	$D_H = 60$	$D_H = 120$	$D_H = 180$
	z					
0.1	6 (5)	6	6	6	7	7
0.15	9 (8)	9	9	9	10	11
0.2	13 (11)	13	14	14	16	17
0.25	20 (15)	20	21	22	26	30
0.3	32 (24)	33	35	39	48	61
0.35	58 (41)	62	67	78	111	176
0.4	133 (89)	150	170	224	515	$P_{success} = 1$

Conclusion. The results obtained show that probability of the double spend attack increases with growth of the block delivery time and intensity of block generation. The larger the block delivery time, the larger the number of confirmation blocks to prevent the attack. Moreover, if the block delivery time is sufficiently large, then the attack probability will be 1 irrespective of the number of confirmation blocks, even when attackers are in the minority, as e.g. in the right lower cell of Table 1.

References

[1] Peter Gaži, Aggelos Kiayias, and Alexander Russell. Tight consistency bounds for bitcoin. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 819–838, 2020.

[2] Cyril Grunspan and Ricardo Pérez-Marco. Double spend races. *International Journal of Theoretical and Applied Finance*, 21(08):1850053, 2018.

[3] Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenko, Mariia Rodinko, Oleksiy Shevtsov, and Roman Oliynykov. Decreasing security threshold against double spend attack in networks with slow synchronization. *Computer Communications*, 154:75–81, 2020.

[4] Satoshi Nakamoto. A peer-to-peer electronic cash system. 2008.

[5] Carlos Pinzón and Camilo Rocha. Double-spend attack models with time advantange for bitcoin. *Electronic Notes in Theoretical Computer Science*, 329:79–103, 2016.

[6] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

Entropoid Based Cryptography

Danilo Gligoroski*

April 12, 2021

Abstract

The algebraic structures that are non-commutative and non-associative known as entropic groupoids that satisfy the *"Palintropic"* property i.e., $x^{\mathbf{AB}} = (x^{\mathbf{A}})^{\mathbf{B}} = (x^{\mathbf{B}})^{\mathbf{A}} = x^{\mathbf{BA}}$ were proposed by Etherington in '40s from the 20th century. Those relations are exactly the Diffie-Hellman key exchange protocol relations used with groups. The arithmetic for non-associative power indices known as Logarithmetic was also proposed by Etherington and later developed by others in the 50s-70s. However, as far as we know, no one has ever proposed a succinct notation for exponentially large non-associative power indices that will have the property of fast exponentiation similarly as the fast exponentiation is achieved with ordinary arithmetic via the consecutive rising to the powers of two.

In this paper, we define ringoid algebraic structures $(G, \boxplus, *)$ where $(G, \boxplus)$ is an Abelian group and $(G, *)$ is a non-commutative and non-associative groupoid with an entropic and palintropic subgroupoid which is a quasigroup, and we name those structures as Entropoids. We further define succinct notation for non-associative bracketing patterns and propose algorithms for fast exponentiation with those patterns.

Next, by an analogy with the developed cryptographic theory of discrete logarithm problems, we define several hard problems in Entropoid based cryptography, such as Discrete Entropoid Logarithm Problem (DELP), Computational Entropoid Diffie-Hellman problem (CEDHP), and Decisional Entropoid Diffie-Hellman Problem (DEDHP). We post a conjecture that DEDHP is hard in Sylow q-subquasigroups. Next, we instantiate an entropoid Diffie-Hellman key exchange protocol. Due to the non-commutativity and non-associativity, the entropoid based cryptographic primitives are supposed to be resistant to quantum algorithms. At the same time, due to the proposed succinct notation for the power indices, the communication overhead in the entropoid based Diffie-Hellman key exchange is very low: for 128 bits of security, 64 bytes in total are communicated in both directions, and for 256 bits of security, 128 bytes in total are communicated in both directions.

Our final contribution is in proposing two entropoid based digital signature schemes. The schemes are constructed with the Fiat-Shamir transformation of an identification scheme which security relies on a new hardness assumption: computing roots in finite entropoids is hard. If this assumption withstands the time's test, the first proposed signature scheme has excellent properties: for the classical security levels between 128 and 256 bits, the public and private key sizes are between 32 and 64, and the signature sizes are between 64 and 128 bytes. The second signature scheme reduces the finding of the roots in finite entropoids to computing discrete entropoid logarithms. In our opinion, this is a safer but more conservative design, and it pays the price in doubling the key sizes and the signature sizes.

We give a proof-of-concept implementation in SageMath 9.2 for all proposed algorithms and schemes in an appendix.

Keywords: Post-quantum cryptography, Discrete Logarithm Problem, Diffie-Hellman key exchange, entropic, Entropoid, Entropoid Based Cryptography

*Department of Information Security and Communication Technologies, Norwegian University of Science and Technology - NTNU

Linear Algebraic Public Key Encryption Scheme

Gábor Harangozó, Hungary
harangozo.gabor.dr@gmail.com

Abstract A new linear algebraic public key encryption scheme is introduced for post-quantum cryptography. The mathematical problem behind the encryption algorithm is based on matrix factorization and the solution of a linear system of matrix equations including singular matrices as coefficients.

Keywords: post-quantum cryptography, linear algebraic equations, singular matrices, matrix factorization

1. Introduction

Nowadays the most common public key encryption algorithms, like the RSA (Rivest–Shamir–Adleman) algorithm, or the EEC (elliptic-curve cryptography) algorithm, belong to those cryptographic schemes which can be broken using a sufficiently powerful future quantum computer within reasonable time. The security of these algorithms relies on hard mathematical problems, like the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem, which can be solved on a powerful quantum computer running Shor's algorithm within polynomial time duration. Therefore new algorithms are needed that are substantially secure against the quantum computers. The candidate quantum-resistant encryption algorithms should be based on a mathematical problem, the solution of which has a computational complexity of at least NP-complete. Such a mathematical problem is, among others, the exact nonnegative matrix factorization (NMF), the computational complexity of which is proved to be NP-hard [1]. Various attempts have been previously made to use NMF in public key cryptography, however, most of them applied approximate NMF for decryption [2]. Furthermore, a quantum algorithm has been recently published by Du at al. [3] for solving separable NMF (SNMF) under a logarithmic runtime. However, no sub-exponential algorithm is currently known for general exact NMF.

