QuantiXLie Center of Excellence
&
Department of Mathematics, Faculty of Science,
University of Zagreb

Book of Abstracts

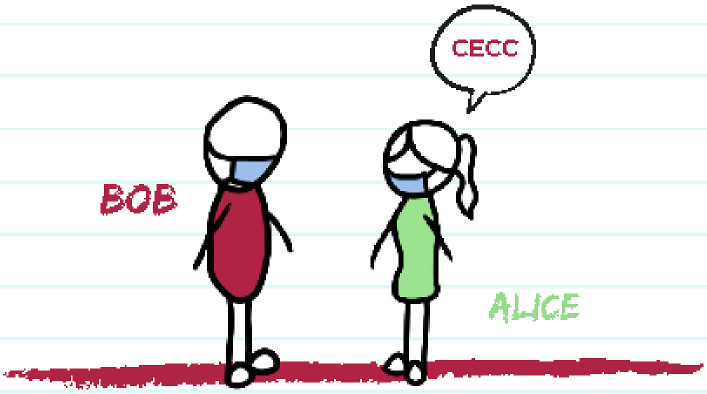
20th Central European Conference on Cryptology

CECC 2020

June 24 – 26, 2020, Zagreb, Croatia

JUNE 24-26 2020 ZAGREB, CROATIA

20TH CENTRAL EUROPEAN CONFERENCE ON CRYPTOLOGY



INVITED SPEAKERS

Elena Andreeva
Lilya Budaghyan
Florian Mendel
Marcin Pawłowski

ORGANIZERS

Andrej Dujella
Zrinka Franušić
Matija Kazalicki
Ivan Krijan
Filip Najman
Tomislav Pejković
Vinko Petričević
Antonela Trbović

Organized by

QuantiXLie Center of Excellence

Department of Mathematics, Faculty of Science, University of Zagreb

Technical organizer

Perfecta Travel d.o.o.

Supported by

QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004)

The Foundation of the Croatian Academy of Sciences and Arts

Znanstveni centar izvrsnosti
za kvantne i kompleksne sustave te
reprezentacije Liejevih algebri

Projekt KK.01.1.1.01.0004

Projekt je sufinancirala Europska unija iz Europskog fonda za regionalni razvoj. Sadržaj ovog seminara isključiva je odgovornost Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI
I INVESTICIJSKI FONDOVI

Operativni program
KONKURENTNOST
I KOHEZIJA

EUROPSKA UNIJA
Europski fond za regionalni razvoj

Program Committee

Andrej Dujella, University of Zagreb (chairman)
Nicolas Courtois, University College London
László Csirmaz, Central European University
Claus Diem, University of Leipzig
Peter Gaži, IOHK Research
Jan Hajny, Brno University of Technology
Clemens Heuberger, Alpen-Adria-Universität Klagenfurt
Bernadin Ibrahimpašić, University of Bihać
Aleksandar Jurišić, University of Ljubljana
Matija Kazalicki, University of Zagreb
Miroslaw Kutyłowski, Wrocław University of Science and Technology
Vashek Matyáš, Masaryk University, Brno
Florian Mendel, Infineon Technologies
Filip Najman, University of Zagreb
Karol Nemoga, Slovak Academy of Sciences
Attila Pethő, University of Debrecen
Andrea Pintér-Huszti, University of Debrecen
Stefan Porubsky, Czech Academy of Sciences
Håvard Raddum, Simula UiB, Norway
Vincent Rijmen, KU Leuven and University of Bergen
Martin Stanek, Comenius University
Rainer Steinwandt, Florida Atlantic University
Damian Vizar, CSEM, Switzerland
Pavol Zajac, Slovak University of Technology in Bratislava

Organizing Committee

Andrej Dujella, University of Zagreb
Zrinka Franušić, University of Zagreb
Matija Kazalicki, University of Zagreb
Ivan Krijan, University of Zagreb
Filip Najman, University of Zagreb
Tomislav Pejković, University of Zagreb
Vinko Petričević, University of Zagreb
Antonela Trbović, University of Zagreb

Abstracts of invited talks

Forkciphers: New Cryptographic Primitives

Elena Andreeva

Technical University of Denmark

elean@dtu.dk

In symmetric cryptography we build encryption and/or authentication cryptographic schemes with classical primitives, such as (tweakable) block ciphers, permutations and hash functions. In this talk I will introduce a novel cryptographic primitive called forkcipher which, contrary to classical primitives, expands its fixed length input to a larger fixed length output. Forkcipher can improve the efficiency for many existing encryption, authentication and authenticated encryption designs.

I will show concrete examples of authenticated encryption (AE) and encryption schemes instantiated with the first concrete forkcipher ForkSkinny. I will illustrate how ForkSkinny for AE achieves improved efficiency for short messages - an important use case for numerous lightweight applications.

I will also explore the uses of forkciphers in encryption only modes where significant efficiency over classical encryption schemes is gained with the number of processed message blocks. I will conclude this talk with forkcipher generalizations and future novel applications.

Optimal cryptographic functions solving hard mathematical problems

Lilya Budaghyan

University of Bergen

Lilya.Budaghyan@uib.no

Vectorial Boolean functions are used in cryptography, in particular in block ciphers. An important condition on these functions is a high resistance to the differential and linear cryptanalyses, which are among the main attacks on block ciphers. The functions which possess the best resistance to the differential attack are called almost perfect nonlinear (APN). Almost bent (AB) functions are those mappings which oppose an optimum resistance to both linear and differential attacks. An interesting fact is that APN and AB functions also define optimal objects in other domains of mathematics and information theory such as coding theory, finite geometry, sequence design, algebra, combinatorics, et al.

In this talk we will discuss problems and recent advances in construction and analysis of these functions and their influence to solutions of hard mathematical problems.

Lightweight Authenticated Encryption

Florian Mendel

Infineon Technologies

florian.mendel@gmail.com

Driven by a demand for cryptographic protection in resource-constrained embedded devices, lightweight cryptography has been actively studied in the last decades. While block ciphers and hash functions have received a great deal of attention from the cryptographic community resulting in plenty of new designs, authenticated encryption schemes have been arguably less popular among researchers for a long time. At the same time, message secrecy - as provided by plain encryption - is often of limited value in practice if not accompanied by message authentication, thereby showing the need for dedicated authenticated encryption schemes in the ?eld. This is also re?ected by the CAESAR competition and NIST's standardization efforts that resulted in plenty of new proposals for lightweight authenticated encryption schemes tailored for resource-constrained devices in the last few years, usually optimizing the area and power consumptions of the primitive in hardware and/or software.

Moreover, resource-constrained devices are often used in environments in which side-channel attacks need to be considered and countermeasures against the attacks need to be implemented with limited resources, which is a challenging task. Today, there exist essentially two different approaches to counteract side-channel attacks. The first approach works by hardening the implementation of cryptographic algorithms with techniques like hiding or masking. The drawback of this approach is that the overhead for securing a cryptographic primitive against side-channel attacks might be very high and depends on the cryptographic primitive itself. Therefore, in the past several ciphers have been proposed to reduce this cost. For example, several of the authenticated encryption schemes submitted to CAESAR and the NIST standardization process have been designed with this goal in mind. The second approach to counteract side-channel attacks is to design cryptographic protocols or schemes in such a way that certain types of side-channel attacks cannot be performed on the underlying cryptographic primitive, thereby significantly reducing the cost for implementing additional countermeasures.

An example of such an approach is leakage-resilient cryptography and fresh re-keying that has recently adapted for authenticated encryption and resulted in a number of new schemes.

In this talk, we will review both approaches and discuss their advantages for particular use cases by means of two examples Ascon and ISAP, both submitted to the NIST standardization process. First, we will discuss Ascon, the primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR, and show that the simple design of Ascon allows quite efficient implementations of countermeasures against side-channel attacks in both software and hardware. This makes Ascon, in general, an excellent choice for applications that need some side-channel protection.

Then we will discuss ISAP, an authenticated encryption scheme that incorporates ideas from fresh re-keying and leakage-resilient cryptography and addresses most classes of side-channel attacks already on an algorithmic level. This allows very efficient implementations of the scheme with low overhead in scenarios where side-channel robustness is needed, albeit at the cost of a higher runtime compared to dedicated schemes in scenarios where this is not needed. Thus, ISAP is best suited for applications where performance is not critical, but robustness against side-channel attacks is needed, and code size and area matters.

Quantum Random Number Generators

Marcin Pawłowski

International Centre for Theory of Quantum Technologies

marcin.pawlowski@ug.edu.pl

The main difference between Quantum Random Number Generators (QRNGs) and other hardware generators is that, due to intrinsic randomness of quantum mechanics, they can be made self-testing. It means that the device, during its normal operation, constantly returns a lower bound on the entropy of its output. This allows QRNGs of this type to immediately report malfunction or attack and makes it impossible to produce them with backdoors.

I will start my talk by explaining the quantum mechanical properties that allow for generation of randomness and show how they can be exploited to build a QRNG. Then I will explain the methods that can be used to prove the lower bounds on entropy of their outcomes. Next I will present security proofs against a wide range of attacks and backdoors focusing on their limitations. I will conclude by presenting the state of the art of both commercially available devices and experimental hardware.

Extended abstracts of contributed talks

Sufficient conditions of five-valued spectra Boolean functions

Samed Bajrić

Jožef Stefan Institute, Laboratory for Open Systems and Networks, 1000 Ljubljana, Slovenia; **email:** *samed@e5.ijs.si*

Abstract. The main purpose of this paper is to present sufficient conditions for a function of the form $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$ to be five-valued with the Walsh spectrum $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$, where $g(x)$ is some known bent function. The importance of our result lies in the fact that we can control the algebraic degree of function $f(x)$ by adding an arbitrary product of linear functions, which is not the case with the recently proposed results.

Keywords: Boolean function · Linearized polynomials · Five-valued.

1 Introduction

Plateaued Boolean functions seem not very numerous and they do not seem to have a simple structure. There are only a few design methods of so-called 5-valued spectra Boolean functions whose Walsh spectra takes the values in $\{0, \pm 2^{\lambda_1}, \pm 2^{\lambda_2}\}$. It is well-known that these functions may satisfy multiple cryptographic criteria. The main existing research related to the design of 5-valued spectra functions can be traced to the early work of Maitra and Sarkar, and some recent articles [1, 2, 4]. In a recent article, Xu et al. [4] have characterized several classes of five-valued spectra functions by adding the product of three or two linear functions to some known bent functions. We generalize this result by adding an arbitrary product of linear functions to some known bent function, so that we are able to control the algebraic degree of $f(x)$. This characterization of five-valued spectra functions allow us to design functions with good algebraic degree to be resistant to various types of cryptanalytic attacks.

2 Five-valued spectra functions

We briefly describe how to compute the Walsh–Hadamard transform of a Boolean function $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$ which is very useful for the proving the main theorem of this section. Though the following lemma can be seen as a consequence of a theorem recently proved by Tang et. al [3] (cf. Theorem 8), where the authors gave a generic construction of bent functions, they did not consider the possibilities of constructing five-valued spectra Boolean functions. Moreover, the authors in [4] considered only the particular case ($l = 3$).

Lemma 1. *Let n and l ($l < 2^n - 1$) be two positive integers and $u_j \in \mathbb{F}_{2^n}^*$, where $j = 1, \ldots, l$. Let $g(x)$ be a Boolean function defined over $\mathbb{F}_{2^n}$. Define the Boolean function $f(x)$ by $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$. Then, for every $a \in \mathbb{F}_{2^n}$,*

$$\begin{aligned}
W_f(a) = \frac{1}{2^{l-1}}[(2^{l-1}-1)W_g(a) + W_g(a+u_1) + W_g(a+u_2) + \ldots + W_g(a+u_l) - \\
W_g(a+u_1+u_2) - W_g(a+u_1+u_3) - \ldots - W_g(a+u_{l-1}+u_l) + \\
W_g(a+u_1+u_2+u_3) + W_g(a+u_1+u_2+u_4) + \ldots + W_g(a+u_{l-2}+u_{l-1}+u_l) - \\
\vdots \\
+(-1)^{l-1}W_g(a+u_1+\ldots+u_{l-2}+u_{l-1}+u_l)].
\end{aligned}$$

Using the above lemma it can be proved the following theorem, which allows us to construct an infinity family of five-valued spectra functions.

Theorem 1. *Let $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$, where $n = 2m$ is a positive integer, $l < 2^n - 1, u_j \in \mathbb{F}_{2^n}^*$. Let $g(x) = Tr_1^m(\lambda x^{2^m+1})$, $\lambda \in \mathbb{F}_{2^m}^*$ be the monomial Niho quadratic bent function with Walsh transform given by [4], $W_g(a) = -2^m(-1)^{Tr_1^m(\lambda^{-1}a^{2^m+1})}$. If*

$$Tr_1^n(\lambda^{-1}u_1^{2^m}u_2) = 1 \text{ and } Tr_1^n(\lambda^{-1}u_1^{2^m}u_3) = \ldots = Tr_1^n(\lambda^{-1}u_{l-1}^{2^m}u_l) = 0,$$

then f is a five-valued spectra function with the Walsh spectrum $\{0, \pm 2^m, \pm 2^{m+1}\}$.

3 Conclusions

In this paper we have addressed some important issues related to the sufficient conditions for a given function to be five-valued. The presented method can be easily combined with some other type of known bent functions such as Gold-like monomial or Maiorana-McFarland type of bent functions.

References

1. S. Hodžić, E. Pasalic, and W. G. Zhang. Generic constructions of 5-valued spectra Boolean functions. *IEEE Transaction on Information Theory*, vol. 65(11), pp. 7554–7565, 2019.
2. S. Mesnager and F. Zhang. On constructions of bent, semi-bent and five valued spectrum functions from old bent functions. *Advances in Mathematics of Communications*, vol. 11(2), pp. 339–345, 2017.
3. C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth. Generic construction of bent functions and bent idempotents with any possible algebraic degrees. *IEEE Transaction on Information Theory*, vol. 63(10), pp. 6149–6157, 2017.
4. G. Xu, X. Cao and S. Xu. Several classes of Boolean functions with few Walsh transform values. *Applicable Algebra in Engineering, Communication and Computing*, vol. 28(2), pp. 155–176, 2017.

Computing Minimal DNF of Boolean Functions for Digital Implementations

Reni Banov[1]
[1]University of Applied Sciences, Zagreb.

1 Introduction

Most modern high-speed communication systems rely on technologies for a secure and reliable fast information exchange. Reliable communication is achieved by introducing error-correction codes into transferred messages, while security is achieved by encrypting the message before its transfer and its decryption afterwards. In both technologies Boolean functions of n variables

$$f : \mathbb{F}_2^n \to \mathbb{F}_2$$

are applied in order to implement error detecting/correcting codes or S-boxes into symmetric cryptographic systems such as DES, AES, only to name a few. Since today's communication channels operate at extremely high throughputs (10^{10} bits per seconds are common), it has become increasingly important how Boolean functions are implemented in the hardware to cope with such a tremendous speed demand. Intrigued by this, it has herein been the author's intention to trace the existing solutions for the Boolean function minimization which eventually are to result in their efficient utilization in cryptographic systems. Further to that, the selection of the Boolean function for that purpose must be carried out carefully, even if we dispose over 2^{2^n} Boolean functions of n variables. Among all Boolean functions, the *Bent* functions [8], i.e. Boolean functions, having *Hamming* distance of $2^{n-1} - 2^{\frac{n}{2}-1}(n - even)$ from all n variable *affine* functions, play an important role in the implementation of cryptographic systems. For every Boolean function exists a unique representation with polynomial

$$f(x_1,\ldots,x_n) = \sum_{v\in\mathbb{F}_2^n} a_v x^v,\, a_v \in \mathbb{F}_2 \qquad \text{(E1)}$$

from $\mathbb{F}_2[x_1,\ldots,x_n]/(x_1^2 + x_1,\ldots,x_n^2 + x_n)$, the so called *Algebraic Normal Form*, shortly ANF. As ANF forms are not convenient for a minimization of digital circuits needed to implement Boolean functions [9], it is more appropriate to use *Disjunctive Normal Form* (DNF), especially their minimal form. However, finding the minimal DNF form for any Boolean function is a *NP-Complete* problem, even for the simplest class of *monotonic* Boolean functions [5]. The time and space complexity of a problem requires a novel data structure to represent Boolean functions. Usually, Boolean functions are presented with *truth tables*, but the Boolean Decision Diagrams (BDD) structure [6], i.e. a variant of *directed acyclic graph* with two terminal vertices, are far more efficient for implementation. The BDDs and their variations may be used to compute minimal DNF of any Boolean function as well as to solve many other optimization problems [10].

2 Implementation

The BDDs for Boolean functions are derived from the Shannon identity

$$f^n(\mathbf{x}) = \left(x_i \wedge f^{n-1}_{x_i=1}(\mathbf{x})\right) \vee \left(\overline{x_i} \wedge f^{n-1}_{x_i=0}(\mathbf{x})\right) \qquad \text{(E2)}$$

applied recursively to each function $f^{n-1}_{x_i=1}, f^{n-1}_{x_i=0}$ in expansion. Each Shannon step generates a part of a full binary tree with the vertices structured as shown in Figure 1, up to the bottom of the tree with two terminal vertices representing Boolean values $\{0,1\}$. The Shannon identity (E2) with BDDs is commonly expressed by means of the If-Then-Else (*ite*) construction, for instance, the tree structure from Figure 1 is written as $ite\left(x_i, f^{n-i}_{x_i=1}, f^{n-i}_{x_i=0}\right)$. When BDDs are implemented with complemented edges [2], the negative *ite* has the meaning of a logical negation ($\neg$) of the represented function. If an order of variables is the same (preserved) on each path from any vertices down to terminal vertices, the BDD is denoted as *Ordered BDD*. While the expansion is performed the vertices for each unique Boolean function $f^i(\ldots)$ are generated only once, thereby making an ordered BDD *reduced* and ensuring the uniqueness of representation, i.e. the canonical representation of the Boolean function. The BDD structure allows an efficient implementation of usual logical operations [3], which makes it a suitable tool for manipulating Boolean functions.

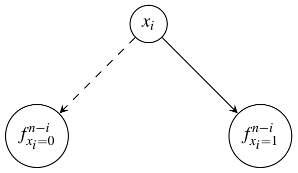


Figure 1: The BDD of $ite\left(x_i, f^{n-i}_{x_i=1}, f^{n-i}_{x_i=0}\right)$

A critical step in the application of the BDDs for a Boolean function representation is the variable order selection. The problem of finding the optimal order of variables for the Shannon expansion is an open problem belonging to the class of *NP-hard* problems. Even the problem of improving some variable orders is *NP-complete* [1]. Nevertheless, a large class of Boolean functions can be manipulated efficiently with BDDs.

As a contribution to finding a variable order the author has elaborated a new heuristic algorithm. The idea of this algorithm leans on the fact that Boolean functions can be written with their parse tree, and by traversing the latter in the *depth-first* manner, it is possible to build the variable order iteratively. In reaching every interior node during the traversing procedure, the order of the respective node is combined in a new way from the orders of the child nodes. The final variable order corresponds to the parse tree top node order. It will herein be shown, that the variable order built in that way allows an efficient application of BDDs for the minimization of Boolean functions in digital implementations.

2.1 DNF minimization algorithm

Every Boolean function can be represented in its *full* DNF form

$$f(x_1,\ldots,x_n) = \bigvee_k \left(\bigwedge_{i_k=1}^{n} \xi_{i_k}\right) \qquad \text{(E3)}$$

containing a disjunction of conjunction terms consisting of $\xi_i \in \{x_i, \overline{x_i}\}$, i.e. variables or their negations only, but not both in the same term.

It is obvious from the Boolean function *full* DNF form that

$$p(\mathbf{x}) = 1 \implies f(\mathbf{x}) = 1$$

applies for any conjunction term p. The conjunction term p containing *some* literals

$$p = \bigwedge_{i=1}^{k} \xi_i,\, k \le n$$

having no sub terms

$$q \subset p : q(\mathbf{x}) = 1 \implies f(\mathbf{x}) = 1$$

is called *prime implicants*. For the purposes of the Boolean function digital circuit implementation we seek to finding its minimal DNF form in the sense of the definition from [9], i.e. to find the minimal number of *prime implicants* which conjunction represents the considered Boolean function.

This is an extended abstract. The full paper will be available at the
20^{th} Central European Conference on Cryptology

As stated in the quoted reference, such a minimal DNF form, being implemented in the digital circuit, shall be optimal in the restricted class of two-level digital circuits (disjunction of conjunctions) made of $\{\vee, \wedge, \neg\}$ gates.

The minimization of the *full* DNF form of the Boolean function is based on the following fact from [7]. For every Boolean function of n variables, the set of all terms from the *full* DNF form (E3) can be partitioned

$$\left\{ \bigwedge_{i_k=1}^{n} \xi_{i_k} : k = 1, \ldots, l \right\} = P_{x_i} \cup P_{\overline{x_i}} \cup P_*,$$

into three sets of terms

- P_{x_i} – containing variable x_i
- $P_{\overline{x_i}}$ – containing negation of variable x_i
- P_* – **not** containing variable x_i.

In the light of that fact, Coudert [4] developed an algorithm for the minimization of Boolean functions based on the BDDs and their variation *Zero-suppressed Decision Diagrams* (ZDDs) for manipulation of sets of combinations. The essential part of his algorithm is the approach of solving the minterm set covering problem by the set covering problem on lattices. For that the author used a BDD and ZDD data structure to implement a novel algorithm to find the set cover fixed point on lattices. The fixed point is further searched by the Branch-and-Bound algorithm to find essential minterms contained within. It is important to mention that the complexity of the author's algorithm is exponential, since the set covering problem is *NP-complete*. Once the minimal DNF form of the Boolean function is found it can be implemented in the hardware with a minimal number of digital circuits.

2.2 Example

As an example, let us minimize (for the digital circuit implementation) the Bent function $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ defined in ANF form (E1)

$$f(x_0, x_1, x_2, x_3) = x_0 * x_1 + x_2 * x_3 + x_0 + x_1$$

with the truth table as follows

x_3	x_2	x_1	x_0	$f(x_0, x_1, x_2, x_3)$
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Applying the Shannon identity (E2), and assuming the variable ordered set $\{x_0, x_1, x_2, x_3\}$, their minimal DNF form is calculated with the algorithm from the previous section

vertex	*variable*	*then*	*else*
v_0	x_0	v_1	$\overline{v_2}$
v_1	x_1	v_2	$\overline{v_2}$
v_2	x_2	1	v_3
v_3	x_3	1	$\overline{1}$

representing the function

$$\begin{aligned} f(\mathbf{x}) &= \left((x_0 \wedge x_1) \wedge \overline{(x_2 \vee x_3)} \right) \vee \left(\overline{(x_0 \wedge x_1)} \wedge (x_2 \vee x_3) \right) \\ &= (x_0 \wedge x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2) \vee (\overline{x_1} \wedge x_3) \vee (\overline{x_0} \wedge x_2) \vee (\overline{x_0} \wedge x_3). \end{aligned}$$

The minimal DNF form of the function $f(\mathbf{x})$, depicted in the second table, is represented with the vertex $\overline{v_0}$, where *ite* constructs are shown with complemented edges. In the end, the function can be implemented with a digital circuit containing a two *OR*, three *AND*, and two *NOT* gates operating on four input variables (digital lines), and what is most important with only three clock cycles overhead. Modern digital circuit implementations allow even a parallelization of such a circuit operation within a single clock cycle.

3 Conclusion

The key step in the application of BDDs is a variable order for Shannon expansion which allows efficient operations with Boolean functions, e.g., their minimization. As it was shown in the example, the minimization of Boolean functions can be used to produce optimal digital circuits for the implementation of an important class of cryptographic functions. In addition to that, this topic presents open problems for further research in the field of combinatorial optimizations, such as variable ordering in Shannon expansion and set covering problem. It is also important to mention that the properties of Boolean (Bent) functions can be further elaborated by research on graph properties of BDDs and their variants.

References

[1] B. Bollig and I. Wegener. Improving the variable ordering of OBDDs is NP-complete. *IEEE Transactions on Computers*, C-45(9):993–1002, September 1996.

[2] K. Brace, R. Rudell, and R. Bryant. Efficient Implementation of a BDD Packages. In *Proceedings of the 27th ACM/IEEE Design Automation Conference*, pages 40–45, 1990.

[3] R.E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, 35(8):677–691, 1986.

[4] O. Coudert. Doing Two-Level Logic Minimization 100 Times Faster. In *Proceedings of the sixth annual ACM-SIAM symposium on Discrete algorithms*, pages 112–121, 1995.

[5] J. Goldsmith, M. Hagen, and M. Mundhenk. Complexity of DNF and Isomorphism of Monotone Formulas. In *International Symposium of Mathematical Foundations of Computer Science*, pages 410–421, 2005.

[6] C. Meinel and T. Thorsten. *Algorithms and Data Structures in VLSI Design*. Springer-Verlag, ISBN: 3-540-64486-5, 1998.

[7] E. Morreale. Recursive operators for prime implicant and irredundant normal form determination. *IEEE Transactions on Computers*, 19(6): 504–509, 1970.

[8] N. Tokareva. *Bent Functions: Results and Applications to Cryptography*. Academic Press, ISBN: 0128025557, 9780128025550, 2015.

[9] I. Wegener. *The Complexity of Boolean Functions*. Wiley Teubner, ISBN: 978-0-471-91555-3, 1991.

[10] I. Wegener. *Branching Programs and Binary Decision Diagrams: Theory and Applications*. SIAM, ISBN: 0-89871-458-3, 2000.

ALGORITHM FOR SHORT MESSAGES ENCRYPTION ON TWISTED EDWARD CURVES

A. BESSALOV, L. KOVALCHUK, N. KUCHYNSKA, O. TELIZHENKO
IPT National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Abstract. The purpose of our researches is to develop a national standard of short messages encryption, with well-defined procedures, on the one hand, and a sufficient level of security and effectiveness, on the other. In this paper, we propose algorithm for short messages encryption on twisted Edwards curves, with described general cryptosystem parameters and individual parameters of users. The authors proved correctness and security of the proposed algorithm.

Introduction. Nowadays, the ISO/IEC 18033-2:2006 standard is harmonized in Ukraine as DSTU ISO/IEC 18033-2: 2015. However, an urgent task for Ukrainian cryptographic researchers today is to develop a public-key encryption algorithm for short messages that could be used as a National Standard, with clearly specified procedures that should have acceptable performance and a sufficient level of security.

In addition, among the national standards, we should note the Belarusian standard STB 34.101.45-2013 [1] that approves algorithms for digital signature and key transport on elliptic curves. This standard contains defined algorithms in detail, where the asymmetric key transport algorithm is based not only on elliptic curves but also on National block encryption algorithm BelT STB.

Algorithm description. Considering advantages of using cryptosystems on elliptic curves, we proposed to develop an algorithm for short messages encryption on twisted Edwards curves [2]. We should make certain remarks that the proposed algorithm is recommended only for the transition period to the post-quantum cryptography.

Taking into the account properties of the Edwards curves [3], we use the curve $Edw\left(F_p\right)$ over a finite field F_p where $p \equiv 5 \bmod 8$, given by the following equation:

$$Edw\left(F_p\right): x^2 + ay^2 = 1 + dx^2y^2,\ a \neq d,\ a, d \notin Q_p, \tag{1}$$

where Q_p is a set of quadratic residues modulo p.

We define the general parameters of the cryptosystem below.

- Security level λ that actually determines choice of other parameters. Recommended values of λ are given in Table 1.
- Prime number p with bit length $l(p) = \lfloor \log_2 p \rfloor + 1 = 2(\lambda + 1)$ that determines the finite field F_p.
- $Edw\left(F_p\right)$ is a twisted Edwards curve (1) over F_p; for all recommended curves we set $a = 2$.
- Base point P of the curve $Edw\left(F_p\right)$ such that $ord(P) = n$.
- A private key, or a decryption key, is an element $e \in F_p$. The corresponding public key, or the encryption key, is some point of the twisted Edwards elliptic curve computed as $Q = eP$.
- Hash-function H, where the length of its output is l_H. As a recommended hash-function, we assume to use DSTU 7564:2014.
- l-bit block and k-bit key κ of block cipher Kalyna-l/k [4] with basic encryption $E_{l,k}^{(\kappa)}$ and decryption $D_{l,k}^{(\kappa)}$ transformations.

It should be noted that the formatted plaintext M is assumed to be the element of F_p.

Table 1. Connection between λ, $l(p)$ and Kalyna-l/k parameters.

λ	127	191	255	383
$l(p)$	256	384	512	768
l/k	256/256	256/256	512/512	512/512

Encryption algorithm

1. Choose a random integer $\varepsilon : 1 < \varepsilon < n-1$.
2. Compute the point $R = \varepsilon P = \left(x_R, y_R\right)$, set r as a bit representation of x_R of the length $l(p)$.
3. Compute the point $T = \varepsilon Q = \left(x_T, y_T\right)$ and set $\kappa = x_T^{(l)}$ as the lowest l bit of x_T.
4. Compute $t = E_{l,k}^{(\kappa)}\left(M\right)$.
5. The ciphertext is $C = (r \,\|\, t)$.

Decryption algorithm

1. Compute $u = \left(1 - r^2\right)\left(a - dr^2\right)^{-1} \bmod p$ and root $y = \sqrt{u} \bmod p$, set $R = \left(r, y\right)$.
2. Compute $T' = \left(x_{T'}, y_T'\right) = eR'$ and set $x_T^{(l)}$ as the lowest l bit of x_T.
3. Compute the message $M = D_{l,k}^{(\kappa)}\left(t\right)$.

Security and efficiency of the algorithm. We proved that an attack on the proposed algorithm (the key recovery or the plaintext recovery) is no easier than one of the two problems – CDH or DLP. We also proved its security against distinguishing attacks.

Conclusion. We propose the algorithm of short messages encryption on twisted Edwards curves. General parameters of the cryptosystem and individual parameters of users are described. This algorithm is similar with STB key transport algorithm [1], but uses another form of elliptic curves and make use of National Ukrainian Standards hash-function and symmetric encryption. The authors also constructed all general parameters of the proposed cryptosystem.

References

1. STB 34.101.45-2013. Electronic digital signature and key transport algorithms based on elliptic curves. Standard of Belarus http://apmi.bsu.by/assets/files/std/bign-spec29.pdf
2. RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA). Edwards-Curve Digital Signature Algorithm (EdDSA) Електронний доступ: https://tools.ietf.org/html/rfc8032
3. Бессалов А.В. Эллиптические кривые в форме Едвардса и криптография: монографія. Киев, КПИ им. Игоря Сикорского, изд. «Политехника». 2017. 272с. http://elibrary.kubg.edu.ua/id/eprint/21879/1/A_Bessalov_Polytechnika_2017_FIT.pdf
4. Roman Oliynykov et.al. A new encryption standard of Ukraine: The Kalyna block cipher. IACR Cryptology ePrint Archive, 2015:650, 2015. http://eprint.iacr. org/2015/650.

Note: this is second version of algorithm. We thank anonymous reviewers for pointing out some aspects of security.

On Reducing Annihilation Degree inside Nonlinear Invariant Attacks on T-310 and DES

Nicolas T. Courtois[1], Matteo Abbondati[2], and Aidan Patrick[3]

[1] University College London, Gower Street, London, UK
[2] Independent maths teacher based in London, UK
[3] Cryptography Team, British Telecom Plc. Martlesham Heath, UK

Abstract. A major open problem in block cipher cryptanalysis is the discovery of new non-linear invariant attacks. There is no systematic method for construction of such attacks however there are some ad-hoc heuristic constructions [4]. A key problem is to find attacks with smaller degree and using less variables. **Key Words:** block ciphers, Boolean functions, Feistel ciphers, T-310, Generalized Linear Cryptanalysis, polynomial invariants, annihilator space, invariant theory.

A frequently cited paper by Knudsen and Robshaw from Eurocrypt'96 cf. [5]. claimed that nonlinear polynomial attacks cannot or will not work for Feistel ciphers. There is no doubt non-linear invariant attacks CAN be made to work for Feistel ciphers, cf. [4]. For example in a recent paper we show that a certain non-zero polynomial of degree 7, namely $\mathcal{P} = (A+B)\ (C+D)\ (D+F)(B+F)\ (E+F)(G+F)(G+H)$ with $A = (i+m)$, $B = (j+n)$ $C = (k+o)$, $D = (l+p)$, $E = (y+O)$, $F = (z+P)$, $G = (M+Q)$ and $H = (N+R)$ is an invariant for T-310 for any key any IV and any number of rounds, this if a certain product of polynomials such as $(Z+1)*(a+d+e+f+1)(d+a)(d+a+b+c+1)$ is annihilated, cf. [3]. The same approach was then applied to DES [4]. Here the degree of annihilators tends to increase a lot, or the attacks work only for a tiny fraction of the key space. Is there any hope to do better than this? In this paper we show a theoretical possibility to find more annihilations, or to annihilate polynomials which would never be annihilated in the strict framework of any previously known attack.