2.1. Concept of the algorithm

In the proposed encryption algorithm, the plaintext message is represented by a square matrix and the ciphertext message is represented by multiple square matrices. The matrix entries are defined over a finite field F_q, where $q = 2^m$. The ciphertext message is produced using multiple linearly independent linear algebraic equations, in which the variables include the encoded plaintext message and random error components, which are also nxn square matrices. Due to the random error components, the encryption algorithm is probabilistic.

In the linear equations, the random error components are multiplied, at least on their one side, with a respective singular matrix, where the singular matrices themselves are defined as the product of an nxr matrix and an rxn matrix, where r<n. The equation system formed of these linearly independent matrix equations can be solved only through multiplicative decomposition of the singular coefficient matrices into the specific matrix factors. The matrix coefficients of the equation system together form the public key, whereas a specific set of matrices defined using the multiplicative matrix factors of the public key matrices will form the private key.

2.2. Encryption

The ciphered message is computed using the following linear algebraic equations:

$$K_1E_1K_2 + K_3E_2 = Y_1 \qquad \text{(Eq. 1)}$$

$$K_4E_1K_5 + K_6E_2 = Y_2 \qquad \text{(Eq. 2)}$$

$$K_7E_1K_8 + K_9E_2 + M = Y_3 \qquad \text{(Eq. 3)}$$

where M is an nxn matrix representing the plaintext message, E_1 and E_2 are arbitrary nxn random error matrices, K_i are nxn singular matrices, and Y_1, Y_2 and Y_3 are nxn code matrices which together form the ciphered message. The public key matrices K_i are defined as follows:

$$K_1=FT;\ K_2=QA;\ K_3=CR;\ K_4=HT;\ K_5=K_2=QA;\ K_6=DR;\ K_7=JT;\ K_8=QB;\ K_9=GR,$$

where A, B, R and T are arbitrary full-ranked rxn matrices, C, D, F, G, H, J and Q are arbitrary full-ranked nxr matrices, where r<n, A≠ B, and C, D and G are mutually different matrices. Each of the matrices A, B, C, D, F, G, H, J, Q, R and T, which define the public key matrices K_i, should be kept in secret. Additionally, the random error matrices E_1, E_2 are also to be kept in secret by the ciphering party.

From the above definitions of the public key matrices K_i, it is clear that since each of K_i is a singular matrix, the linear equation system cannot be solved using the matrices K_i themselves for determining either the plaintext message matrix M or the random error matrices E_1, E_2.

2.3. Decryption

To determine the plaintext message matrix M from the above equation system, the following steps are to be taken:

a) Let us express the matrix product RE_2 from Eq. 1 as a function of the code matrix Y_1 and the matrix product TE_1Q, i.e. $RE_2 = f_1(Y_1, TE_1Q)$, where C^{-1} is the Moore-Penrose pseudoinverse of C:

$$RE_2 = C^{-1}(Y_1 - FTE_1QA)$$

b) Let us express the matrix product TE_1Q from Eq. 2 as a function of code matrices Y_1 and Y_2, i.e. $TE_1Q = f_2(Y_1, Y_2)$, where A^{-1} is the Moore-Penrose pseudoinverse of A:

$$TE_1Q = (H - DC^{-1}F)^{-1}Y_2A^{-1} - (H - DC^{-1}F)^{-1}DC^{-1}Y_1A^{-1}$$

c) By using the expression of step b) for the matrix product TE_1Q and combining Eq. 1 with Eq. 3, we can express matrix M as a function of the three code matrices Y_1, Y_2 and Y_3, i.e. $M = f_3(Y_1, Y_2, Y_3)$, where $P = (H - DC^{-1}F)$, P is an nxr matrix and is assumed to be full-ranked, P^{-1} is the Moore-Penrose pseudoinverse of P, and I is an nxn identity matrix:

$$M = JP^{-1}DC^{-1}Y_1A^{-1}B - GC^{-1}(I + FP^{-1}DC^{-1})Y_1 - JP^{-1}Y_2A^{-1}B + GC^{-1}FP^{-1}Y_2 + Y_3$$

If P turns out to be rank-deficient, any one or more of C, D, F and H should be changed so that P be full-ranked.

By introducing the following definitions:

$$S_1 = JP^{-1}DC^{-1};\ S_2 = A^{-1}B;\ \ S_3 = GC^{-1}(I + FP^{-1}DC^{-1});\ \ S_4 = JP^{-1};\ S_5 = A^{-1}B;\ \ S_6 = GC^{-1}FP^{-1}$$

the plaintext message matrix M can be expressed as

$$M = S_1Y_1S_2 - S_3Y_1 - S_4Y_2S_5 + S_6Y_2 + Y_3$$

The above defined matrices S_i are nxn square matrices, and they will together form the private key.

2.4. Security considerations

One possible attack against the present encryption scheme is where the attacker attempts to determine the private key matrices on the basis of the public key matrices. As it can be seen from the definition of the public key matrices K_i, the matrices A, B, C, D, F, G, H and J should be determined by the attacker to compute the private key matrices S_i. However, factorization of the public key matrices K_i into the product of two specific matrices is a hard mathematical problem. According to Moitra [4], the best NMF algorithm known runs in time $O\,(2^r mn)^{O(r^2)}$. The security of the present algorithm against chosen plaintext attacks (CPA) and chosen ciphertext attacks (CCA) has not been deeply analysed yet, but preliminary researches show that with appropriate parameter settings, the algorithm will likely be IND-CPA and IND-CCA2 secure.

3. Conclusion

The proposed encryption scheme is very robust and easy to implement, and it involves a high degree of randomness and great freedom for the selection of the public key matrix factors. Once its security has been justified by the crypto society, it may become a candidate algorithm for post-quantum cryptography.

References

[1] Stephen A. Vavasis, *On the complexity of nonnegative matrix factorization,* SIAM Journal on Optimization, Volume 20, Issue 3, August 2009, pp. 1364-1377.

[2] Shengli Xie et al., *Nonnegative Matrix Factorization Applied to Nonlinear Speech and Image Cryptosystems*, IEEE Transactions on Circuits and Systems, I: Regular Papers, Vol. 55., No. 8, September 2008, pp. 2356-2367.

[3] Yuxuan Du et al., *Quantum Divide-and-Conquer Anchoring for Separable Non-negative Matrix Factorization,* Proc. of the 27th International Joint Conference on Artificial Intelligence (IJCAI-18), 2018, pp. 2093-2099.

[4] A. Moitra, *An almost optimal algorithm for computing nonnegative rank*, Proceedings of SODA, 2013, pp. 1454–1464.

A new secure encryption scheme based on the automorphism group of the Ree function field

Gennady Khalimov[(1)] Yevgeniy Kotukh[(2)] *Svitlana Khalimova*[(1)]

[(1)]*Kharkiv National University of Radioelectronics*Kharkiv, Ukraine
[(2)]*Sumy State University*Sumy, Ukraine

Abstract. *The article describes a new encryption implementation based on the MST cryptosystem for the group of automorphisms of the Ree functional field. The main difference from the known one is the use of homomorphic encryption to construct coverings of logarithmic signatures for all parameters of the group. In this case, the secrecy of the cryptosystem is ensured at the level of a brute-force attack.*

Keywords: *MST cryptosystem, logarithmic signature, random cover, automorphism group, Ree function field.*

I. INTRODUCTION

Classical public key cryptosystems use the idea of the complexity of solving the problem of factorizing large numbers. This idea became insecure with the implementation of quantum algorithms. Since the early 2000s, several dozen cryptosystem schemes have been proposed that are resistant to quantum cryptanalysis. One of them is the MST cryptosystem based on factorization in finite groups of permutations, called the logarithmic signature [1]. In 2009 Lempken et al. [2] proposed a public key cryptographic system - MST3, based on random covers and Suzuki's 2-group. In 2010, Swaba et al. [3] analyzed all published references to attacks on MST cryptography and built a more secure eMST3 cryptosystem by adding a secret homomorphic coverage. The construction of MST cryptosystems based on multiparameter non-commutative groups was proposed in [4,5].

The automorphism group of the functional field Ree is four-parameter and has the largest group order in comparison with other multi-parameter groups. The first implementation of the cryptosystem on the group of automorphisms of the functional field Ree is presented in [5] and does not provide protection against attacks with key recovery using the brute force method. Analysis of MCT cryptosystems by group shows their vulnerability to selected text attacks. The design feature of all known MST implementations is the presence of known texts and, as a consequence, the possibility of such cryptanalysis. A new secure encryption scheme is proposed based on the use of homomorphic encryption to construct coverings of logarithmic signatures for all group parameters.

II. PROPOSAL

The group of automorphisms of the Ree function field $A(P_\infty)$ is defined over a finite field F_q, $q=3^{2s+1}$, where $s\in N\setminus\{0\}$ and $q_0=3^s$ [10]. The each element of $A(P_\infty)$ can be expressed uniquely $A(P_\infty)=\left\{S(a,b,c,d)\middle| a\in F_q^*:=F_q\setminus\{0\}, c,b,d\in F_q\right\}$ and group operation is defined as

$$S(a_1,b_1,c_1,d_1)\cdot S(a_2,b_2,c_2,d_2)=S\left(\ a_1a_2, a_2b_1+b_2, a_2^{q_0+1}c_1+a_2b_1b_2^{q_0}+c_2, a_2b_1b_2^{2q_0}-a_2^{q_0+1}b_2^{q_0}c_1+a_2^{2q_0+1}d_1+d_2\ \right)$$

The identity is the 4-triple $[1,0,0,0]$ and the inverse of $S(a,b,c,d)$ is

$$S(a,b,c,d)^{-1}=S\left(\ a^{-1},-a^{-1}b,\left(a^{-1}b\right)^{q_0+1}-a^{-(q_0+1)}c,-\left(a^{-1}b\right)^{2q_0+1}-a^{-(2q_0+1)}b^{q_0}c-a^{-(2q_0+1)}d\ \right).$$

In the new implementation of the cryptosystem, we changed the encryption algorithm to bind the keys of logarithmic signatures, to protect against sequential recovery attacks and attacks with chosen text. Our suggestion is to use homomorphic encryption for random covers. In this case, the complexity of the key recovery attack will be determined by exhaustive search over the entire group of automorphisms.

Description of the Scheme. Key Generation.

Input: a large group on the field F_q, $q=3q_0^{\,2}$, $q_0=3^s$, $A(P_\infty)=\left\{S(a,b,c,d)\middle| a\in F_q^*:=F_q\setminus\{0\}, c,b,d\in F_q\right\}$.

Choose a tame logarithmic signatures $\beta_{(k)}=\left(b_{ij}\right)_{(k)}$, $\left(b_{ij}\right)_{(k)}\in A(P_\infty)$ of type $\left(r_{1(k)},...,r_{s(k)}\right)$, $i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$, $k=\overline{1,3}$. Group element $\left(b_{ij}\right)_{(k)}$ has a value in only one coordinates b, c or d. For example $\left(b_{ij}\right)_{(1)}=S\left(1,b_{ij(1)_a},0,0\right)$.