A crucial ingredient. If we look at the proof in Section 4 of [3] why this attack works, it defined a certain polynomial $\mu = (B+C)(G+H)(B+H)(B+F)(C+D)$ and it is crucial that we have $\mu(W+Y) = 0$. This was seen many times in T-310. The problem is that $W+Y$ has 12 variables, a property far beyond general results on classifying all known Boolean functions for up to 6 variables [Maiorana]. Why this matters? Consider for example DES S8, we actually cannot hope that $(a+e)*(e)*W8(a,b,c,d,e,f) = 0$ because none of the 32 Boolean functions in DES whatsoever has an annihilator which is a product of 2 linear factors. However we have:

$$(\mathrm{Z3} + \mathrm{Z7} + \mathrm{R08} + \mathrm{R09} + \mathrm{R10} + \mathrm{R12} + \mathrm{R13} + \mathrm{R24} + \mathrm{R27} + \mathrm{R28} + \mathrm{R29}) *$$

$$(\mathrm{R08} + \mathrm{R10} + \mathrm{R11}) * (\mathrm{R26}) * (\mathrm{R08} + \mathrm{R26}) * (\mathrm{R25} + \mathrm{R26}) = 0$$

We see that we can hope to reduce the degree in polynomial invariant attacks if 1) we are allowed to annihilate things such as $(W+c+e)+(Y+a'd')$, which is allowed using the general methodology of [4], and 2) if maybe we can somewhat magically annihilate $(W + c + e) + (Y + a'd')$ without annihilating individual components. Now for a very long time we thought his was strictly impossible and none of the current attacks on T-310 has this property. In fact in [3] we surely have $\mu(W+Y) = 0$ with $\mu W \neq 0$ however unhappily we have $\mu(W+1) = 0$ and $\mu(Y+1) = 0$. We have not discovered anything new. Is there any hope that a sum of two Boolean function with **disjoint** variables (direct sum) can be annihilated in a **new way** different than currently, and a lower degree, as it is impossible to have degree 2 annihilators in DES? The expert interpretation of the equality on $Z3 + Z7$ above is that a sum of two outputs in DES is 4-weakly-normal instead of 6 expected in the worst case [2]. This is a significant vulnerability knowing that we have as many as 12 variables. 12 variables are in some sense reduced or compressed to just 4 linear combinations of these variables. We obtain new powerful optimized ways to eliminate totally, some very complex Boolean functions with 12 variables inside a polynomial invariant attack. The reader will check that $\mu W \neq 0$ and $\mu(W + 1) \neq 0$ and the same for Y. However finding just one example is not enough. In cryptanalysis we want to have a systematic construction. Here is our existence theorem:

Theorem 0.1. If $WY \neq 0$ and $WY + W + Y \neq 1$, then $\exists \mu \in \mathbf{B}_n$ s.t.:

$$(*)\begin{cases} \mu(W+Y) = 0 & (1) \\ \mu W \neq 0 & (2) \\ \mu Y \neq 0 & (3) \\ \mu(W+1) \neq 0 & (4) \\ \mu(Y+1) \neq 0 & (5) \end{cases}$$

Proof. $WY \neq 0 \Rightarrow \exists p \in \mathbb{F}_2^n$ s.t. $W(p) = Y(p) = 1$ and $WY + W + Y \neq 1 \Leftrightarrow (W+1)(Y+1) \neq 0 \Rightarrow \exists q \in \mathbb{F}_2^n$ s.t. $W(q) = Y(q) = 0$. We define:

$$\mu(x) = \begin{cases} 1 & \text{if } x \in \{p, q\} \\ 0 & \text{otherwise} \end{cases}$$

We check that this particular μ satisfies all our claims. □

References

1. C. Carlet, H. Dobbertin and G. Leander: *Normal extensions of bent functions,* IEEE Transactions on Information Theory 50 (11), pp. 2880-2885, 2004.
2. Pascale Charpin: *Normal Boolean functions,* Journal of Complexity, vol. 20, Issues 2–3, pp 245–265, 2004.
3. Nicolas T. Courtois, Aidan Patrick, Matteo Abbondati: *Construction of a polynomial invariant annihilation attack of degree 7 for T-310,* To appear in Cryptologia in 2020, DOI = 10.1080/01611194.2019.1706062.
4. Nicolas T. Courtois, Matteo Abbondati, Hamy Ratoanina, and Marek Grajek: *Systematic Construction of Nonlinear Product Attacks on Block Ciphers,* In ICISC 2019, LNCS 11975, pp 20-51, Springer, 2020.
5. Lars R. Knudsen, Matthew J. B. Robshaw: *Non-Linear Characteristics in Linear Cryptoanalysis,* Eurocrypt'96, LNCS 1070, Springer, pp. 224–236, 1996.

On weak rotors, latin squares, linear algebraic representations, invariant differentials and cryptanalysis of Enigma

Nicolas T. Courtois[1] and Marek Grajek[2]

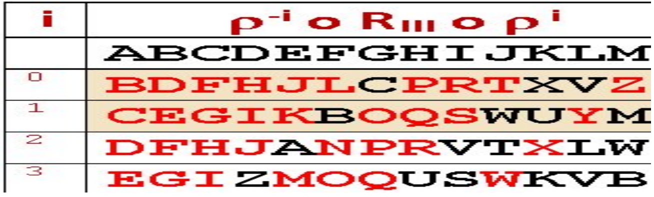
University College London, Gower Street, London, UK
Independent expert on crypto history, Grodzisk Mazowiecki, Poland

Abstract. Since 1930s until today it was assumed that Enigma rotors do not have a particular weakness or structure. A curious situation compared to hundreds of papers about S-boxes and weak setup in block ciphers. Any weak rotors with Enigma? Yes and some have strong linear and differential properties.

Keywords: Enigma · Block ciphers· Linear Cryptanalysis · Differential Cryptanalysis · Weak keys · Latin squares · Turing-Welchman attack

1 Introduction

In block ciphers the algebraic structure is relative to the vector space structure of $\mathbb{F}_2^n$ and the key will transform one affine space into another. In rotor machines the key is applied by rotation of the rotor, which corresponds to +1 mod 26 without a multi-dimensional vector space structure. A classical approach here is to study multiple "permuted alphabets" jointly. Interestingly, there are some collisions if you do so. For no real-life rotor you get a latin square, cf. p. 138-139 in [2]. In general interesting properties are those which are those which uniformly cover the whole 26^2 cases. On 1 June 1930 the Wehrmacht introduces an Enigma machine with simple (compared to other machines which already existed in 1920s) rotor movement, but with an important complication, a stecker. Surprisingly, all original rotors have remained in active use until 1945, and at least one is weak as we show here. There are $26! \approx 2^{88}$ possible wirings for one rotor. Rejewski was able to reverse recover Enigma rotors by maths. Turing also studied this in 1940 [4] his Prof's book using so called "boxes" formed by product of two involutions which can be uniquely factored back using old theorem by Rejewski. Do weak Enigma rotors exist? We construct a table of permuted alphabets. A strange order reigns for old wartime Rotor III:



i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

Not found before? In Knox/Turing work contacts had different names (losing lexicographic order). If renaming letters conceals our property, could we have a hidden permutation? Not quite. Analysis of differences would reveal the hidden permutation completely. We claim that the ONLY plausible way to get something which works for a good fraction of 26^2 cases use the full power of the ring of integers modulo 26 with both + and x. We have in fact, mixing both group operations modulo 26,

$$\rho^{-i} \circ R_{III} \circ \rho^{i}(j) \overset{?}{=} i+2\cdot j+1 = \quad \text{with A=0, B=1, etc. with } Pr = \frac{10}{26}$$

Nothing else than a **linear** approximation of an old Enigma rotor from 1929. Who says LC was invented in 1993? In the full paper we present 4 invariance theorems: our events have the same frequency in every line, every column and for every input or output letter. We also show that there is a strong correlation between on which side (< 13 or not) is the input, and numerous output letters [3]. This opens many possibilities where attacker focuses on half of the letters and guesses the position of rotor i mod 2, just one bit of information and the attacker can infer a lot of things without knowing this part of the key. It is remarkable knowing that in the first Enigma UKW-A reflector even letters are mapped to even letters with probability 11/13. Later in 1937 it became stronger: 8/13 for UKW-B. We note that unlike block ciphers, in Enigma the key translation ρ^i is applied twice, a weakness, leading to focus on invariant differential properties $k \rightarrow k$.

Could this approximation happen by accident? The probability of our property is estimated as $\binom{26}{10}\frac{15!}{26!} \approx 2^{-25}$. Rotor 3 was certainly not chosen as a random permutation. The probability to obtain a latin square is about: $(26!/26^{26})^2 \approx 2^{-67.6}$ and it is an open problem if there exist efficient algorithm for generating a rotor for Enigma uniformly at random so that this specific table becomes a latin square. We have 4 more invariance theorems: the collisions have the same frequency for every line, every column, and every I/O letter concerned. How these apply to attacks? We can design many statistical attacks combining Friedman's Index of Coincidence with our biases. Not a latin square $\Rightarrow$ each column has entropy $< log_2(26) = 4.7$ bits. Probability results show that all Engima rotors after 1938 are very close to a latin square and very far from an ideal (random) permutation. Another way is to speed up the best WW2 Turing-Welchman attack by simulating a 2 rotor Enigma combined with reflector CHEAPER with less entropy to guess. For example we get 15/26 with either $i+2j+1$ or $-3i-2j+13-1$ which are disjoint. Attack optimization shows that it is profitable to discard some ciphertext letters where approximations don't work and rather break another message with the same stecker. If we implement Rotor III by $\rho^{-i} \circ R_{III} \circ \rho^{i}(j) i+2j+b$ with variable b, entropy of b is only $2.9 \ll 4.7$ hence faster guessing step in known attacks.

Conclusion. We show that historical Enigma rotors are weaker than expected, this can improve brute force part in many major attacks on Enigma for every rotor ever made [we examined 63 rotors: German, Swiss, Italian Spanish, Norvegian etc]. In the same way as in block ciphers we show that weak keys matter – and they matter a lot for choice of the fast rotor. We need to develop a theory on how to select stronger rotors.

References

1. Mavis Batey: *Dilly Knox - A Reminiscence of this Pioneer Enigma Cryptanalyst,* In Cryptologia, Vol. 32, Iss. 2, pp. 104-130, 2008.
2. Friedrich L. Bauer: *Decrypted Secrets: Methods and Maxims of Cryptology,* 525 pages, Springer, Nov. 2006.
3. Nicolas T. Courtois: *Si seulement Enigma tournait moins vite, ou cryptanalyse d'Enigma avec un rotor faible,* Bulletin de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information, Issue number 46, Paris, France, 2020.
4. Alan Turing: *Mathematical Theory of ENIGMA Machine* , UK national archives, c. 1940.

Multipartite secret sharing revisited

Laszlo Csirmaz[*]

CECC'20, Zagreb

1 Introduction

A secret sharing scheme is *multipartite* if the participants can be grouped into (typically a few) groups such that participants in the same group play the same role. Multipartite secret sharing schemes received a considerable attention, see [2] and the references therein. Perhaps surprisingly, there are many unsolved problems even in the bipartite case. Ideal multipartite schemes are of special interest. A scheme is *ideal* if the maximal share size of the participants is the smallest possible one, namely the size of the secret, and an *access structure* describing qualified and unqualified subsets is ideal if it can be realized by an ideal scheme. Ideal bipartite and tripartite structures has been studied, among others, in [5, 2, 3].

A general method to obtain a lower bound on share sizes uses tools from information theory to keep track of information different subsets of the participants have. An access structure is *κ-ideal* if this lower bound equals the secret size. To each κ-ideal structure corresponds a *matroid* [1], and the structure is ideal (without the κ) if this matroid is representable in a certain sense.

Using this connection a comprehensive description of all κ-ideal multipartite access structures is given. In the bipartite and in the tri-partite cases the emerging matroids are linearly representable, thus we have a complete description of ideal bipartite and tripartite structures.

1.1 Schemes defined by group ranks

Let P be the set of participants which consists of m nonempty disjoint groups as $P = P_1 \cup \cdots P_m$. Participants in each group play the same role; or, put in another way, any permutation of P which maps each group P_i into itself leaves the collection of qualified subsets intact. Suppose a non-negative integer $f(I)$ is assigned to each non-empty set $I \subseteq \{1, \dots m\}$ of the groups. This number is called the *importance* or *rank* of the group. A subset $A \subseteq P$ of participants is *I-large* if for each $J \subseteq I$ there are at least a total of $f(J)$ members who are from groups in J.

Clearly, such a rank function must be non-decreasing and sub-modular: if $J \subset J'$ then $f(J) \le f(J')$ and $f(J) + f(J') \ge f(J \cap J') + f(J \cup J')$ (otherwise there is no way for a subset to be I-large).

Example 1. Suppose we have two groups $m = \{1, 2\}$, the ranks are $f(1) = a$, $f(2) = b$, and $f(12) = c$. Then a set of participants is 12-large, if it has at least a members from the first group, at least b members from the second group, and all together it has at least c members. Of course, such an arrangement is possible only if $c \le a + b$.

Example 2. If we have only one group with rank t, then 1-large subsets are those which have at least t members. This corresponds to the threshold structure.

1.2 Results

Theorem 1. *For every κ-ideal multipartite structure there is a non-decreasing and submodular ranking f of the subsets of the groups $\{1, \dots, m\}$, and (pairwise incomparable) subsets I_1, ...,*

[*] UTIA, Prague, Renyi Institute, Budapest

$I_s \subseteq \{1,\dots,m\}$ such that $A \subseteq P$ is qualified if and only if A is I_ℓ-large for some $1 \le \ell \le s$.

The converse of this theorem is also true: starting from any ranking of the group subsets and then picking $I_1, \dots, I_s \subseteq \{1,\dots,m\}$, the collection of I_ℓ-large subsets of participants determines a κ-ideal structure. For $m = 1$ this is the threshold structure, for $m = 2$ the collection $I_1, \dots I_s$ can have one elements (three possibilities) or two elements (only one possibility: $\{\{1\},\{2\}\}$), which means four different types. For $m = 3$ the description is quite lengthy and involved, but requires no new ideas.

By the next theorem for $m \le 3$ this description provides all ideal m-partite structures, giving a full characterization for these cases.

Theorem 2. *In the $m \le 3$ cases all κ-ideal structures are ideal.*

The same statement does not hold for $m = 4$ as there is a κ-ideal 4-partite structure which is not ideal.

Acknowledgments

This was a joint work with Fero Matúš and Carles Paró.

The author was supported by the GACR grant number 19-045798, and by the Lendület program of the HAS.

References

[1] E. F. Brickell and D. M. Davenport (1991), On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 6:157–168.

[2] O. Farràs, J. Martí-Farré, C. Padró (2012), Ideal Multipartite Secret Sharing Schemes, *J. Cryptology*, **25**(3), pp 434-463.

[3] O. Farràs, J. Ruth Metcalf-Burton, C. Padró, L. Vázquez (2012), On the optimization of bipartite secret sharing schemes. *Des. Codes Cryptography*, 63(2):255–271.

[4] C. Padró (2012), Lecture notes in secret sharing, *Cryptology ePrint archive*, report 2012/674

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

Discrete logarithm problem in some families of sandpile groups

K. Dsupin and Sz. Tengely

Institute of Mathematics, University of Debrecen
P. O. Box 400, 4002 Debrecen, Hungary
e-mail: krisztian.dsupin@gmail.com
e-mail: tengely@science.unideb.hu

Abstract

Finding a usable representation of a group for discrete logarithm problem (dlp) is a popular research area in cryptography. Sandpile groups of certain class of graphs were suggested for cryptosystems by Biggs in [1]. His proposal was a modification of the wheel graph, which has a special property to form a cyclic sandpile group. Blackburn in [2] and Shokrieh in [5] independently showed that the dlp in that case is efficiently solvable.

Moreover Shokrieh suggested that with the modification of his method the dlp can be also solved in non-cyclic sandpile groups. Hou, Woo and Chen introduced the C_n^2 graph in [4]. Its sandpile group is non-cyclic. Our goal is to show that with the idea mentioned above it can be solved efficiently. Furthermore using the special structure of the group, one can give parametric solution for the problem, making it even more vulnerable.

In [4] the sandpile group of C_n^2, denoted by $\mathcal{S}(C_n^2)$ is described. It is the direct sum of two or three cyclic groups depending on the parameter n, more precisely $\mathcal{S}(C_n^2) \cong \mathbb{Z}_{(n,F_n)} \oplus \mathbb{Z}_{F_n} \oplus \mathbb{Z}_{\frac{nF_n}{(n,F_n)}}$, where F_n denotes the nth Fibonacci number. Considering the Laplacian matrix of the C_n^2 graph it can be easily seen that it is a circulant matrix. Cline, Plemmons and Worm showed in [3] that the pseudoinverse of these type of matrices are also circulant. Moreover they could give a computational form for the pseudoinverse. Combining these results we can give parametric solution to the dlp based on the input factors.

Let $c_1, c_2 \in \mathcal{S}(C_n^2)$ be configurations, which are the elements of the sandpile group. The dlp can be described as the following: we are looking for a $2 \leqslant x \leqslant \operatorname{ord}(\mathcal{S}(C_n^2))$ such that $(x \cdot c_1)^\circ = c_2$, where $(x \cdot c_1)^\circ$ means the stabilization of the configuration in the group. Denote the Laplacian of $\mathcal{S}(C_n^2)$ with

$$L = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}.$$

The main steps of solving the dlp are the following:

- We can calculate the pseudoinverse, using the form given by Cline, Plemmons and Worm. Let $\mu_0, \dots, \mu_{n-1}$ the eigenvalues, ω primitive nth root of unity, λ is also an nth root of 1 in this special case, because the Laplacian L is a k-circulant matrix with $k = 1$. Keeping the notation from L, the first row of the Laplacian's pseudoinverse matrix $(b_0, \dots, b_{n-1})$ can be given by:

  $$b_i = \frac{1}{n} \sum_{j=0}^{n-1} \beta_j (\lambda \omega^j)^{-i}, \quad i = 0, 1, \dots, n-1,$$

  where

  $$\beta_j = \begin{cases} 0 & \text{if } \mu_j = 0, \\ \frac{1}{\mu_j} & \text{if } \mu_j \neq 0. \end{cases}$$

- Denote the pseudoinverse with P, the divisors of the configurations c_i with $\overline{c_i}$, the generators of the group with g_j, their divisors with $\overline{g_j}$, calculate $\overline{c_1}^T \cdot P \cdot \overline{g_j} = r_{j,1} + \mathbb{Z}$, and $\overline{c_2}^T \cdot P \cdot \overline{g_j} = r_{j,2} + \mathbb{Z}$.

- Solve the Diophantine equations $r_{j,2} = r_{j,1}x + y$. Using the Chinese remainder theorem we get x (mod $\mathrm{ord}(\mathcal{S}(C_n^2))$).

Following Shokrieh's idea we extended his method to non-cyclic sandpile groups. If we know the generators of the group, then we can provide parametric solutions.

References

[1] N. Biggs. "The critical group from a cryptographic perspective". In: *Bulletin of the London Mathematical Society* 39 (Aug. 2007). DOI: 10.1112/blms/bdm070.

[2] S. Blackburn. "Cryptanalysing the critical group: Efficiently solving Biggs's discrete logarithm problem". In: *Journal of Mathematical Cryptology* 3 (2009). See http://eprint.iacr.org/2008/170, pp. 199–203. ISSN: 1862-2976.

[3] R.E. Cline, R.J. Plemmons, and G. Worm. "Generalized inverses of certain Toeplitz matrices". In: *Linear Algebra and its Applications* 8.1 (1974), pp. 25–33. ISSN: 0024-3795. DOI: https://doi.org/10.1016/0024-3795(74)90004-4. URL: http://www.sciencedirect.com/science/article/pii/0024379574900044.