Select a random covers $\alpha_{(k)}=\left(a_{ij}\right)_{(k)}=S\left(a_{ij(k)_a},a_{ij(k)_b},a_{ij(k)_c},a_{ij(k)_d}\right)$, $w_{(k)}=\left(w_{ij}\right)_{(k)}=S\left(1,w_{ij(k)_b},w_{ij(k)_c},w_{ij(k)_d}\right)$ of the same types as $\beta_{(k)}$, where $a_{ij},w_{ij}\in A(P_\infty)$, $a_{ij(k)},w_{ij(k)}\in F_q\setminus\{0\}$, $i=\overline{0,s(k)}$, $j=\overline{1,r_{i(k)}}$, $k=\overline{1,3}$.

Choose $t_{i(k)}=S\left(t_{i(k)_a},t_{i(k)_b},t_{i(k)_c},t_{i(k)_d}\right)$, $\tau_{i(k)}=S\left(\tau_{i(k)_a},\tau_{i(k)_b},\tau_{i(k)_c},\tau_{i(k)_d}\right)$, where $t_{i(k)},\tau_{i(k)}\in A(P_\infty)\setminus Z$, $i=\overline{0,s(k)}$, $k=\overline{1,3}$. $t_{i(k)_\beta},\tau_{i(k)_\gamma}\in F_q/\{0\}$. Let's $t_{s(k-1)}=t_{0(k)}$, $\tau_{s(k-1)}=\tau_{0(k)}$. Let's define an additional group operation

$$S(a_1,b_1,c_1,d_1)\circ S(a_2,b_2,c_2,d_2)=S\left(\ a_1a_2,a_2b_1+b_2,a_2^{q_0+1}c_1+c_2,+a_2^{2q_0+1}d_1+d_2\ \right).$$

The inverse element is $\overline{S}(a,b,c,d)^{-1} = S(\ a^{-1}, -a^{-1}b, -a^{-(q_0+1)}c, -a^{-(2q_0+1)}d\ )$. Let $f(a)$ be a homomorphic cryptographic transformation with respect to addition $f(a+b) = f(a) + f(b)$, $a,b \in F_q$ and the corresponding inverse transformation $\hat{f}(a) = a$. We calculate the covering of the logarithmic signatures

$\gamma_{(1)} = \left[h_{1(1)},...,h_{s(1)}\right] = t_{(i-1)(1)}^{-1} \cdot \left(w_{ij}\right)_{(1)} \cdot \left(b_{ij}\right)_{(1)} \cdot t_{i(1)}$, $\gamma_{(k)} = \left[h_{1(k)},...,h_{s(k)}\right] = \overline{t}_{(i-1)(k)}^{-1} \circ \left(w_{ij}\right)_{(k)} \circ \left(b_{ij}\right)_{(k)} \circ t_{i(k)}$,

$\lambda_{(1)} = \left[g_{1(1)},...,g_{s(1)}\right] = \tau_{(i-1)(1)}^{-1} \cdot f\left(w_{ij}\right)_{(1)} \cdot \tau_{i(1)}$, $\lambda_{(k)} = \left[g_{1(k)},...,g_{s(k)}\right] = \overline{\tau}_{(i-1)(k)}^{-1} \circ f\left(w_{ij}\right)_{(k)} \circ \tau_{i(k)}$,

$f(w_{(k)}) = f\left(w_{ij}\right)_{(k)} = S\left(1, f(w_{ij(k)_b}), f(w_{ij(k)_c}), f(w_{ij(k)_d})\right)$, $i = \overline{1,s(k)}$, $j = \overline{1,r_{i(k)}}$, $k = 2,3$.

An output public key $(\alpha_k, \gamma_k, \lambda_k)$, and a private key $\left[\beta_{(k)}, \left(t_{0(k)},...,t_{s(k)}\right), \left(\tau_{0(k)},...,\tau_{s(k)}\right)\right]$, $k = \overline{1,3}$.

Encryption *Input*: a message, $m = S(m_1, m_2, m_3, m_4)$, $m_1 \in F_q \setminus \{0\}$, and the public key $(\alpha_k, \gamma_k, \lambda_k)$, $k = \overline{1,3}$.

Choose a random $R = (R_1, R_2, R_3)$, $R_k \in Z_{|Z|}$, $k = \overline{1,3}$. Compute the ciphertext y_1, y_2, y_3

$y_1 = \alpha'(R) \cdot m = \alpha_1(R_1) \cdot \alpha_2(R_2) \cdot \alpha_3(R_3) \cdot m$, $y_2 = \gamma_1'(R_1) \cdot \left(\gamma_2'(R_2) \circ \gamma_3'(R_3)\right)$, $y_3 = \lambda_1'(R_1) \cdot \left(\lambda_2'(R_2) \circ \lambda_3'(R_3)\right)$.

Decryption *Input*: a ciphertext (y_1, y_2, y_3) and private key $\left[\beta_{(k)}, \left(t_{0(k)},...,t_{s(k)}\right), \left(\tau_{0(k)},...,\tau_{s(k)}\right)\right]$, $k = \overline{1,3}$.

To decrypt a message m, we need to restore random numbers $R = (R_1, R_2, R_3)$.

Compute $D(R) = t_{0(1)} y_2 \circ \overline{t}_{s(3)}^{-1}$, $G(R) = \tau_{0(1)} y_3 \circ \overline{\tau}_{s(3)}^{-1}$, $D(R)' = D(R) \cdot \hat{f}(G(R)_b)^{-1} = S(1, \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)_b}, *, *)$

Restore R_1 with $\beta_{(1)}(R_1) = \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)_b}$ using $\beta_{(1)}(R_1)^{-1}$, because β_1 is simple. For further calculation, it is necessary to remove the component $\gamma_1'(R_1)$ from y_2 and $\lambda_1'(R_1)$ from y_3.

Compute $y_2^{(1)} = \gamma_1'(R_1)^{-1} \cdot y_2$, $y_3^{(1)} = \lambda_1'(R_1)^{-1} \cdot y_3$, $D(R)^{(1)} = t_{0(2)} \circ y_2^{(1)} \circ \overline{t}_{s(3)}^{-1}$, $G(R)^{(1)} = \tau_{0(2)} \circ y_3^{(1)} \circ \overline{\tau}_{s(3)}^{-1}$,

$D(R)'' = D(R)^{(1)} \circ \hat{f}(G(R)_c)^{-1} = S(1, *, \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)_c}, *)$ and restore R_2 with $\beta_{(2)}(R_2) = \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(1)_c}$ using $\beta_{(2)}(R_2)^{-1}$, because β_1 is simple. Remove the component $\gamma_2'(R_2)$ from $y_2^{(1)}$ and $\lambda_2'(R_2)$ from $y_3^{(1)}$.

As a result, we get $D(R)''' = D(R)^{(2)} \circ \hat{f}(G(R)_d)^{-1} = S(1, *, *, \sum_{i=1, j=R_{i(3)}}^{s(3)} \beta_{ij(3)_d})$, restore R_3 with $\beta_{(3)}(R_3)$ using $\beta_{(3)}(R_3)^{-1}$ and recovery the message $m = \alpha'(R_1', R_2', R_3')^{-1} \cdot y_1$.

Security Analysis All classic attacks on the MST cryptosystem work with the ability to analyze ciphertexts from known texts. In all previous implementations, an array of logarithmic signatures was generated from a randomly selected but known coverage $\left(a_{ij}\right)_{(k)}$. In this implementation, all $\gamma_{(k)}, \lambda_{(k)}$ elements do not have this dependency. Therefore, one can only rely on a brute-force attack with complexity q^3.

III. CONCLUSIONS

The new cryptosystem MST, based on the non-commutative automorphism group Ree of a functional field with homomorphic encryption, fully implements the concept of constructing cryptosystems with an intractable word problem. The ciphertext components have no known texts, and the associated keys are protected against sequential recovery attacks using logarithmic signatures.

REFERENCES

[1] S. S. Magliveras, "A cryptosystem from logarithmic signatures of finite groups," in Proceedings of the 29th Midwest Symposium on Circuits and Systems , pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.

[2] W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei, "A public key cryptosystem based on non-abelian finite groups", J. of Cryptology, 22 (2009), 62–74.

[3] P. Svaba and T. van Trung, "Public key cryptosystem MST3 cryptanalysis and realization", Journal of Mathematical Cryptology,vol.4,no.3,pp.271–315,2010.

[4] G. Khalimov, Y. Kotukh, S.Khalimova "MST3 cryptosystem based on the automorphism group of the hermitian function field" // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, pp. 865–868.

[5] G. Khalimov, Y. Kotukh, S.Khalimova "Encryption scheme based on the automorphism group of the Ree function field" 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192

Using GeMSS in a Multivariate Ring Signature Scheme

Viliam Hromada *

Slovak University of Technology in Bratislava, Slovakia
viliam.hromada@stuba.sk

In today's world, there is a need for quantum-secure multiple-users cryptographic primitives. For example, the post-quantum authenticated group key establishment [1], which enables more than two participants to agree on a shared high-entropy secret key, whilst the process is quantum-secure. Other multiple-users-scenarios include the ring signature schemes.

A ring signature scheme is a signature scheme where a user can sign messages anonymously as a member of some group $\mathcal{R}$. The verifier can verify, whether a signature was generated by a member of the group $\mathcal{R}$, but cannot reveal the identity of the signer. In 2017, Mohamed and Petzold proposed a simple multivariate ring signature scheme [2], which allows the participants to use an arbitrary multivariate signature scheme as a building block. Currently, there are two promising multivariate signature schemes in the NIST Post-Quantum Cryptography Competition: Rainbow [4] and GeMSS [3].

In the ring signature scheme proposed in [2], each member of the group $\mathcal{R}$ generates an instance of a private and a public key of some multivariate signature scheme. The original proposal of [2] uses the scheme Rainbow as the building block. In our work, we investigate the possibility of using GeMSS [3] as the main building block. A similar work has been already done in [5]. However, the mentioned paper only suggests the usage of GeMSS and omits any performance results or the proposal of parameter values to achieve desired levels of security. We present the proposed parameters for using GeMSS in a ring signature scheme [2] based on the number of members of the group $\mathcal{R}$ and we also give the performance results.

In the scheme [2], the resulting public key, which is used to verify the ring signature, is a concatenation of all public keys of all users. Therefore the number of polynomials and indeterminates in the resulting public key changes according to the number of members of the group $\mathcal{R}$. This affects the overall level of security, therefore the parameters of GeMSS change not only with the desired level of security, but also with the number of members of the group $\mathcal{R}$. Here, we present the proposed parameters for 128-bit level of security for GeMSS and measured average signature and verification time in milliseconds. Times were measured on a notebook with Intel Core i7-3630QM @ 2.40Ghz with 8GM RAM running Ubuntu 18.04.01, gcc version 7.5.0. The scheme was built upon the optimized implementation of GeMSS available in the NIST PQC Competition. In table 1, k represents the number of members of group $\mathcal{R}$ ($k = 1$ means the default instance of GeMSS). Without going into too much detail in this abstract, n, Δ, v practically influence the resulting public key in each instance so that it has $n - \Delta$ polynomials and $n + v$ indeterminates.

128-bit security	$k = 1$	$k = 5$	$k = 10$	$k = 20$	$k = 50$
Parameters (n, Δ, v)	(174,12,12)	(178,12,12)	(184,12,12)	(194,11,11)	(227,11,11)
Public Key Size [kB]	352	1 883	4 151	9 661	39 397
Signature Size [b]	264	1 320	2 720	5 440	15 200
Signature generation [ms]	759	792	940	1 523	1 752
Signature verification [ms]	0.16	0.78	1.40	3.04	9.20

Table 1: Proposed parameters for GeMSS in ring signature scheme for 128-bit security

The full version of the paper will contain parameter estimation for 128,192,256-bit levels of security, as well as performance measurements.