[4] Y. Hou, C. Woo, and P. Chen. "On the sandpile group of the square cycle C_n^2". In: *Linear Algebra and its Applications* 418 (Oct. 2006), pp. 457–467. DOI: 10.1016/j.laa.2006.02.022.

[5] F. Shokrieh. "The monodromy pairing and discrete logarithm on the Jacobian of finite graphs". In: *Journal of Mathematical Cryptology* 4 (July 2009). DOI: 10.1515/JMC.2010.002.

Keywords: discrete logarithm problem, sandpile group, critical group

Cryptanalysis of ITRU

H. R. Hashim, A. Molnár and Sz. Tengely

Institute of Mathematics, University of Debrecen
P. O. Box 400, 4002 Debrecen, Hungary
e-mail: hashim.hayder.raheem@science.unideb.hu
e-mail: alexandra980312@freemail.hu
e-mail: tengely@science.unideb.hu

Abstract

In 1996, Hoffstein, Pipher and Silverman [4] proposed a class of fast public key cryptosystems called NTRU (N^{th} degree Truncated Polynomial Ring) cryptosystem, which was published in 1998. This cryptosystem is considered as a lattice-based public key cryptosystem, and it is the first asymmetric cryptosystem based on the polynomial ring $\frac{\mathbb{Z}[X]}{(X^N-1)}$. Indeed, it has very good features comparing to other public key cryptosystems such as reasonably short, easily created keys, high speed, and low memory requirements. Its encryption and decryption procedures rely on a mixing system presented by polynomial algebra combined with a clustering principle based on elementary probability theory. From its lattice-based structure, the security of the NTRU cryptosystem is based on the hardness of solving the Closest Vector Problem (CVP), which is a computational problem on lattices closely related to Shortest Vector Problem (SVP) and considered to be NP hard (non-deterministic polynomial-time hardness) (for more details, see [5] and the references given there).

One of the known variants of NTRU cryptosystem called ITRU cryptosystem, which was presented in 2017 by Gaithuru, Salleh, and Mohamad [3]. Instead of working in a truncated polynomial ring, ITRU cryptosystem is based on the ring of integers. The parameters and the main steps of ITRU cryptosystem are as follows.

- □ The value of p is the small modulus (an integer).
- □ Random integers f, g and r are chosen such that f is invertible modulo p.
- □ A prime q is fixed satisfying $q > p \cdot r \cdot g + f \cdot m$, where m is the representation of the message in decimal form. The suggested conversion is based on *ASCII* conversion tables, that is the one with $a \to 97$.
- □ One computes $F_p \equiv f^{-1} \pmod{p}$ and $F_q \equiv f^{-1} \pmod{q}$. These computations can be done by using the extended Euclidean algorithm.

- □ The public key is consisted of h and q such that $h \equiv p \cdot F_q \cdot g \pmod{q}$.
- □ The encryption procedure is similar to the one applied in NTRU cryptosystem [4], one generates a random integer r and computes $e \equiv r \cdot h + m \pmod{q}$.
- □ To get the plaintext from the ciphertext one determines $a \equiv f \cdot e \pmod{q}$.
- □ Recovering the message is done by computing $F_p \cdot a \pmod{p}$.

The authors claimed that ITRU has better features comparing to the classical NTRU, such as having a simple parameter selection algorithm, invertibility, and successful message decryption, and better security.

In this paper, we present an attack technique against the ITRU cryptosystem, it is mainly based on a simple frequency analysis. As a result, this techniques will recover the corresponding plaintexts immediately with no need of having the private keys. The attack is via eavesdropping on some encrypted messages. If the message is too short, then the attack may fail. Moreover, according to the index of coincidence introduced by Friedman [1] the language of the plaintext may be identified (e.g. in case of English it is about 0.0686). Therefore, once we identify the language correctly, then the frequency analysis works very well in practice. Friedman [2] claimed that 'practically every example of 25 or more characters representing monoalphabetic encipherment of a "sensible" message in English can be readily solved.' In case of ITRU careful parameter selection may yield a few groups (that can be identified) for which frequency analysis can be applied.

References

[1] W. F. Friedman. *The index of coincidence and its applications in cryptography.* Department of Ciphers. Publ 22. Geneva, Illinois, USA: Riverbank Laboratories, 1922.

[2] W. F. Friedman. Codes and ciphers (cryptology). *Encyclopaedia Britannica*, pages 1–8, 1956.

[3] J. N. Gaithuru, M. Salleh, and I. Mohamad. ITRU: NTRU-Based Cryptosystem Using Ring of Integers. *International Journal of Innovative Computing*, 7(1), 2017.

[4] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic number theory. 3rd international symposium, ANTS-III, Portland, OR, USA, June 21–25, 1998. Proceedings*, pages 267–288. Berlin: Springer, 1998.

[5] D. Micciancio. *Closest Vector Problem*, pages 79–80. Springer US, Boston, MA, 2005.

Keywords: NTRU, ITRU

An algorithm for optimal joint expansion with odd digits

Clemens Heuberger[1] and Dunja Pucher[2], University of Klagenfurt[3]

Abstract. Joint expansions of vectors are used to improve the efficiency of the calculation of linear combinations of points of elliptic curves. We consider radix-2 joint expansions for pairs of integers and for the digit sets containing consecutive odd digits. More specifically, we give a right-to-left algorithm which builds minimal weight representations for the digit set $D = \{0, \pm 1, \pm 3\}$ and prove its optimality.

Keywords. Elliptic curve cryptography, double and add method, low-weight digit expansions.

Motivation

The security of cryptographic algorithms relies on efficient one-way functions. In our work we consider the computation of multiples and linear combinations in an Abelian group, which is an essential operation in several elliptic curve-based cryptosystems. We are interested in an efficient implementation of the considered one-way function, because this allows to increase the parameters and thus the security of the cryptosystem.

For a given positive integer n and a point P, the standard method to compute a multiple nP is the binary method—based on the binary expansion of the integer n, the calculation of nP is done with the double and add method. A naive way to compute a linear combination of two points $nP + mQ$ is to simply perform two single point multiplications. However, a more efficient method is to compute a linear combination simultaneously. This can be done by representing the integers m and n as a joint expansion and by using the Straus algorithm, which is based on the fact that the point $P + Q$ can be precomputed and added when the considered vector of the joint expansion equals $\frac{1}{1}$, thus reducing the number of needed additions.

Generally, any reduction of the number of the needed additions improves the efficiency. Still, using the standard binary expansions, i.e. the digit set $\{0, 1\}$, further improvements are not possible. A way to overcome this problem is to introduce other digits in the digit set and to increase the number of zero vectors, i.e. to reduce the joint Hamming weight of the expansions. Since in elliptic curve groups a point subtraction is computationally as expensive as a point addition, this implies that negative digits may also be introduced. However, this leads to redundant number systems. Determining a unique and/or optimal joint expansion as well as the asymptotical analysis of the minimal weights are the main tasks.

Low-weight digit expansions with odd digits

The first algorithm for computing a low-weight digit expansion was given in 2001 [1], and that for the digit set $D = \{0, \pm 1\}$ and dimension $d = 2$, and with the outputs which fulfil predefined syntactic constraints—the so called Joint Sparse Form (JSF). It was shown that every pair of integers m and n has a unique JSF, and that the expected joint Hamming weight among all JSF expansions of length ℓ is asymptotically equal to $1/2\ell$. Compared to the joint binary expansions, where the expected joint Hamming weight is asymptotically equal to $3/4\ell$, this was a considerable improvement. A generalization of the JSF to arbitrary dimensions $d \geq 2$, the so called Simple Joint Sparse Form (SJSF), was given in 2004 [2].

When other odd digits are introduced, the previously considered syntactic restrictions can no longer enforce that a pair of integers admits a unique such expansion, and this changes the situation significantly. An optimal algorithm for other digit sets with odd digits is not given yet. Nevertheless, several authors have investigated asymptotical behavior of the minimal weights and have calculated optimal weights for various digit sets and dimensions. Therefore, for certain digit sets with odd digits it is already known which optimal average weight algorithms should have. However, for these digit sets one can find approximation algorithms, which have a certain offset to the minimal average weight.

[1] clemens.heuberger@aau.at

[2] dupucher@edu.aau.at

[3] The authors are supported by the Austrian Science Fund (FWF): P 28466-N35

Our contribution

We consider the digit set $D = \{0, \pm 1, \pm 3\}$ and construct a right-to-left algorithm which outputs radix-2 joint representations with the digits from the set D for arbitrary pairs of integers.

Our goal is to define a function which chooses the digits of the least significant column in such way, that the number of non-zero columns is minimal. For this purpose we investigate which choices we have based on the given digit set. If a given integer is even, there is always only one digit which can be chosen, and that is the digit 0. But in the case when the given integer is odd, any of the odd digits from the set D can be chosen. Since we have four consecutive odd digits, we know that the digit set contains a representative for all odd residue classes modulo 2^3. Based on this observation, we define so called setting functions—functions which choose a digit $d \in D$ based on the predefined, wanted congruence modulo 2^3.

However, the definition of the wanted congruence modulo 2^3 may not be instantly obvious. Here we note that different choices may lead to different minimal joint representations. A very simple example are integers 5 and 7. Representing digits -1 and -3 as $\overline{1}$ and $\overline{3}$, we have that $\binom{5}{7} = \binom{13}{31}_2 = \binom{101}{103}_2 = \binom{100\overline{3}}{100\overline{1}}_2$, and note that all expansions have (minimal) joint Hamming weight of 2.

Therefore, we have to choose additional syntactic constraints which on the one hand guarantee that every vector has a unique expansion and on the other hand lead to minimal expansions.

Altogether, we define the function for selecting the most suitable digits by modelling cases based on the parities of the given integers. The most challenging case appears when the given integers have different parities, since a selection of the digit is not always unique. Using the digits from the given set D we construct a so called virtually enlarged digit set D_{new}—a set which contains a representative for all odd residue classes modulo 2^4, and which enables us to calculate possible alternatives more efficiently and reduces the decision problem.

Results

For the given integers m and n and the digit set $D = \{0, \pm 1, \pm 3\}$ we show that

- the outputs of the algorithm fulfil predefined syntactic constraints,
- the algorithm terminates, and
- the necessary look-ahead for an optimal selection of the digits from the digit set D which form A_s, the least significant column of a joint expansion of a pair of integers, is 7.

Furthermore, we prove the optimality of the algorithm. We show that

- the expected weight of an expansion of length ℓ is asymptotically equal to $281/786\ell$, and
- the outputs of the algorithm are minimal weight joint expansions.

With regard to complexity, the algorithm needs precomputation of 12 points on the curve. Compared with [1], where 2 points need to be precomputed, this requires 10 additional curve operations. However, as the expected weight decreases from 0.5ℓ to approximately 0.36ℓ, this means that the costs for the precomputation are offset after 71 bit. Note that if using the same cryptosystem several times, precomputation is required only once. The overhead of the integer operations to compute the expansion seems to be negligible.

References

[1] Jerome A. Solinas. Low-weight Binary Representations for Pairs of Integers. Technical report, University of Waterloo, 2001, URL http://cacr.uwaterloo.ca/techreports/2001/corr2001-41.ps, accessed 29.09.2019.

[2] Peter J. Grabner, Clemens Heuberger, and Helmut Prodinger. Distribution results for low-weight binary representations for pairs of integers. *Theoretical Computer Science*, 319:307–331, 2004.

Encryption scheme based on the extension of automorphism group of the Hermitian function field

Gennady Khalimov
Kharkiv National University of Radioelectronics
Kharkiv, Ukraine
hennadii.khalimov@nure.ua

Yevgen Kotukh
University of Customs and Finance
Dnipro, Ukraine
yevgenkotukh@gmail.com

Svitlana Khalimova
Kharkiv National University of Radioelectronics
Kharkiv, Ukraine
svitlana.khalimova@nure.ua

Abstract. *The article describes a new implementation of MST3 cryptosystems based on the automorphism group extension of the Hermitian function field.*

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

INTRODUCTION

Development of efficient cryptographic cryptosystems that can withstand quantum attacks has become an actual problem. The idea of constructing public-key cryptosystems on the basis of the intractable word problem was proposed by Wagner and Magyarik in [1]. The basis is the use of permutation groups. Since the 2000s, several dozen group cryptosystems schemes have been proposed [2,3].

Magliveras proposed a practical implementation of Wagner's and Magyarik's idea [4]. He proposed a symmetric cryptosystem based on a special type of finite groups factorization called logarithmic signatures for finite permutation groups. Further improvements to this scheme were made by Svaba and van Trung in [5]. They introduced a secret cover of a random cover. The Magliveras cryptosystem has several improvements and the last option proposed based on the Suzuki group is known as MST3 [6]. In this paper, MST3 cryptosystems based on the automorphism group extension of the Hermitian function field will be presented.

The automorphism group $A(P_\infty)$ of the Hermitian function field $H|F_{q^2}$ acting on it as $\sigma(x),\sigma(y)$ has a greater $ordA(P_\infty)=q^3(q^2-1)$ than the orders of the other automorphism groups [7-9]. The order group $A(P_\infty)$ also greater than the order of corresponding Suzuki group. Suzuki groups, which appear in MST3 cryptosystems, are isomorphic to the projective linear group $PGL(3,F_q)$, where $q=2q_0^2$, $q_0=2^n$ and has order q^2. A larger group order gives an advantage to cryptosystem secrecy.

I. PROPOSAL

From the general results of MST3 construction we assume that advantage is given to the group $A(P_\infty)$ based on the automorphism $\sigma(x),\sigma(y)$.

Each element of $A(P_\infty)$ can be expressed uniquely

$$A(P_\infty)=\left\{S(a,b,c)\middle| a\in F_{q^2}^*:=F_{q^2}\setminus\{0\},b\in F_{q^2},c^q+c=b^{q+1}\right\}$$

where

$$S(a,b,c)=[a,b,c]$$

and the group operation is defined as

$$S(a_1,b_1,c_1)\cdot S(a_2,b_2,c_2)=S\left(a_1a_2,a_2b_1+b_2,a_2^{q+1}c_1+a_2b_2^qb_1+c_2\right),$$

the inverse of $S(a,b,c)$ is

$$S(a,b,c)^{-1}=S\left(a^{-1},-a^{-1}b,a^{-(q+1)}c^q\right) \text{ [8]}.$$

It is simple to show by direct calculations.

The identity is the triple $S(1,0,0)$.

It follows that $|A(P_\infty)|=q^3(q^2-1)$.

The center $Z(A(P_\infty))=\left\{S(1,0,c)\middle| c^q+c=0,c\in F_{q^2}\right\}$ and $|Z(A(P_\infty))|=q$.

Construction of the group elements $A(P_\infty)$ is determined by solving the equation $c^q+c=b^{q+1}$ with respect to c. The difficulty of finding c is proportional to q. We have considered two encryption schemes that overcome this problem.

Let F_{q^2} be a field of odd characteristic.

For an odd characteristic field, the automorphism group $A(P_\infty)$ of the Hermitian function field has the representation

$$A(P_\infty)=\left\{\left[a,b,\frac{b^{q+1}}{2}+c\right]\middle| a\in F_{q^2}^*,b\in F_{q^2} \quad and \quad c^q+c=0\right\}.$$

If γ is a generating element of the field, then the equation $c^q+c=0$ has solutions $c_i=\gamma^{(q+1)/2+i(q+1)}$, $i=0,1,...q-1$. Computation vectors using logarithmic signature matrices and random covers are now easily transcoded into the coordinates b,c of the $A(P_\infty)$ subgroup.

The group operation is defined as

$$S(a_1,b_1,c_1)\cdot S(a_2,b_2,c_2)=$$

$$S\left(a_1a_2,a_2b_1+b_2,a_2^{q+1}\left(b_1^{q+1}/2+c_1\right)+a_2b_2^qb_1+b_2^{q+1}/2+c_2\right)$$

and the inverse of $S(a,b,c)$ is

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

Key Generation

Input: a large group on the field of odd characteristic

$$A(P_\infty) = \left\{S(a,b,c) \middle| a \in F^{*}_{q^2} := F_{q^2} \setminus \{0\}, b \in F_{q^2}, c^q + c = 0\right\}$$

Output: a public key $[\alpha, \gamma, f]$ with corresponding private key $[\beta, (t_0, ..., t_s)]$.

Choose a first tame logarithmic signature $\beta_{(1)} = [B_{1(1)}, ..., B_{s(1)}] = (b_{ij})_{(1)} = S(1, b_{ij(1)}, b_{ij(1)}^{q+1}/2)$ of type $(r_{1(1)}, ..., r_{s(1)})$, $i = \overline{1, s(1)}$, $j = \overline{1, r_{i(1)}}$, $b_{ij(1)} \in F_{q^2}$.

Choose a second tame logarithmic signature $\beta_{(2)} = [B_{1(2)}, ..., B_{s(2)}] = (b_{ij})_{(2)} = S(1, 0, b_{ij(2)})$ of type $(r_{1(2)}, ..., r_{\mathrm{s}(2)})$, $i = \overline{1, s(2)}$, $j = \overline{1, r_{i(2)}}$, $b_{ij(2)} \in F_q \subset F_{q^2}$.

Select a first random cover $\alpha_{(1)} = [A_{1(1)}, ..., A_{s(1)}] = (a_{ij})_{(1)} = S\left(a_{ij(1)_1}, a_{ij(1)_2}, (a_{ij(1)_2})^{q+1}/2\right)$ of the same type as $\beta_{(1)}$, where $a_{ij} \in A(P_\infty)$, $a_{ij(1)_1}, a_{ij(1)_2} \in F_{q^2} \setminus \{0\}$.