*This project is supported by NATO Science for Peace and Security Programme under Grant G5448

References

[1] GONZÁLEZ VASCO, María Isabel; PÉREZ DEL POZO, Ángel L.; STEINWANDT, Rainer. Group Key Establishment in a Quantum-Future Scenario. Informatica, 2020, 31.4: 751-768.

[2] MOHAMED, Mohamed Saied Emam; PETZOLDT, Albrecht. RingRainbow–an efficient multivariate ring signature scheme. In: International Conference on Cryptology in Africa. Springer, Cham, 2017. p. 3-20.

[3] CASANOVA, Antoine, et al. GeMSS: a great multivariate short signature. 2017. PhD Thesis. UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France; LIP6-Laboratoire d'Informatique de Paris 6.

[4] DING, Jintai; SCHMIDT, Dieter. Rainbow, a new multivariable polynomial signature scheme. In: International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2005. p. 164-175.

[5] DEMIRCIOGLU, Murat; AKLEYLEK, Sedat; CENK, Murat. Efficient GeMSS Based Ring Signature Scheme. Malaysian Journal of Computing and Applied Mathematics, 2020, 3.1: 35-39.

THE MODIFICATION OF QUANTUM-RESISTANT AJPS FAMILY PRIMITIVES

Dariya Yadukha

Institute of Physics and Technology

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Ukraine

Keywords: *quantum-resistant cryptographic primitives, the AJPS cryptosystem, modular arithmetic, Mersenne number, generalized Mersenne number, Hamming weight*

In recent years, quantum-resistant cryptography has been steadily developing. Its aim is to develop the cryptographic primitives that would be resistant to attacks using both quantum and classical computers. In 2017, the National Institute of Standards and Technology (NIST) has launched the currently ongoing competition for quantum-resistant asymmetric cryptographic primitives [1]. According to the competition plan, it will be finished in 2024 [2]. As a result, USA will accept new post-quantum public-key cryptography standards, which will specify one or more additional digital signature, public key encryption, and key encapsulation algorithms to augment FIPS 186-4, Digital Signature Standard (DSS), as well as special publications SP 800-56A and SP 800-56B [3]. One of the participants of the first round of the competition is the Mersenne-756839 key encapsulation mechanism, which is based on the AJPS cryptosystem [4].

The AJPS cryptosystem uses arithmetic modulo Mersenne number, which can be efficiently implemented using algorithms for fast computation of cumbersome calculations of modular operations, such as reduction, multiplication, modular multiplicative inverse calculation, bitwise addition and multiplication modulo Mersenne number. AJPS has two versions – bit-by-bit encryption scheme (AJPS-1) and scheme for encrypting a message block (AJPS-2). Security of the AJPS-1 cryptosystem rests upon the conjectured intractability of the *Mersenne Low Hamming Ratio Search Problem* (MLHRSP), and the security of the AJPS-2 cryptosystem relies on the assumption that it is hard to solve the *Mersenne Low Hamming Combination Search Problem* (MLHCSP). The correctness of AJPS-1 and AJPS-2 follows from relations for the Hamming weight of sum and product of two numbers modulo Mersenne number and for the Hamming weight of additive inverse modulo Mersenne number.

To create modifications of AJPS-1 and AJPS-2 by changing the class of numbers which is used in the cryptosystems as a module, it is necessary to obtain the appropriate relations for the Hamming weight. Relations for the Hamming weight of sum and product of the two numbers modulo generalized Mersenne number and relations for Hamming weight of additive inverse modulo generalized Mersenne number and modulo Crandall number were proved [5]. Using these relations and certain conditions on key generation, encryption and decryption algorithms, we have created 4 modifications:

- modification of AJPS-1 using operations modulo generalized Mersenne number $GM_{n,m} = 2^n - 2^m - 1$, $n, m \in \mathbb{N}$, $n > m$;
- modification of AJPS-1 using operations modulo Crandall number $CR_{n,c} = 2^n - c$, $n, c \in \mathbb{N}$, $\log_2 c \leq \frac{n}{2}$;
- modification of AJPS-2 using operations modulo generalized Mersenne number $GM_{n,m}$;
- modification of AJPS-2 using operations modulo Crandall number $CR_{n,c}$.

As a result of the statistical analysis of two modifications of AJPS-1 [5], we found that the advantage of these modifications is not only a significant increase in the class of modules used, but also an increase in the interval length and the number of unique values of the decryption parameter d. Thus, such modifications allow us to increase the resistance of the AJPS-1 cryptosystem to known-plaintext attacks, which are aimed at determining the private key. Also, the constructed modifications of AJPS-1 and AJPS-2 have a greater variability of parameters, in particular, they allow the use of different number classes as a module, which increases the flexibility of the practical application of these cryptosystems.

References

1. Post-Quantum Cryptography Standardization // NIST, Information Technology Laboratory. – 2017. – https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization.
2. Workshops and Timeline Post-Quantum Cryptography // NIST, Information Technology Laboratory – https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline.
3. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process / [G. Alagic, J. Alperin-Sheriff, D. Apon and others] // NIST, Information Technology Laboratory, NISTIR 8240. – 2019. – https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf.
4. A New Public-Key Cryptosystem via Mersenne Numbers / D.Aggarwal, A. Joux, A. Prakash, M. Santha // IACR Cryptology ePrint Archive, Report 2017/481. – 2017. – https://eprint.iacr.org/2017/481.
5. Yadukha D. The Modification and Cryptanalysis of Quantum-resistant AJPS Family Primitives / Yadukha Dariya – Kyiv, 2020. – 135 p. – https://ela.kpi.ua/handle/123456789/34344.