Select a second random cover $\alpha_{(2)} = [A_{1(2)}, ..., A_{s(2)}] = (a_{ij})_{(2)} =$ $S\left(1, a_{ij(2)_2}, (a_{ij(2)_2})^{q+1}/2 + a_{ij(2)_3}\right)$ of the same type as $\beta_{(2)}$, where $a_{ij(2)_2}, a_{ij(2)_3} \in F_q \setminus \{0\} \subset F_{q^2}$.

Choose $t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in A(P_\infty) \setminus Z$, $t_{i(k)} = S\left(t_{i(k)_1}, t_{i(k)_2}, (t_{i(k)_2})^{q+1}/2\right)$, $t_{i(\mathrm{k})_j} \in F^{\times}$, $i = \overline{0, s(\mathrm{k})}$, $j = \overline{1,2}$, $k = \overline{1,2}$. Let's $t_{\mathrm{s}(1)} = t_{0(2)}$.

Construct a homomorphism f_1 defined by $f_1\left(S\left(a_1, a_2, a_2^{q+1}/2\right)\right) = S\left(1, a_1, a_1^{q+1}/2\right)$.

Let's do the following calculations $\gamma_{(1)} = [h_{1(1)}, ..., h_{s(1)}] = (h_{ij})_{(1)} = t^{-1}_{(i-1)(1)} f\left((a_{ij})_{(1)}\right)(b_{ij})_{(1)} t_{i(1)}$, $i = \overline{1, s(1)}$, $j = \overline{1, r_i}$,
where
$f\left((a_{ij})_{(1)}\right)(b_{ij})_{(1)} =$
$S\left(1, a_{ij(1)_1} + b_{ij(1)}, a_{ij(1)_1}^{q+1}/2 + a_{ij(1)_1} b_{ij(1)}^{q} + b_{ij(1)}^{q+1}/2\right)$,
And define a homomorphism f_2

$$f_2\left(S\left(1, a_2, a_2^{q+1}/2\right)\right) = S(1, 0, a_2).$$

Compute

$\gamma_{(2)} = [h_{1(2)}, ..., h_{s(2)}] = (h_{ij})_{(2)} = t^{-1}_{(i-1)(2)} f\left((a_{ij})_{(2)}\right)(b_{ij})_{(2)} t_{i(2)}$, $i = \overline{1, s(2)}$, $j = \overline{1, r_i}$,
where

$$f\left((a_{ij})_{(2)}\right)(b_{ij})_{(2)} = S\left(1, 0, a_{ij(2)_2} + b_{ij(2)}\right).$$

An output public key $[f_1, f_2, (\alpha_k, \gamma_k)]$, and a private key $[\beta_{(k)}, (t_{0(k)}, ..., t_{s(k)})]$, $k = \overline{1,2}$.

Encryption

Input: a message $m \in A(P_\infty)$, $m = S(1, m_2, m_3)$, $m_2 \in F_{q^2}$, $m_3 \in F_q \subset F_{q^2}$ and the public key $[f_1, f_2, (\alpha_k, \gamma_k)]$, $k = \overline{1,2}$.

Output: a ciphertext (y_1, y_2, y_3) of the message m.

Choose a random $R = (R_1, R_2)$, $R_1 \in Z_{|F_{q^2}|}$, $R_2 \in Z_{|Z|}$.

Compute

$$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_1) \cdot \alpha_2'(R_2) \cdot m$$
$$= S\left(a_{(1)_1}(R_1), a_{(1)_2}(R_1) + a_{(2)_2}(R_2), a_{(1)_2}(R_1)^{q+1}/2 + \right.$$
$$\left. a_{(1)_2}(R_1) a_{(2)_2}(R_2)^q + a_{(2)_2}(R_2)^q/2 + a_{(2)_3}(R_2)\right) \cdot m$$
$$= S\left(a_{(1)_1}(R_1), a_{(1)_2}(R_1) + a_{(2)_2}(R_2) + m_2, \right.$$
$$\left. \left(a_{(1)_2}(R_1) + a_{(2)_2}(R_2)\right) m_2^{q} + m_2^{q+1}/2 + m_3 + *\right)$$

The components of $(*)$ in the formula are determined by cross-calculations in the group operation of the product.

Compute

$$y_2 = \gamma'(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2)$$
$$= S\left(*, a_{(1)_1}(R_1) + \beta_{(1)}(R_1) + *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right).$$

Here, the $(*)$ components are determined by cross-calculations in the group operation of the product of $t_{0(k)}, ..., t_{s(k)}$ and for third coordinate is added the product of $a_{(1)_1}(R_1) + \beta_{(1)}(R_1)$.

Compute

$$y_3 = f\left(\alpha_2'(R_2)\right) = S\left(1, 0, a_{(2)_2}(R_2)\right).$$

Output (y_1, y_2, y_3).

Decryption

Input: a ciphertext (y_1, y_2, y_3) and private key $[\beta_{(k)}, (t_{0(k)}, ..., t_{s(k)})]$, $k = \overline{1,2}$.

Output: the message $m \in A(P_\infty)$ corresponding to ciphertext (y_1, y_2, y_3).

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

The parameter $a_{(1)_1}(R_1)$ is known from the y_3 and it is included in the second component of y_2.

Compute

$$D^{(1)}(R_1, R_2) = t_{0(1)} \cdot y_2 t^{-1}_{s(2)}$$
$$= S\left(1, a_{(1)_1}(R_1) + \beta_{(1)}(R_1), \right.$$
$$\left. a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + \left(a_{(1)_1}(R_1) + \beta_{(1)}(R_1)\right)^{q+1}/2 + *\right).$$

and

$$D^*(R) = f(y_1)^{-1} D^{(1)}(R_1, R_2) = S\big(1, a_{(1)_1}(R_1),$$
$$a_{(1)_2}(R_1)^{g+1}/2\big) S\Big(1, a_{(1)_1}(R_1) + \beta_{(1)}(R_1),$$
$$a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + \big(a_{(1)_1}(R_1) + \beta_{(1)}(R_1)\big)^{q+1}/2 + *\Big)$$
$$= S\big(1, \beta_{(1)}(R_1), a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\big).$$

Restore R_1 with $\beta_{(1)}(R_1)$ using $\beta_{(1)}(R_1)^{-1}$, because β is simple.

For further calculation, it is necessary to remove the component of the array $\gamma_1'(R_1)$ from y_2.

Compute

$$y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2)$$
$$= S\big(*, *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\big).$$

Repeat the calculations

$$D^{(2)}(R_2) = t_{0(2)} \cdot y_2 t_{s(2)}^{-1} = S\big(1, 0, a_{(2)_2}(R_2) + \beta_{(2)}(R_2)\big)$$

and

$$D^*(R) = D^{(2)}(R_2) y_3^{-1} =$$
$$D^{(2)}(R_2) S\big(1, 0, a_{(2)_2}(R_2)\big)^{-1} = S\big(1, 0, \beta_{(2)}(R_2)\big)$$

Restore R_2 with $\beta_{(2)}(R_2)$ using $\beta_{(2)}(R_2)^{-1}$.

We obtain the recovery of $R = (R_I, R_2)$ and the message m from y_1

$$m = \alpha'(R_1, R_2)^{-1} \cdot y_1$$

Security Analysis

Since β is tame, the adversary can use a forgery secret key $\left[\beta_{(k)}, \left(t_{0(k)}, \ldots, t_{s(k)}\right)\right]$ to recover the random numbers $R = (R_1, R_2)$. A simple search of parameters R_1, R_2 leads to brute force attack with complexity q^3. The attack using selection in the center of the group is considered in [9]. The complexity estimate is determined by the center power for the automorphism group, which is q^3. Since the automorphism group $A(P_\infty)$ of the Hermitian function field is defined over a large field F_{q^2}, the attack is not computationally feasible.

II. Conclusions

The implementation of a cryptosystem on the automorphism group $A(P_\infty)$ of the Hermitian function field requires the construction of a logarithmic signature β on the vectors whose bases are determined by the characteristic of the quadratic field. The logarithmic signature $\beta = [B_1, \ldots, B_s] = (b_{ij}) = S\left(1, b_{(ij)\cdot b}, b_{(ij)\cdot c}\right)$ from a subgroup of the $A(P_\infty) = \left\{S(a,b,c) \middle| a, b \in F_{q^2}, c^q + c = b^{q+1}\right\}$. This is also true for a random cover $\alpha = [A_1, \ldots, A_s] = (a_{ij}) = S\left(a_{(ij)\cdot a}, a_{(ij)\cdot b}, a_{(ij)\cdot c}\right)$ of the same type as β. The size of the arrays β and α is determined by the type $(r_1, \ldots, r_s)_b$ and $(r_1, \ldots, r_s)_c$ for coordinates b, c for the subgroups of the $A(P_\infty)$. Thus, an important task is to convert the logarithmic signatures and random covers to the group elements.

A solution of this problem is possible for the field of odd characteristic and on the extension of the automorphism group. For an odd characteristic field, the automorphism group $A(P_\infty)$ of the Hermitian function field has a simple representation. Computation vectors using logarithmic signature matrices and random covers are now easily transcoded into the coordinates of the $A(P_\infty)$ subgroup.

The latter solution based on the extension of the automorphism group provides for a larger group. The message size for encryption is q^3 times larger than in the MST3 cryptosystem on the Suzuki group.

References

[1] N.R. Wagner and M.R. Magyarik, "A public-key cryptosystem based on the word problem", Proc. Advances in Cryptology – CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.

[2] K.H. Ko, S.J. Lee, J.H .Cheon, J.W .Han, J. Kang, and C. Park, "New public-key cryptosystem using braid groups", in Advances in cryptology—CRYPTO 2000 ,vol.1880of Lecture Notes in Computer Science , pp. 166–183, Springer, Berlin, Germany, 2000.

[3] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings", Groups, Complexity, and Cryptology ,vol.5,no.1,pp.97–115,2013.

[4] 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.

[5] S.S. Magliveras, P. Svaba, T. Van Trung, and P. Zajac, "On the security of a realization of cryptosystem MST3", Tatra Mountains Mathematical Publications, vol.41, pp.65–78, 2008.

[6] 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), pp.62–74.

[7] H.Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik" I, II, Arch. Math. 24, pp.524–544 and pp.615–631, 1973.

[8] A. Garcia, H. Stichtenoth, C.-P.Xing, "On Subfields of the Hermitian Function Field", Kluwer Academic Publishers, Compositio Mathematica 120: pp.137–170, 2000.

[9] Algebraic Curves and Finite Fields: Cryptography and Other Applications. Edited by Harald Niederreiter, Alina Ostafe, Daniel Panario, Arne Winterhof, Walter de Gruyter GmbH & Co KG, P.251, 2014.

Hierarchical and Dynamic Threshold Paillier Cryptosystem without Trusted Dealer

Andreas Klinger[1], Stefan Wüller[1], Giulia Traverso[2], and Ulrike Meyer[1] *

[1] RWTH Aachen University, Templergraben 55, 52062 Aachen, Germany,
{klinger,wueller,meyer}@itsec.rwth-aachen.de
[2] Technische Universität Darmstadt, Karolinenplatz 5, 64289 Darmstadt, Germany,
gtraverso@cdc.informatik.tu-darmstadt.de

The use of homomorphic threshold cryptosystems for distributed computing on encrypted data has been proposed for various application areas, e. g., for double auction in [2], for privacy preserving data mining in [8], or for data integration and sharing in [3]. In these cryptosystems, the access structure underlying the sharing of the private key between the shareholders is typically assumed to be a fixed flat access structure requiring a minimum number t of n equally powerful shareholders to cooperate during decryption. Many of these use cases could profit from supporting more complex access structures, such as hierarchical access structures, in which each shareholder is associated with a certain level in a hierarchy, as well as supporting dynamicity, such that shareholders may join or leave. A homomorphic cryptosystem with both properties is applicable in many scenarios, among others, online auctions where bidders join at different points in time, or server aided secure multi-party computation. In particular, hierarchical access structures often better reflect the structure within an organization or between different cooperating organizations, and are also well suited for certain functionalities such as adding auditing to distributed computation on encrypted data. Dynamic systems on the other hand allow for reusing previously computed ciphertexts even if shareholders join or leave.

In the past, many (t, n) threshold encryption schemes have been proposed (e. g., as [1, 4–7, 10]). Some of these cryptosystems are homomorphic (e. g., as [4, 7]), others are dynamic (e. g., as [5, 6]), and yet others support hierarchical access structures (e. g., as [1, 10]). However, none of these schemes supports all three properties simultaneously. Straight forward constructions of a dynamic and hierarchical secret sharing scheme from Shamir's Secret Sharing scheme either require the threshold to be adapted continuously or would enable a subset of shareholders to prevent decryption. Recently, a dynamic and hierarchical secret sharing scheme based on Birkhoff interpolation has been proposed [11] that does not exhibit such disadvantages. However, a threshold cryptosystem that uses this secret sharing scheme has not been proposed yet.

We propose the first hierarchical and dynamic threshold Paillier cryptosystem without trusted dealer and prove its security in the malicious adversary model. Nishide and Sakurai proposed a fully distributed threshold Paillier cryptosystem [9] where the public and private key are generated without a trusted dealer, such that the private key is shared with a verifiable (t, n) threshold secret sharing scheme over the integers [9]. We show how to modify the threshold Paillier cryptosystem of [9] in order to obtain a cryptosystem with hierarchical access structure that allows adding and removing shareholders.

To this end, we developed a verifiable hierarchical and dynamic secret sharing scheme that can share a secret over the integers. The new secret sharing scheme combines the verifiable (t, n) threshold sharing scheme over the integers proposed in [9] with the dynamic and verifiable hierarchical secret sharing scheme proposed in [11]. Our novel system allows without secret reconstruction to add new shareholders and reset the access structure,

* This work is supported by the German research council (DFG) Research Training Group 2236 UnRAVeL.

i. e., switch between different access structures. We prove its security in the presence of a malicious adversary corrupting only unauthorized sets of shareholders.

We develop a hierarchical and dynamic threshold Paillier cryptosystem without trusted dealer. Here, we leverage the fact that a flat (t, n) threshold access structure is equivalent to a hierarchical access structure with one level and modify the key generation of the threshold Paillier cryptosystem without trusted dealer proposed in [9] such that the verifiable (t, n) threshold secret sharing scheme [9] becomes a special case of our novel hierarchical and dynamic secret sharing scheme over the integers. In a finalizing step, we then transform the shares of the private key shared with the verifiable (t, n) secret sharing scheme over the integers [9] into our verifiable hierarchical and dynamic secret sharing scheme over the integers. We show that the resulting system is able to cope with mobile adversaries if the access structure is reset in regular intervals. The second challenge we address is the development of a new decryption algorithm in order to cover the hierarchical structure.

The threshold Paillier cryptosystem [9] and our novel system are both probabilistic, as they first generate two prime candidates, check their primality, and if the check fails restart, e. g., x times. The total complexity w. r. t. computation (number of modular exponentiations) and communication (number of messages exchanged) of both systems is $\mathcal{O}\left(xn^2\right)$. For k-bit primes and a security parameter K such that $\frac{1}{K}$ is negligible, the share sizes are bound by $2^{4k+6}tn^{t+7}\Delta^2K^3$, whith $\Delta := n!$ for the threshold Paillier cryptosystem [9], and $\Delta := \mathrm{lcm}(\mathrm{A})$ for our system where $\mathrm{A} \leq 2^{2-t} \cdot (t-1)^{\frac{t-1}{2}} \cdot (t-1)! \cdot n^{\frac{t^2-3t+2}{2}}$ is the largest possible reconstruction matrix for the Birkhoff interpolation and where additionally k has to be chosen such that $k > \log_2(\mathrm{A})$.

Our new hierarchical and dynamic threshold Paillier cryptosystem without trusted dealer allows to dynamically add and remove shareholders while providing a hierarchical access structure. We show that the new cryptosystem is correct, robust and threshold semantic secure in the presence of a probabilistic polynomial time bound malicious adversary corrupting only unauthorized sets of shareholders. The techniques presented here can also be used in cryptosystems where the private key can be shared additively, e. g., RSA.

References

1. Akl, S.G., Taylor, P.D.: Cryptographic Solution to a Problem of Access Control in a Hierarchy. ACM Trans. Comput. Syst. **1**(3), 239–248 (1983)
2. Bogetoft et al.: Secure Multiparty Computation Goes Live. In: Financial Cryptography and Data Security. LNCS, Springer (2009)
3. Clifton et al.: Privacy-preserving data integration and sharing. In: DMKD. ACM Press (2004)
4. Cramer et al.: Multiparty Computation from Threshold Homomorphic Encryption. In: EUROCRYPT. LNCS, Springer (2001)
5. Gennaro et al.: Threshold RSA for Dynamic and Ad-Hoc Groups. In: EUROCRYPT. LNCS, Springer (2008)
6. Ghodosi et al.: Dynamic Threshold Cryptosystems (A New Scheme in Group Oriented Cryptography). PRAGOCRYPT (1996)
7. Grigoriev et al.: Homomorphic Public-Key Cryptosystems and Encrypting Boolean Circuits. AAECC (2006)
8. Mendes, R., Vilela, J.P.: Privacy-Preserving Data Mining: Methods, Metrics, and Applications. IEEE Access **5**, 10562–10582 (2017)
9. Nishide, T., Sakurai, K.: Distributed Paillier Cryptosystem without Trusted Dealer. In: ISA. LNCS, Springer (2010)
10. Pakniat et al.: Distributed key generation protocol with hierarchical threshold access structure. IET Information Security (2015)
11. Traverso et al.: Dynamic and Verifiable Hierarchical Secret Sharing. In: ITS. LNCS, Springer (2016)

Security of Poseidon Hash Function Against Linear and Differential Attacks with Respect to Field Operations

Lyudmila Kovalchuk[1,2], Mariia Rodinko[1,3], and Roman Oliynykov[1,3]

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

Introduction. One of the most important problems arising in construction of SNARK-proofs and STARK-proofs [3, 6, 10] is reduction of the number of constraints describing algorithms of the respective SNARK-system. Hash function is a necessary element of each SNARK-system. For this reason, we need to construct a hash function such as its description would require as few constraints as possible.

One of the first hash functions proposed to be used in SNARK-proofs was the Pedersen function [8]. However, the number of constraints for its description is quite large (approximately 1.68 constraints per bit), and as a result the SNARK-proof using this function works too long. The Poseidon hash function proposed in [4] appeared to be a quite good construction with respect to the number of constraints. For this function, the number of constraints is up to 15 times smaller than for the Pedersen hash function.

To enable using this function in SNARK-systems, it is necessary to provide a full substantiation of its security against the main applicable cryptographic attacks. The Poseidon hash function is based upon the SPONGE construction [7] that uses the HADES block cipher algorithm [5] as the inner permutation. For this reason, the main part of the security substantiation for the Poseidon hash function is to show that the HADES algorithm is indistinguishable from a random permutation [4, 7].

The authors of the HADES algorithm, and later the authors of the Poseidon hash function present detailed argumentation claiming security of these constructions against some class of attacks that they named ”algebraic attacks”. However, for these algorithms, substantiation of security against linear and differential cryptanalysis attacks used some heuristic techniques, and that requires further analysis to achieve a strict formal substantiation. E.g. in substantiation of the algorithm security against linear attacks, the authors considered coordinate functions of S-boxes that shows that they analyzed its security against ”classical” linear attacks with respect to bitwise addition. However, as shown in [1, 2], it is necessary for such construction to analyze specifically security against linear and differential cryptanalysis with respect to field operations, as both the key adder and the linear layer use operations in a prime field instead of binary operations.

Main results. The paper contains the following results.

1. Security estimations were built against linear and differential attacks with respect to field operations. Let us note that construction of such estimates uses a serious algebraic apparatus; in particular, various relations containing sums of characters for an additive group of a finite field.
2. We present the general parameters for the Poseidon hash function that allow using this hash function in recurrent SNARK-proofs based on MNT4 and MNT6 triplets.
3. We showed how it is possible to choose S-Boxes for such function for this choice to be optimal from the point of view of the number of constraints and security.
4. We showed how many full rounds is sufficient to guarantee security of this hash function against linear and differential attacks with respect to field operations.
5. We calculated the number of constraints per bit that is achieved in the proposed implementation; a considerable gain as compared to the Pedersen hash function was demonstrated.

We provided strict formal proofs for all listed results. Following [4] and [5], we chose round functions for random permutations and their parameters in the following way:

- the number of rounds with a full S-Box layer is chosen as the minimal number that guarantees security against differential and linear attacks;
- the number of rounds with a partial S-Box layer is chosen as the minimal number that guarantees security against other attacks given in [5, 7];
- S-Boxes are chosen as power functions in the finite field.

Considering specific features of the hash function application and the need for its compatibility with MNT4 or MNT6 triples [9], we chose the following parameters of the round functions:

- a prime field F_p where p is a prime number that is used in MNT4, of the length of 753 bits;
- exponent of the function describing the S-Box was chosen so as from one side to guarantee the required level of security against attacks, and from the other side to minimize the number of constraints;
- one round with a full S-Box layer contains three S-Boxes, and a round with a partial S-Box layer contains one S-Box.

Such selection of parameters allows obtaining the following characteristics of the hash function at the set security level of $\lambda = 128$ bits: 4 rounds with a full S-Box layer (two rounds at the beginning and two at the end); from 56 to 60 rounds with a partial S-Box layer; from 0.1 to 0.3 constraints per bit.

Conclusions. The results obtained show that the Poseidon hash function is secure against linear and differential attacks with respect to field operations. Given the security level, we can choose parameters of this hash that guarantee its cryptographic security. An indisputable advantage of the hash function with such structure is its effectiveness at its utilization for SNARK-proofs.

References

[1] Mohamed Ahmed Abdelraheem, Martin Ågren, Peter Beelen, and Gregor Leander. On the distribution of linear biases: Three instructive examples. In *Annual Cryptology Conference*, pages 50–67. Springer, 2012.

[2] Thomas Baigneres, Jacques Stern, and Serge Vaudenay. Linear cryptanalysis of non binary ciphers. In *International Workshop on Selected Areas in Cryptography*, pages 184–211. Springer, 2007.

[3] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptology ePrint Archive*, 2018:46, 2018.

[4] Lorenzo Grassi, Daniel Kales, Dmitry Khovratovich, Arnab Roy, Christian Rechberger, and Markus Schofnegger. Starkad and poseidon: New hash functions for zero knowledge proof systems. *IACR Cryptology ePrint Archive*, 2019:458, 2019.

[5] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a generalization of substitution-permutation networks: The hades design strategy. Technical report, Cryptology ePrint Archive, 2019.

[6] Jens Groth. On the size of pairing-based non-interactive arguments. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 305–326. Springer, 2016.

[7] Bertoni Guido, Daemen Joan, P Michaël, and VA Gilles. Cryptographic sponge functions, 2011.

[8] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol specification: Version 2019.0-beta-37 [overwinter+ sapling]. Technical report, Tech. rep. available at https://github. com/zcash/zips/blob/master/protocol . . . , 2019.

[9] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for fr-reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 84(5):1234–1243, 2001.

[10] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. Pinocchio: Nearly practical verifiable computation. In *2013 IEEE Symposium on Security and Privacy*, pages 238–252. IEEE, 2013.

EVALUATION AND MINIMIZATION OF KLEPTOGRAPHY RISKS IN CRYPTOGRAPHIC ALGORITHMS

Bohdan Kovalenko[1], Anton Kudin[2],
[1] *Ring Inc., animantbk@gmail.com*
[2] *National Technical University of Ukraine "KPI", pplayshner@gmail.com*

Abstract. The most of modern standard cryptographic algorithms are developed during public (e.g., AES or NESSIE) and semi-public (internal state-level researches) competitions. It increases the algorithm's resistance against common cryptographic attacks and guaranties sufficient security level. However, risks belong to the kleptographic backdoor implementation are still high because of two reasons: first, the state-wise or world-wise cryptographic standard, that are implemented in thousands and millions of products, which are out of the secure perimeter, are susceptible to target manipulations, and second, modern cryptoanalysis approaches often aren't efficient for kleptographic trapdoor detection. The goal of our research is to create a metric to estimate risks of kleprographic backdoor existence. The metric allows additionally to evaluate cryptographic algorithms during the standardization process and reject suspicious algorithms on the early estimation stage.

Keywords. Kleptography, cryptographic algorithm, subliminal channel, kleptographic trapdoor, eSTREAM, NESSIE, AES, Streebog.

1 Introduction

The idea of kleptography trapdoors was introduces by G. Simmons as subliminal channels in the prisoner's problem [4]. The further development of the idea is modifying of existent cryptosystem to allow hidden transmission of additional sensitive information: DSA private key [4], Diffie-Hellman session secret key or RSA private key [5]. Also, there are examples in symmetric cryptography: DES cipher (suspected to be weakened to simplify analysis for NSA), DualEC DRBG [2] (developer may guess RNG output because of backdoor), hash function "Stribog"[1] (a lot of additional entropy in the structure without appropriate argumentation).

A lot of public cryptography standard competitions like as AES, NESSIE or eSTREAM (and numerous of local ones) targeted mostly on security and performance aspects of new cipher's candidates. However, kleptography risks are still without high attention, that leads to risks belong to kleptography backdoor existence.

The main goal of this research is to formalize process of backdoor implementation and suggest methods to decrease kleptography risks at development and standardization stages.

2 Main results

General formal model of kleptographic backdoor. In the research, we start from the standard Shannon's model of secret system [3] but extended with the additional actor – Developer, who is considered to be an attacker (like Eva) but with the additional capability to develop and deploy crypto algorithms on communication endpoints. The are numerous ways to do this – attacks on endpoints, malware infection, distribution of vulnerable crypto libraries or lobby in crypto algorithms standardization but here we focus on the last one.

One of the investigation's goals is to define a metric that shows kleptographic risks. We introduced the metric called "kleptographic potential": $\phi : \mathbb{A} \rightarrow \mathbb{R}$, where $\mathbb{A}$ is a set of all possible crypto algorithm's, moreover if $\phi(A) < \phi(B), A, B \in \mathbb{A}$ than "risks" of klepto backdoor existence are higher in the algorithm B.

Let $Prim$ be a crypto algorithm (new crypto standard candidate) in the form $Prim : Par \rightarrow Out$, where Par – the space of inputs, (examples of inputs: plain text, secret key, initial vector, salt, etc.), Out – the space of outputs (e.g., cipher text, hash code, signature digest, salt, etc.). Let $\mathbb{F}_{Prim} \subset Par^{Out}$ be a set of all alternative implementations of the candidate $Prim$. (example of alternative implementations: algorithms with modified S-boxes, round constants, initial values, etc.) Further, let's suppose, Developer have a publicly known method, that is an injective function, which generates crypto algorithm with kleptographic trapdoor based on Developer's secret from the secret's space Ω: $TrapGen_{Prim} : \Omega \rightarrow \mathbb{F}_{Prim}$. Thus, our goal is to estimate maximal amount of Developer's information that is brought into a structure of algorithm.

Here, we use Shannon's entropy [3] to formalize the uncertainty of algorithm's structure and Developer's information impact.

Let's consider a probabilistic ensemble X and Y. Unconditional Shannon's entropy for ensemble X is: $H(X) = \sum_{x \in X} p(x) log_2 \frac{1}{p(x)}$. Also we need conditional entropy $H(X|Y)$ that shows residual uncertainty after the realization of the variable from ensemble Y: $H(X|Y) = \sum_{y \in Y} \sum_{x \in X} p(x,y) log_2 \frac{1}{p(x|y)}$.

Now, let's define the kleptographic potential.

Definition 1. (Kleptographic potential). Let $\mathbb{F}_{Prim}$ be a set of possible functions (according to restrictions that follow from cryptographic properties and general design requirements), which are acceptable as new candidate algorithm $Prim$.

"Kleptographic potential" we call maximal amount of information, that is embedded into algorithm's structure by Developer:

$$\phi(Prim) = H(\mathbb{F}_{Prim}) - H(\mathbb{F}_{Prim}|D) \leq log_2(|\mathbb{F}_{Prim}|),$$

where $H(\cdot)$ – unconditional entropy of algorithm's structure before publication, $H(\cdot|D)$ – uncertainty of algorithm's structure before publication but after initializing by Developer.

The idea of such metric: we estimate the entropy in the design of the crypto algorithm candidate and subtract the part of uncertainty which isn't under the Developer's control, so the final value is exactly Developer's information amount that remains in the algorithm.In some use cases, e.g. where final design is negotiated by many parts, we need conditional entropy in the expression.

The kleptographic potential is a metric of a risk of trapdoor existence: it is the upper estimate of Developer's secret size in the design. Actually, Developer's huge kleptographic potential doesn't indicate that the trapdoor really exists, rather that there are no arguments against such existence. However, a small value indicates that trapdoor is an absence at all: anybody who knows trapdoor design is able to obtain Developer's secret in practical time.

Examples of kleptographic potential potential. The important general example is a parametrized framework. "A framework" we call an algorithm, whose parameters and constants, that may be mapped from some N-bit sequence by some defined function, are put out of the suggested design and may be initialized later. If a framework has N bits of uninitialized parameters, we claim, the kleptographic potential is at least N. One of the way to reduce the lower boundary of kleptographic potential (by value N) is initializing of parameters and constants after candidate negotiation. The initialization process must disallow Developer to handle some amount of information of future constants.

Also, suggested metric allows to estimate the lower bound of kleptographic potential for existing existing crypto algorithms using the trick: given crypto algorithms is reduced to a framework putting out constant parameters (s-boxes, round constants, etc.). These modification must keep cryptographic properties and general design of the origin. These requirements are informal enough, they mean rather that modifications should be considered by the cryptology community as "equivalent algorithms but with modified parameters". Further, we are able to estimate kleptographic potential for the framework and the value of potential is a maximal Developer's secret size (because all these constants in the origin are initialized by Developer). Examples of such evaluation was performed for some of the algorithms and shown in the table 1:

Table 1: The kleptographic potential of different crypto algorithms

Algorithm	Construction	Potential source	Klepto potential
AES	SP-network	SubBytes and MixColumns procedures	32b
SHA-256	unbl. Feistel scheme	nonlinear functions	78b
GOST R 34.12-2015 "Kuznechik"	SP-network	S-box and linear transformation	2176b
GOST R 34.11-2012 ”Streebog”	SP-network	S-box, bytewise permutation, linear transformation, round constants	12582.19b

We see here, the least potential has been detected in AES encryption standard and the most one is in Russian hash function standard ”Streebog” – 12582.19 bits.

3 Conclusion

During this research, the authors analyzed way to ensure low kleptographic risks in crypto algorithm candidates in a public competition process. As a result, we suggested the formalization of kleptographic risks model of crypto algorithm. Also, we introduced a metric of kleptographic risks – "kleptographic potential" that means maximal amount of information that Developer may insert into the algorithm's structure. Further, we evaluated and compared kleptographic potentials for several widespread symmetric crypto algorithms.

References

[1] Alex Biryukov, Leo Perrin, and Aleksei Udovenko. *Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 (Full Version)*. Cryptology ePrint Archive, Report 2016/071. `http://eprint.iacr.org/2016/071`. 2016.

[2] DanielR.L. Brown and Kristian GjA steen. "A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator". English. In: *Advances in Cryptology - CRYPTO 2007*. Ed. by Alfred Menezes. Vol. 4622. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, pp. 466–481. ISBN: 978-3-540-74142-8.

[3] Claude E. Shannon. "Communication Theory of Secrecy Systems". In: *The Bell System Technical Journal* 28.4 (Oct. 1949), pp. 656–715.

[4] Gustavus J. Simmons. "The Subliminal Channel and Digital Signatures". In: *Advances in Cryptology*. Ed. by Thomas Beth, Norbert Cot, and Ingemar Ingemarsson. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 364–378. ISBN: 978-3-540-39757-1.

[5] Adam Young and Moti Yung. "Kleptography: Using Cryptography Against Cryptography". In: *Advances in Cryptology — EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings*. Ed. by Walter Fumy. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 62–74. ISBN: 978-3-540-69053-5.

Cryptanalysis of the permutation based algorithm SpoC

Liliya Kraleva, Raluca Posteuca, Vincent Rijmen

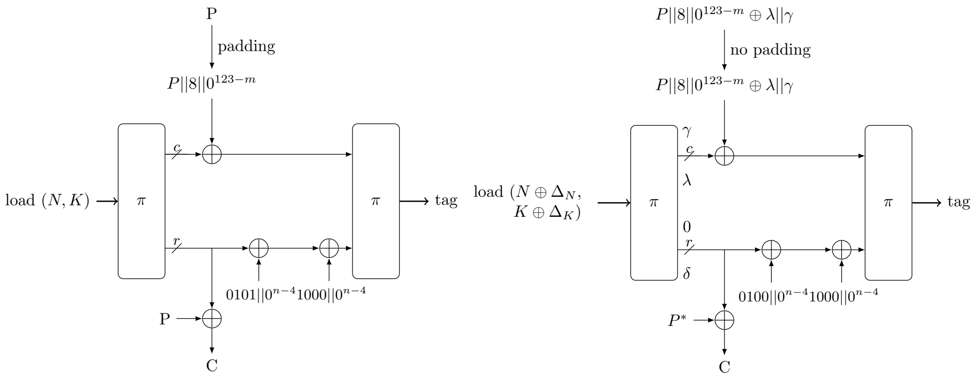
Since most of the currently standardized algorithms are designed for desktop and server usage, they are not suitable for constrained environments, such as RFID tags, sensor nodes or smart cards. Due to the increased need of lightweight primitives, NIST organised a competition aiming at standardizing a portfolio of lightweight algorithms, targeting authenticated encryption with associated data (AEAD) ciphers and hash functions. In order to contribute to the public research efforts in analysing the candidates of the on-going second round, we focused on the SpoC cipher, a permutation based AEAD. In this paper we present the results of a security research on both versions of SpoC, namely SpoC-64 and SpoC-128. We analyse the sLiSCP-light permutation used in the algorithm, as well as the structural behaviours of SpoC-64.

In this paper we introduce tag-forgery attacks based on differential cryptanalysis approach on round-reduced versions of both SpoC primitives. Additionally, a key-recovery attack is introduced for the full round version of SpoC-64, based on preimage attacks. To the best of our knowledge, this is the first research that analyses the security of the sLiSCP-light permutation and the first published results on SpoC.

Our **differential analysis** is based on the following 3 observations of SpoC. First, a null AD or an empty message impose the corresponding phase to be skipped. Second, in each phase a different constant is added to the rate part. Third, compared to SpoC-64, the initialization phase of SpoC-128 consists only of loading the key and nonce to the state. More generally, our attack exploits the similarities between the associated data addition and the plaintext addition, together with the similarities between the processing of a padded and a full block of input.

Our attacks based on differential cryptanalysis exploit the appearance of differences in some particular usages of SpoC. For example, let us consider the encryption of an incomplete plaintext block P and the complete plaintext block $P^* = padded(P)$, using the same key-nonce pair and the same associated data. The only difference between these two encryption processes is given by the difference between the added constants of the plaintext processing phase, i.e. $0001||0^{n-4}$. Depending on the size of the input (plaintext, associated data), the difference between constants can also be $0110||0^{n-4}$ or $0111||0^{n-4}$.