Towards the security of McEliece's cryptosystem based on Hermitian subfield subcodes

By Sabira El Khalfaoui and Gábor P. Nagy

Abstract. The study of subfield subcodes of linear codes has been started in the 1960s. It has shown that this particular class of codes yields some good codes, which are of interest because of their applications to public-key cryptography due to McEliece and Niederreiter and to signature schemes based on error-correcting codes. In our previous work [3, 2], we established several results about the properties of subfield subcodes of Hermitian codes. This motivates us to build a McElice cryptographic scheme using these code parameters. Indeed, one of the crucial issues in cryptography today is to reduce the key size and improve the security level of the McEliece cryptosystem, which is a promising cryptographic scheme for the post-quantum era [1, 5].

The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding (ISD) algorithm using Hermitian subfield subcode parameters. Our approach focuses on the optimal parameters that improve the key size for a given security level. Furthermore, due to practical considerations, the key size of several parameter selections is compared to that of the classical McEliece cryptosystem submitted to NIST [4] for the same security level. Besides, we identify the Hermitian subfield subcodes parameters that achieve a Schur square dimension roughly equal to that of random codes. This technique is employed in the so-called distinguisher attack, and that may allow the attacker to determine the Schur square dimension of the code used as a public key.

Key words and phrases: code-based cryptography, McEliece Cryptosystem, Hermitian subfield subcodes, Schur square dimension.

Project no. 2018-1.2.1-NKP-2018-00004 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.

References

[1] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[2] Sabira El Khalfaoui and Gábor P. Nagy. Estimating the dimension of the subfield subcodes of Hermitian codes. *Acta Cybernet.*, 24(4):625–641, 2020.

[3] Sabira El Khalfaoui and Gábor P. Nagy. On the dimension of the subfield subcodes of 1-point Hermitian codes. *Adv. Math. Commun.*, 15(2):219–226, 2021.

[4] USA National Institute of Standards and Technology. Post-quantum crypto project. In *USA National Institute of Standards and Technology: Gaithersburg, MA, USA*, 2016.

[5] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

BOLYAI INSTITUTE
UNIVERSITY OF SZEGED
ARADI VÉRTANÚK TERE 1
H-6720 SZEGED
HUNGARY

E-mail: sabiraelkhalfaoui@gmail.com

DEPARTMENT OF ALGEBRA
BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS
EGRY JÓZSEF UTCA 1
H-1111 BUDAPEST
HUNGARY

BOLYAI INSTITUTE
UNIVERSITY OF SZEGED
ARADI VÉRTANÚK TERE 1
H-6720 SZEGED
HUNGARY

E-mail: nagyg@math.bme.hu

Benchmarking Post-Quantum KEMs for Group Key Establishment in TEE*

Peter Špaček

Slovak University of Technology in Bratislava, Slovakia
peter.spacek@stuba.sk

Keywords: Post-Quantum, Cryptography, Hardware Security Module, Group key establishment

Current development of quantum computers gives rise to a new area of post-quantum cryptography. NIST is currently in the final phase of the standardization process for post-quantum key encapsulation mechanisms (KEMs), that should replace public key cryptography used today. In adapting these algorithms, we have to consider several trade-offs. That may include running time or memory preference. Some of the algorithms are better suitable for lightweight systems, while others can only be used with better hardware.

In the work of [5], the authors proposed a new scheme for group communication. The system is secure under the assumption, that the adversary may gain an access to quantum computers in the future. Our present work focuses on evaluations of the NIST's PQC challenge KEM candidates for the group communication scheme. Our evaluation is focused on a scenario, where secure parts of the protocol are implemented in the hardware module.

A lot of attention has been given to the concept of a trusted execution environment (TEE). The main advantage of using a TEE is that the critical segments of the code should be unreachable by (standard) malware. No run-time code provisioning brings higher levels of trust for the system. Inspired by this concept, we can use similarly hardware security modules (HSM). Not only they can hide the code, but they can also store sensitive data, such as private keys.

We present the evaluation of post-quantum KEM candidates in particular HSM, SEcube. SEcube is a 3-in-1 solution that introduces a low-power ARM Cortex-M4 processor, FPGA, and an EAL5+ certified SmartCard. For the scope of this experiment, we use STM32F4. Preliminary implementation of the protocol on SEcube SDK was presented by [8]. The original implementation used a single fixed post-quantum KEM: NewHope by [1]. However, this KEM was not selected as a finalist for the NIST PQC project. In our present work, we extended the architecture of the system, and added other suitable KEMs: CRYSTALS-KYBER by [2], NTRU by [4], and SABER by [10].

In table 1 we present benchmarking results showing differences between clean implementations collected in pqclean project by [7], and its optimized versions. We also added masked implementation by [9], protected against side-channel attacks.

Table 1: KEM operations in CPU cycles

Implementation	keypair	encapsulation	decapsulation
clean ntruhps4096821 from [7]	226 008 483	2 922 913	7 483 006
optimized ntruhps4096821 from [6]	221 845 974	1 150 760	1 578 353
clean FireSaber from [7]	6 528 289	8 098 762	8 504 551
optimized FireSaber from [10]	3 648 631	4 511 196	4 180 551
clean Kyber1024 from [7]	4 390 006	5 323 618	5 004 678
optimized Kyber1024 from [3]	3 871 506	4 638 430	4 075 736
protected Kyber1024 from [9]	5 444 009	6 190 159	5 826 134

In our presentation, we will discuss this new modular architecture, and compare results from using various KEM, and the impact of parameter choice and SCA protections on the protocol runtimes.

*This research was sponsored by the NATO Science for Peace and Security Programme under grant G5448.

References

[1] E. Alkim et al. "Post-quantum key exchange—a new hope". In: *25Th {USENIX} security symposium ({USENIX} security 16)*. 2016, pp. 327–343.

[2] R. Avanzi et al. "CRYSTALS-Kyber algorithm specifications and supporting documentation". In: (2017).