In order to exploit these observations, we designed differential characteristics covering a round-reduced version of the permutation, such that, after the plaintext processing phase, this difference is cancelled by the output difference of the characteristic. In this case, the internal states before the tag generation phase are equal, thus, they produce equal tags. Moreover, in order to optimize the probability of the characteristic, we relaxed the conditions of the output difference, searching for characteristics having the output difference of the form $(\delta, \lambda, 0, \gamma)$, where δ is the difference between the constants, while the differences λ and γ can be cancelled through the plaintext block difference. The processing of P and P* is shown in Figure 1.



P
padding
$P||8||0^{123-m}$
load (N, K)
π
c
r
π
tag
$0101||0^{n-4}1000||0^{n-4}$
P
C
$P||8||0^{123-m} \oplus \lambda||\gamma$
no padding
$P||8||0^{123-m} \oplus \lambda||\gamma$
load $(N \oplus \Delta_N,$
$K \oplus \Delta_K)$
π
γ
c
λ
0
r
δ
π
tag
$0100||0^{n-4}1000||0^{n-4}$
P^*
C

(a) (b)

Figure 1: The encryption of (a) a partial block P and (b) a full block $P^* = \mathit{padded}(P) \oplus \lambda||\gamma$, with null AD in both cases

The characteristics were constructed with the SAT-based tool ArxPy. After obtaining optimal characteristics over the SBox using the tool, we empirically verified the total differential probability and chose the intermediate differences accordingly. The characteristic used to attack SpoC-128 covers 6 rounds (out of 18) of the sLiSCP-light permutation with probability 2^{-106}. After further improvements, the time complexity of this attack is $2^{105.32}$ Sbox calls, while the data complexity is $2^{104.32} + 2^{86.63}$. The characteristic used to attack SpoC-64 covers 7 rounds of the permutation (out of 18), with the probability of $2^{-110.78}$. The time complexity of the attack is $2^{110.78}$ Sbox calls, while the data complexity is $2^{110.78} + 2^{88.23}$. For the attack on SpoC-128 we assume a key-related nonce-related scenario with chosen key and nonce differences, whereas for SpoC-64 only nonce-related scenario is assumed, the ciphertexts being encrypted under the same key.

The **key-recovery attack** on SpoC-64 is based on the existence of multiple (key, nonce) pairs that lead to the same state after the initialization phase. Moreover, the encryption of the same message under (key, nonce) pairs that lead to the same internal state results in equal ciphertexts and tags. The key-recovery attack consists of an offline and an online phase. In the offline phase, the encryption of a common short message M is generated and stored under different (key, nonce) pairs. In the online phase, ciphertext and tag pairs are intercepted and the first blocks are compared with the stored ones. When a match is found, the adversary can compute the user's key, decrypt the message or even impersonate the user. The memory complexity of this attack is 2^{110} table entries, while the time complexity is 2^{110} SpoC-64 encryptions. For 2^{67} intercepted messages, the success probability of the attack is 2^{-15} (twice the attack probability claimed by the authors). In comparison, an exhaustive search with the same success probability of 2^{-15} would require a data complexity of 2^{113}.

We stress that all attacks presented in this abstract satisfy the security claims of Spoc. The setup of our attacks assume a nonce-respecting adversary, while the time complexity is below the one claimed by the authors. Regarding the data complexity, the authors claim that no more than 2^{50} data can be encrypted using the same key. In the case of our attacks, even though the data complexity is higher than 2^{50}, the encryption/decryption is performed under sets of different keys, respecting the constraint that no more than 2^{50} data is encrypted/decrypted under the same key.

Comparative analysis of ARX transformations

(extended abstract)

Victor Ruzhentsev
victorruzh@gmail.com
Department of Secure Information Technologies, Kharkiv National University of Radioelectronics,
Kharkiv, Ukraine

Introduction

Lightweight cryptography is a rapidly growing field of symmetric cryptography. Confirmation of this is a global Lightweight cryptography project of the American National Institute of Standards and Technology. One of the most important issues in constructing lightweight algorithms is the approach to building nonlinear elements. On the one hand, it is known that bigger S-boxes are more effective in terms of cryptographic strength. On the other hand, bigger S-boxes tend to cost more on memory usage, which is an important parameter for lightweight cryptography. We reflect on which philosophy in lightweight cryptography is more advantageous: use large S-boxes based on efficiently implemented computational operations, for example, ARX operations (Addition, Rotation, Xor), or use small-size substitutions (4 to 4 bits).

The aim of this work is to find the optimal approach to building ARX transformations in terms of maximum speed and cryptographic security. To achieve the goal, we will analyze the most famous solutions for building ARX transformations. Considering the fact that ARX algorithms are easily scalable, we will develop reduced models for their comparison and determine how many rounds are needed to achieve the cryptographic parameters of random permutation.

1 Reduced ARX models

Only brief description of considered models is presented in this extended abstract.

The first ARX scheme is a quarter-round of stream cipher ChaCha 2 with reduced subblock size. The 16-bit state of the reduced model ChaCha consists of four 4-bit subblocks.

The second ARX scheme is a simplified scheme of the Speckey algorithm. The simplification is the absence of two cyclic shift operations, which in the original version preceded the modular addition operations. The Speckey 16-bit block consists of two 8-bit subblocks.

Next scheme is a reduced model of the Simon encryption algorithm. Three modifications of original scheme are also considered in this work. Simon1 and Simon2 use modular addition instead of AND and some XOR operations. Simon3 uses two cyclic shifts of the left subblock, XOR addition of these two shift results and modular addition of the result to the right subblock. The 16-bit block of all Simon's variants consists of two 8-bit subblocks.

Another one ARX scheme is a reduced scheme of the Chaskey algorithm. The 16-bit Chaskey block consists of four 4-bit subblocks.

Another scheme is the ARX S-box of the Sparkle algorithm, called Alzette. Block consists of two 8-bit blocks.

In our experiments, all models, at first, use the XOR addition of 16-bit block with a random key of the same size, and then use keyless rounds.

2 Analysis of cryptographic security

The most important cryptographic parameters of an encryption function or substitution are:

- maximum probability of the difference propagation (determines the resistance of the cipher to differential attacks);
- maximum probability of linear approximation (determines the resistance of the cipher to linear cryptanalysis);
- nonlinear order (determines the resistance of the cipher to interpolation attacks).

It is possible to estimate these parameters for 16-bit models of encryption functions.

The maximum probability of the difference propagation was searched for the considered ARX schemes. 64 randomly selected keys were used in the search. The detailed results will be presented in the full version of the report. As a rule, the models come to a stable value $2^{-11.7}$ after using sufficient number of rounds. Speckey, ChaCha and Chaskey require 5 rounds for this, Simon1 – 7 rounds, Simon2 – 6 rounds, Simon3 – 8 rounds, Alzette – 9 rounds. Scheme Simon, on the other hand, does not match the random permutation value $2^{-11.7}$ for any number of rounds.

Maximum probability of linear approximation was searched for the few variants of the input mask and for the 5 randomly selected keys. The detailed results will be presented in the full version of the report. The models come to a stable value of $2^{-6.4}$ after using sufficient number of rounds. Simon2 and Chaskey require 5 rounds, Speckey and ChaCha – 6 rounds, Simon3 and Alzette – 7 rounds.

The nonlinear order for a random permutation 16 to 16 bits must be 15. It was determined that all models come to this value after using 3 rounds.

These three cryptographic parameters were used to determine how many addition and shift operations are required to provide cryptographic parameters of random permutation. Tables 1 and 2 show required number of operations to provide cryptographic parameters of random permutation, respectively, for the 8-bit and 4-bit ARX schemes.

Table 1 – Number of 8-bit operations to provide cryptographic parameters of 16-bit random permutation

Schemes	Min. number of rounds	Number of operations			
		Addition	Rotation	Xor	Total
Speckey	6	12	12	12	36
Simon2	6	6	18	12	36
Simon3	8	8	16	8	32
Alzette	9	9	18	9	36

Table 2– Number of 4-bit operations to provide cryptographic parameters of 16-bit random permutation

Schemes	Min. number of rounds	Number of operations			
		Addition	Rotation	Xor	Total
ChaCha	6	24	24	24	72
Chaskey	5	20	20	20	60

Table. 1 and 2 show that Chaskey is the most efficient 4-bit scheme, and Simon3 is the most efficient 8-bit scheme. In general, the considered schemes demonstrate quite a similar result. For example, the difference in the number of operations for 8-bit schemes does not exceed 4.

Conclusions

1 The analysis of cryptographic parameters of reduced models (16 bit block) of the most known ARX encryption algorithms was performed. These algorithms are Salsa, ChaCha, Cypress, Speckey, Simon, Chaskey, Sparkle and their modifications. It has been demonstrated that most models come to stable value of most important cryptographic parameters after using sufficient number of rounds. But this situation is not true for maximum probability of the difference propagation for ARX scheme from Simon cipher. Therefore, a reduced model of the Simon algorithm requires additional more careful consideration.

2 ARX schemes which use 8-bit operations and schemes which use 4-bit operations are considered in the work. Using these schemes it is shown that, potentially, ARX schemes with larger size of operations are more flexible and efficient, since, according to our results, they require, approximately, half the number of operations to provide cryptographic parameters of random permutation.

3 According to the Table 1 and 2 Chaskey model is the most efficient ARX scheme with 4-bit operations, and Simon3 is the most efficient scheme with 8-bit operations. At the same time, for example, implementation on 8-bit processor of Simon3 requires almost twice less operations than Chaskey to achieve cryptographic parameters of random permutation.

A Note on Low Order Assumptions in RSA groups

István András Seres and Péter Burcsi

Eötvös Loránd University

April 2020

Abstract

In this short note, we show that substantially weaker Low Order assumptions are sufficient to prove the soundness of Pietrzak's protocol for proof of exponentiation in groups of unknown order. This constitutes a first step to a better understanding of the asymptotic computational complexity of breaking the soundness of the protocol. Furthermore, we prove the equivalence of the (weaker) Low Order assumption(s) and the Factoring assumption in RSA groups for a non-negligible portion of moduli. We argue that in practice our reduction applies for a considerable amount of deployed moduli. Our results have cryptographic applications, most importantly in the theory of recently proposed verifiable delay function constructions. Finally, we describe how to certify RSA moduli free of low order elements.

1 Introduction

Verifiable delay functions (VDF) are powerful cryptographic tools [BBBF18] that opened up a plethora of applications, such as non-interactive timestamping [LSS19], proof of replication [FBGB19] or randomness beacons [BGB17]. A VDF is a function whose evaluation takes $\mathcal{O}(T)$ sequential steps and cannot be sped up by parallelism. Additionally, a prover, or evaluator, can produce publicly verifiable and succinct proofs that the function evaluation was correct. A crucial requirement for a VDF that there needs to be an exponential gap between function evaluation and proof verification time, more precisely verification time should be in $\mathcal{O}(\log T)$. Naturally, we require correctness and soundess from the applied proof systems. Specifically, an honest prover should always be able to convince the verifier, while a malicious prover should only be able to produce correct proofs with negligible probability.

Recent VDF constructions [Pie18, Wes19] proposed by Pietrzak and Wesolowski instantiate VDFs in groups of unknown order, i.e. groups for which the order cannot be computed efficiently [RSA78]. The existence of verifiable delay functions in the random oracle model is ruled out [MSW], moreover groups of unknown order are shown to be mandatory for generic group delay functions [RSS]. Both constructions [Pie18, Wes19] rely on novel, non-standard cryptographic assumptions. The soundness of these constructions can be proved by assuming the Low Order (LO) or Adaptive Root (AR) assumptions in groups of unknown order. Therefore there is an emerging need to understand better these new, non-standard cryptographic assumptions. In this note, we turn our attention to the LO assumption as it is a potentially weaker assumption than the AR assumption [BBF18].

Our contribution. In this note, we provide the following contributions.

- We observe that for the soundness of Pietrzak's proof of exponentiation succinct argument, one can assume substantially weaker LO assumptions than as previously defined in [BBF18]. In other words, we show that potentially it is harder to break soundness of Pietrzak's argument than as it was argued in [BBF18].
- We prove the equivalence of the LO and Factoring assumptions in RSA groups for non-negligible portion of moduli. We argue that this result has practical consequences and that in practice one can deem the LO assumption to be equivalent to Factoring for the majority of used RSA moduli.
- We show how one could certify RSA moduli being free of low order elements using a non-interactive honest-verifier zero-knowledge proof system by Goldberg et al [GRSB19].

The rest of this note is organized as follows. In Section 2 we provide background on the recently introduced LO and AR assumptions. We show the sufficiency of weaker LO assumptions in Section 3. In Section 4 we provide our reduction from Factoring to LO asumption for non-negligible RSA moduli. We describe a method to certify RSA moduli free of low order elements in Section 5. Finally, we point out open problems in Section 6.

References

[AVD] Vidal Attias, Luigi Vigneri, and Vassil Dimitrov. Implementation study of two verifiable delay functions.

[BBBF18] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In *Annual international cryptology conference*, pages 757–788. Springer, 2018.

[BBF18] Dan Boneh, Benedikt Bünz, and Ben Fisch. A survey of two verifiable delay functions. *IACR Cryptology ePrint Archive*, 2018:712, 2018.

[BBF19] Dan Boneh, Benedikt Bünz, and Ben Fisch. Batching techniques for accumulators with applications to iops and stateless blockchains. In *Annual International Cryptology Conference*, pages 561–586. Springer, 2019.

[BGB17] Benedikt Bünz, Steven Goldfeder, and Joseph Bonneau. Proofs-of-delay and randomness beacons in ethereum. *IEEE Security and Privacy on the blockchain (IEEE S&B)*, 2017.

[BN06] Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 390–399, 2006.

[BS13] Eric Bach and Jonathan P Sorenson. Approximately counting semismooth integers. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 23–30, 2013.

[FBGB19] Ben Fisch, Joseph Bonneau, Nicola Greco, and Juan Benet. Scaling proof-of-replication for filecoin mining. Technical report, Technical Report. Stanford University. Accessed May, 2019.

[GRSB19] Sharon Goldberg, Leonid Reyzin, Omar Sagga, and Foteini Baldimtsi. Efficient noninteractive certification of rsa moduli and beyond. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 700–727. Springer, 2019.

[LSS19] Esteban Landerreche, Marc Stevens, and Christian Schaffner. Non-interactive cryptographic timestamping based on verifiable delay functions. *IACR Cryptology ePrint Archive*, 2019:197, 2019.

[MSW] Mohammad Mahmoody, Caleb Smith, and David J Wu. A note on the (im) possibility of verifiable delay functions in the random oracle model.

[Pie18] Krzysztof Pietrzak. Simple verifiable delay functions. In *10th innovations in theoretical computer science conference (itcs 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[RSS] Lior Rotem, Gil Segev, and Ido Shahaf. Generic-group delay functions require hidden-order groups.

[ŠNS+16] Petr Švenda, Matúš Nemec, Peter Sekan, Rudolf Kvašňovskỳ, David Formánek, David Komárek, and Vashek Matyáš. The million-key question—investigating the origins of {RSA} public keys. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pages 893–910, 2016.

[War90] Richard Warlimont. Sieving by large prime factors. *Monatshefte für Mathematik*, 109(3):247–256, 1990.

[Wei01] Andreas Weingartner. Integers free of prime divisors from an interval, i. *Acta Arithmetica*, 98:117–131, 2001.

[Wes19] Benjamin Wesolowski. Efficient verifiable delay functions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 379–407. Springer, 2019.

Musipher: Hiding information in music composition

Peter Spacek, Pavol Sobota
peter.spacek@stuba.sk,sobotapavol9@gmail.com
Slovak University of Technology in Bratislava, Slovakia

April 2020

1. Introduction

In information hiding, we can see two basic approaches. Steganography focuses on hiding existence of the message. Cryptography, on the other hand, focuses on hiding the meaning of the message. The advantages of this approach are summarized as Kerckhoffs's principle [4].

The idea of hiding information into music is very old. Gaspar Schott in a book *Schola Steganographica* [7] published in 1680 introduced a simple scheme of how to hide messages in music, where each music note corresponds to one letter. This idea was used repeatedly by many composers, including Robert Schumann, Johann Sebastian Bach, Johannes Brahms, or more recent Dmitri Shostakovitch [3].

We can also find this idea in 21st century. An interesting example is the use of radio hit in Columbia. In 2010, The Revolutionary Armed Forces of Colombia (FARC) held Colombian soldiers prisoners. Colombian Army decided to send a message of hope in Morse code, hidden in pop-song ”Mejores Dias” broadcasted nationwide [6].

2. System design

Our design does not not hide information in the sound like modern steganography, but it is more similar to the work of classical composers mentioned above. The system takes the information and transform it into musical structure of the song. It uses harmony, rhythm and melody, so that its not easy to tell that the song was composed automatically and has a hidden meaning.

Our system consists of two modules: stegano-module is a music composition module and for decisions in music composition, we need high entropy. This is provided by the output of the crypto-module that handles diffusion and confusion. Whole system is deterministic, so with the same key, and same input we get the same music.

3. Crypto-module

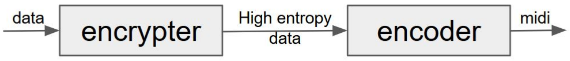


Figure 1: System scheme

The task of the crypto-module is to go from input data bit sequence to random bit sequence with use of the cryptographic key. This randomness for output is needed for hiding the meaning of the message as well as for the music encoder. For our needs, we chose AES cipher.

4. Stegano-module

The main question here is how to go from random bit sequence to meaningful music (output in MIDI format). We can take inspiration from simple modified Turing. We wanted output from our music encoder to be indistinguishable from other music, so the listener is not able to tell our deterministic composition from arbitrary simple human music composition.

We started with Jamie Henke's work [2], where we can also find some basic music terminology: Standard period of music is one ”musical sentence”. Our period consist of 8 measures. Music measure (or bar) is a group of beats (basic rhythmic unit). Usually we work with 3 or 4 beats in one measure. In our work we use 4 beats.