[3] L. Botros, M. J. Kannwischer, and P. Schwabe. *Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4*. Cryptology ePrint Archive, Report 2019/489. `https://eprint.iacr.org/2019/489`. 2019.

[4] C. Chen et al. "Algorithm Specifications And Supporting Documentation". In: (2019).

[5] C. Colombo et al. "Secure communication in the quantum era:(group) key establishment". In: *Advanced Technologies for Security Applications*. Springer, 2020, pp. 65–74.

[6] M. J. Kannwischer et al. *pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4*. Cryptology ePrint Archive, Report 2019/844. `https://eprint.iacr.org/2019/844`. 2019.

[7] M. Kannwischer et al. *The PQClean Project, August 2020*. 2020.

[8] Peter Malo. *Implementation of the Protocol*. SPS Programme Meeting, Smolenice Castle, Slovakia. Mar. 2020.

[9] P. Ravi et al. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020.3 (June 2020), pp. 307–335. DOI: `10.13154/tches.v2020.i3.307-335`. URL: `https://tches.iacr.org/index.php/TCHES/article/view/8592`.

[10] I. F. Vercauteren. "SABER: Mod-LWR based KEM (Round 3 Submission)". In: (2020).

On the feasibility of algebraic cryptanalysis by bit flipping

Pavol Zajac *

Slovak University of Technology in Bratislava, Slovakia

Modern lightweight cipher designs, such as LowMC [2], and MiMC [1], try to minimize the number of (specific) logic gates required to realize the encryption algorithm. Lower overall number of gates leads to more efficient implementations [3] and lower power consumption. Furthermore, there are important cryptographic applications of primitives with low number of (non-linear) gates, such as homomorphic encryption [5], side channel protection [4], MPC [10], and others.

On the other hand, lower number of gates, especially non-linear AND gates, can have a negative impact on cipher security. In [9] we have investigated a generic reduction of an algebraic attack to an instance of a decoding problem. We have provided a lower bound on the number of AND gates required in the cipher design (relative to the security level) to resist attacks utilizing generic decoding algorithms. Note that this analysis is based on generic asymptotic bounds for the complexity of decoding algorithms and assumes a random linear layer of the cipher.

Suppose that a lightweight design have both low number of both AND gates and XOR gates. Algebraic cryptanalysis of such a design can be transformed into a multiple right-hand sides (MRHS) equation system [6] with a specific form of right hand side sets (RHS), and a sparse joint matrix.

Unlike our prior research in deterministic solving methods [8, 7], in our present contribution, we investigate heuristic methods for solving sparse MRHS systems. New methods are inspired by soft decoding techniques for LDPC codes. The main idea of the first algorithm is adaptive bit flipping. We start from a random potential solution, and we try to change some bits based on the information on from the RHS sets. We investigate different bit-flipping strategies, and their combinations.

Our preliminary experimental results show that adaptive bit flipping with local information is only slightly more efficient than fully random search. It also requires a careful optimization of the used heuristics. Selection of strategies is not straightforward, as each RHS is influenced by multiple bits. The main problem of locally informed bit-flipping approach seems to be higher potential for cycles than in comparison to classical LDPC decoding.

We get much better results with bit flipping strategies based on global information similar to Hill climbing. Our optimization function is the number of unsolved RHSs. Starting with a random potential solution, we evaluate each potential bit flip, and continue by a greedy strategy: we flip the bit which provides the best number of solved RHSs. If no bit flip leads to a better situation, we restart from another random potential solution. This simple strategy is a significant improvement on bit flipping based on local information (and exhaustive search). Note that this approach is different from classical heuristic optimization approaches to solving ciphers, as it does not work on key space bits, but instead works with all internal bits and their interconnections. While our experiments are based on random sparse equations, they may lead to new algebraic attacks on ciphers with sparse diffusion layer.

References

[1] M. Albrecht et al. "MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2016, pp. 191–219.

[2] M. R. Albrecht et al. "Ciphers for MPC and FHE". In: *Advances in Cryptology–EUROCRYPT 2015*. Springer, 2015, pp. 430–454. DOI: 10.1007/978-3-662-46800-5_17.

[3] N. Courtois, D. Hulme, and T. Mourouzis. "Solving Circuit Optimisation Problems in Cryptography and Cryptanalysis." In: *IACR Cryptol. ePrint Arch.* 2011 (2011), p. 475.

*This research was sponsored by Slovak Republic under grant VEGA 2/0072/20.

[4] D. Goudarzi and M. Rivain. "On the multiplicative complexity of boolean functions and bitsliced higher-order masking". In: *International Conference on Cryptographic Hardware and Embedded Systems*. Springer. 2016, pp. 457–478.

[5] P. Méaux et al. "Improved Filter Permutators: Combining Symmetric Encryption Design, Boolean Functions, Low Complexity Cryptography, and Homomorphic Encryption, for Private Delegation of Computations". In: *Proceedings of INDOCRYPT 2019* (2019).

[6] H. Raddum and I. Semaev. "Solving Multiple Right Hand Sides linear equations". In: *Design, Codes and Cryptography* 49.1 (2008), pp. 147–160. DOI: 10.1007/s10623-008-9180-z.

[7] H. Raddum and P. Zajac. "MRHS solver based on linear algebra and exhaustive search". In: *Journal of Mathematical Cryptology* 12.3 (2018), pp. 143–157. DOI: 10.1515/jmc-2017-0005.

[8] P. Zajac. "A new method to solve MRHS equation systems and its connection to group factorization". In: *Journal of Mathematical Cryptology* 7.4 (2013), pp. 367–381.

[9] P. Zajac. "Connecting the Complexity of MQ-and Code-Based Cryptosystems". In: *Tatra Mountains Mathematical Publications* 70.1 (2017), pp. 163–177. DOI: 10.1515/tmmp-2017-0025.

[10] G. Zaverucha, M. Chase, et al. "The Picnic Signature Algorithm". In: (2018). URL: https://microsoft.github.io/Picnic/.