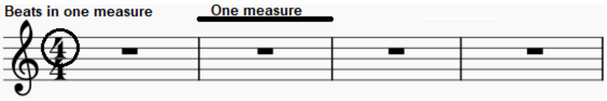


Figure 2: Half of the period (phrase)

In song structure we can use several different periods. The most common used ones are intro, verse, chorus, bridge, and outro. We compose every period separately, then add them together to compose a song.

Every musical element in our music composition is based on the binary input. We are composing music on three levels:

4.1. Harmony

For simplicity we use the same key for all periods of the song. The key determines chords used in the period as well as last note of the period. Cho-

[0] This work is supported by project VEGA 1/0159/17

sen chords are then permuted, used in a harmonic progression of the song and stored. They are later used in automaton for composing a melody 3.

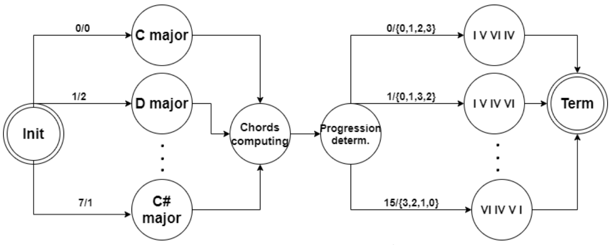


Figure 3: Finite state machine for harmony

4.2. Rhythm

There are many types of rhythmic units across all music genres. In our music composition we use exactly eight different rhythmic units. Their common property is that they divide a single beat by a ratio, which is labeled by number, and used for a counter to determine in which part of the period we are. The interpretation of the process which chooses what unit we use with particular beat can be seen in figure 4.

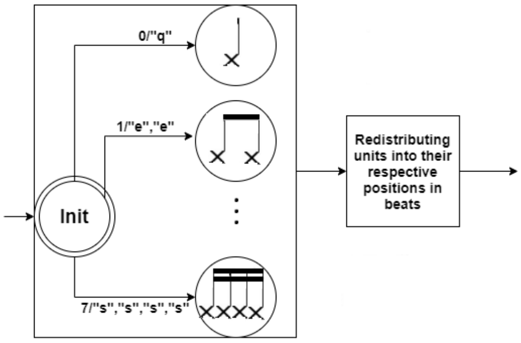

0/"q"
1/"e","e"
Init
7/"s","s","s","s"
Redistributing units into their respective positions in beats

Figure 4: Finite state machine for rhythm

4.3. Melody

The process of creating melody can be simplified into transformation of melodic pitch of each note based on previous note. Pitch can be changed into higher or lower notes, with shorter or longer pitch intervals. The shortest interval changes are called ”steps” and longer ”leaps”. This method can be interpreted with Mealy machine in figure 5. In output of some transitions, ”m” represents previous note and numerical value represents pitch change in respective key. Value ”k” represents temporal variable used to compute pitch change in leaps.

There are other composition practises we use in melody creation, such as adding chords notes into measures, copying measures etc. We cannot store as many information bits into those decisions as in previous method in figure 5.

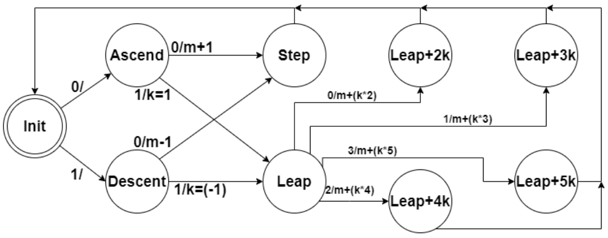


Figure 5: Finite state machine for melody

5. Implementation

This system is implemented into simple Java application, where the user is able to transform a message or data set into a short song with the use of a unique cipher key. The user can also decompose a song, decipher and extract the message. We use JFugue[5] library to work with music in Java.

6. Results & discussion

In our GitHub repository [1] there is a system implementation in Java, as well as some MIDI files and sheet music of the generated song examples.

The most important lesson we have learned from this work is that music has the ability to be interpreted in many ways. We can use this ability not only for mere composition of music, but for storing and hiding information as well.

Currently we are experimenting with the question of proper ratio of stored bits and more natural feeling of the song.

For future research, we are planning to experiment with different harmonies and more complicated music structures to understand the topic more closely, and produce even better sounding result. Moreover, we consider producing more music genres. This work is going to be published as a bachelor thesis.

References

[1] github.com/xsobotap/Music-cipher.

[2] J. Henke. Basic Concepts of Music Theory. *iTunes U*, 2011.

[3] T. Judd. Musical Cryptograms: Five Scores that Contain Hidden Messages. *The Listeners' Club*, 2019.

[4] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, Jan, Feb:5–83, 161–191, 1883.

[5] D. Koelle. Music programming for java^{TM} and jvm languages. jfugue.org.

[6] J. Maysh. THE CODE: A declassified and unbelievable hostage rescue story. *The Verge*, 2015.

[7] G. Schott. Schola steganographica: in classes octo distributa. *Jobus Hertz, printer*, 1680.

Provision mechanism of authenticity of data origin in cloud environment based on Blockchain technology

Pavel Stetsenko, Gennadiy Khalimov

At this time, the usage of cloud computing services is reaching a new level in various commercial and military spheres to ensure reliable data storage and dynamic "elastic" provisioning of resources for computing "on demand" of the cloud customers. Securing management and data transfer within and between the clouds is one of the key challenges for organizations, which implement cloud approach to their business. Cloud auditing can only be effective when all data operations can be reliably tracked. Ensuring the authenticity of the history of data origin is a process that determines the history of a data object, starting from its creation [1]. Provisioning of the authenticity of data origin can help detect malicious activity in architectures built on the cloud platform basis [2].

The history of data origin will play an important role for cloud security engineers when debugging hacks of a system or network or performing digital forensics. Cloud computing environments are typically characterized by the transfer of data between different system and network components. Data usually does not follow the same path because of the many copies of the data and the variety of paths used to ensure system stability. Such a diverse data streams creates a certain difficulty for security engineers to correctly and accurately respond to a possible security incident, determine which software and / or hardware components contained vulnerabilities that led to a successful attack, the source and the surface of the attack, as well as the attack blast-radius. The history of the data origin in the cloud can be a key tool for identifying security incidents with a high degree of granularity and evidence. Modern data ownership cloud-systems support the above tasks using logging and auditing technologies. These technologies are inefficient in cloud computing systems, which are complex in nature due to several levels of interaction between software and hardware components, covering various geographical and organizational boundaries. To identify and eliminate malicious actions in the cloud requires analysis of data and logs from a diverse and heterogeneous set of sources for a limited time period using digital forensics, which is an insurmountable task. Although the exchange of information related to cyberthreats may be one of the options for achieving situational awareness of the cloud attack surface with less investment, this approach is prone to information forgery threats [3-5]. A reliable history of data origin will help to track all operations performed on each data object in the cloud, and Blockchain technology will guarantee data reliability and integrity.

This paper presents a provision mechanism of authenticity of data origin in cloud environments based on Blockchain technology, which ensures the reliability of data operations in cloud storage, while increasing privacy and accessibility. The architecture proposed in this work records all operations for each data object and stores them as a history of data origin, which is hashed then in the Merkle tree [6]. The list of origin data hashes will compose the Merkle tree, and the root node of the tree will be tied to the Blockchain-transaction. The list of transactions will be used to form the block, and the block must be confirmed by a set of nodes in the Blockchain network in order to be included in the Blockchain transaction ledger. Attempting to modify the record of data origin will require the attacker to locate the transaction and the block in the ledger. The underlying cryptography in Blockchain technology will only allow a block record to be modified if an attacker can submit a longer version of the Blockchain ledger than the rest of the fair network, which is quite difficult to achieve especially in decentralized systems with large amount of members.

The proposed architecture allows achieving the following goals:

1. Reliability of the history of data origin in the cloud in real time – user operations are captured in real time to collect information about the history of origin, which will further support the application of access control policies and intrusion detection systems. However, a delay occurs when placing records in blocks and processing them by the Blockchain network but capturing data events is real time process.

2. Protection against unauthorized access – a reliable history of the data origin is collected and then published to the Blockchain ledger to achieve data integrity. Then all data are distributed between nodes. The architecture provides creation of a public log with all user operations on cloud data with time stamps and without a trusted third party. A special construction

called “Blockchain receipt” is assigned to each record for further verification. Moreover, according to the principle of least privilege an access to proposed mechanism can be configured more granularly with cloud Identity and Access Management.

3. Increased confidentiality. Each entry in the data origin history is associated with a hashed user identifier in order to maintain its confidentiality, so that no Blockchain network node can match data records associated with a specific user. The data origin auditor can access information related to the user, but can never determine his identity. Only a service provider (cloud provider) can associate identifiers with the actual owners of each record in the data origin history. As for regulation compliance – the proposed mechanism is focused mainly on internal audit and operates with data generated by employees of the organization with cloud access, and GDPR or CCPA are focused on the privacy of customer's data i.e. consumers not employees.

4. Confirmation of the reliability of the data origin history in the cloud – a record of the history of the origin of data is published globally in the Blockchain network, where several nodes provide confirmation for each block. To check each record of the history of data origin, a Blockchain receipt is used.

The following methods were used in the architecture development to achieve the goals mentioned above:

- real-time monitoring of user actions using interceptors and listeners, so that each user file operation will be collected and recorded to obtain a history of data origin;
- storing all hashed data in the form of blocks in the Blockchain transactional ledger. Each node in the system can verify operations by analyzing the block so that the origin of the data is reliable and protected from falsification;
- hashing the user ID when adding data to the Blockchain ledger so that the network and the auditor cannot determine the identity of the user and operations with the data.

The cloud auditor of data origin history performs verification by extracting transactions from the Blockchain network using the Blockchain receipt, which contains information about the block and transactions.

The proposed architecture uses a cloud file as a data unit and monitors file operations to provide the Blockchain service for the reliability of data origin. After each file operation is detected, a history record of data origin is generated. The cloud service provider then uploads a history record of origin to the Blockchain network. It is important to note that the system can be scaled by increasing the number of nodes in the Blockchain network (scaling-out) or by deploying more powerful nodes with the same number of them (scaling-up), the database component with origin history can be scaled in the same way. Thus possibility of changing data unit and scalability of system components are important benefits of proposed mechanism comparing to previous researches in this field [7-8].

The cloud implementation of the proposed system allows stability, fault tolerance, elasticity and scalability. The implementation discussed in this paper can be taken as a basis for various applications – for the implementation of a more secure cloud-based security information and event management system (SIEM), offer users as an option of Blockchain-validity of journal entries for existing cloud-based logging services (for example, for AWS CloudTrail or Azure Monitor). Instead of a file, another granularity as a data unit can be used, such as a data block in a cloud object storage (AWS S3 or Azure Blob Storage). Collected data can be used for creation of behavioral patterns, which in turn can be used for developing of automated event-driven security responses by using ML and serverless tools.

References:

1. Simmhan Y. L., Plale B., Gannon D. "A survey of data provenance in e-science". – ACM Sigmod Record, vol. 34, N 3. – 2005. – pp. 31-36. 2. Lee B., Awad A., Awad M. "Towards secure provenance in the cloud”. – IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC). – 2015. – pp. 577-582. 3. Tosh D. K., Shetty S., Liang X., Kamhoua C., Kwiat K., Njilla L., "Security implications of Blockchain cloud with analysis of block withholding attack”. – International Symposium on Cluster, Cloud and Grid Computing. – IEEE/ACM, Madrid, 2017. 4. Ethereum project. [Online]. 2018. Available: https://www.ethereum.org/. 5. Greenspan G. "Multichain private Blockchain white paper" [Online] 2015. Available: http://www.multichain.com/download/Multichain.White Paper.pdf. 6. Merkle R. C. "Protocols for public key cryptosystems”. – IEEE Symposium on Security and Privacy, April 1980. – 122 p. 7. Sultana S., Bertino E. "A file provenance system” // In Proceedings of the Third ACM Conference on Data and Application Security and Privacy, ACM. – 2013. – pp. 153-156. 8. Suen C. H., Ko R. K., Tan Y. S., Jagadpramana P., Lee B. S. "S2logger: End-to-end data tracking mechanism for cloud data provenance” // In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE. – 2013. – pp. 594-602.

A Review of Encryption Schemes Used in Modern Ransomware*

Peter Švec[1] and Roderik Ploszek[1]

[1]Slovak University of Technology in Bratislava
Faculty of Electrical Engineering and Information Technology
Ilkovičova 3, 812 19 Bratislava, Slovak Republic
{peter.svec1, roderik.ploszek}@stuba.sk

1 Introduction

Ransomware is a special type of malware that encrypts personal user data. It focuses on documents, photos and other similar files stored on hard drive that may have some value to the owner of the computer. Original files are deleted and replaced with the encrypted version. After some time, the ransomware provides instructions how to get the files back, usually by paying some amount of money—hence the name **ransom**ware.

Ransomware was reported as a top threat in 2019 IOCTA [3]. This same report states that ransomware attacks are shifting focus from targeting individual citizen to more profitable private companies and public entities. According to Coveware report from Q4 2019, the average paid ransom is $84,116 [1].

As any other malware, ransomware uses sophisticated techniques to obfuscate its inner workings. The same goes to used encryption schemes—modern ransomware uses complex encryption schemes using combination of various ciphers and even custom cryptography algorithms.

2 Encryption Scheme Analysis

In this paper, a review of ransomware is presented. Analyzed samples were no older than one year to analyze current trends. These include Ryuk, Clop, Dharma and others. Following aspects of ransomware are examined:

- the encryption scheme—how many keys are used and where are they stored,
- types of ciphers used (symmetric and/or asymetric) ,
- key sizes,
- key generation (`rand()` or some more sophisticated generator)

*This research was sponsored by Slovak Republic under grant VEGA 1/0159/17.

- cipher modes,
- hash types, if used,
- and implementation used (system API, library or custom implementation).

Gathered data are compared to findings in previous publications [2] and online blogs. From this it is deduced how the development of ransomware has changed, whether the shortcomings of previous generations have been improved or if they are still present. At the same time, the accuracy of the information posted on the blogs of antivirus companies is checked against presented findings.

The samples were analyzed using a combination of static and dynamic analysis employing tools such as IDA, Ghidra and other disassemblers and debuggers.

3 Conclusion

This work presents a complex analysis of encryption schemes used in latest ransomware. The main goal is to find out the current trends in implementations circulating over the Internet. Findings are compared to previous works in the field.

References

[1] Coveware. Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate, 2020.

[2] Vlad Craciun, Andrei Mogage, and Emil Simion. *Trends in Design of Ransomware Viruses: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers*, pages 259–272. 01 2019.

[3] Europol. Internet Organised Crime Threat Assessment (IOCTA). Technical Report. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, 2019.

FORMAL LANGUAGE IDENTITY-BASED CRYPTOGRAPHY

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

Identity-based Cryptography (IBC) is an essential branch of public-key cryptography. The original concept behind IBC was coined by Adi Shamir in 1984 [1], who managed to build an identity-based signature scheme. However, Identity-based Encryption (IBE) remained an unsolved problem until Dan Boneh and Matthew Franklin created their pairing-based scheme in 2001 [2], providing feasible performance for practical use.

The uniqueness of IBC lies in the fact that its public key is a string that identifies an entity in a particular domain. One may think about an email address, a username or a phone number. This is in direct connection with the core idea of the IBC, which was to simplify the certificate management and eliminate the need for certification authorities. In the public key infrastructure scenario, public keys and user identities are bound together with certificates. With IBC, however, there is no need for such certificates, since the public key corresponds directly to the user identity.

Furthermore, the public key may contain more information than just the identity of the user. This extension of the public key with domain-specific data enables a wide spectrum of advanced use cases. Although, one limitation of IBC is that the public key of the receiver must be bit-accurate to the encryption key to be able to extract the belonging private key. Consequently, IBC is not able to handle finely granulated access policies.

A possible solution to this problem is Attribute-based Cryptography (ABC) [3, 4]. This type of cryptosystem uses an access policy to determine which cyphertexts a user can decrypt. The core idea is to treat the keys as expressions, which contain logical operators between attributes and values, thereby the keys are more flexible. A significant drawback of the ABC schemes is that they require more computation on the user-side (encryption and decryption functions) with the growth of the complexity of the access policy. This directly affects the usability of these protocols, since several potential applications target devices with limited computational power.

To keep the description as brief as possible, we will introduce our construction through the encryption model. Our goal is to design a solution that combines the benefits of identity- and attribute-based models: rapid client-side computation (independent from the complexities of access control) and flexible public keys.

The model we designed is based on IBE, thus we inherit a system where every entity has a public key, which is an identity and some linked domain-specific data. In the standard IBE model, this public key is also the encryption key. In our protocol, that is not the case. The main novelty of our model is the authorization expression, which is defined by the encryptor entity as an access policy, and that the public keys are used as authorization keys. Hence everyone whose public key satisfies the authorization expression is authorized to extract the belonging decryption key. This inspection is handled by the trusted Private Key Generator, which is also inherited from the IBE protocol. To stay within the bounds of IBE, the decryption and encryption key pair is still a valid IBE key pair. The encryption key is an extension of the encryptor entity's public key with a generated value. This value should be unique for every distinct authorization expression to prevent unauthorized decryptions.

Furthermore, to utilize the potential of the construction, we use formal languages in multiple segments of it. The most significant component employing this feature is the authorization expression, which is built from attribute constraints, concatenated with logical operators. Each attribute constraint comprises a formal language, defining which entities may have access and which may not. Hence, the protocol provides robust tools for defining a fine-grained access policy targeting an arbitrary group of entities.

In conclusion, we designed a protocol, which provides flexible access control, like the ABC schemes. Furthermore, we were able to keep the property of IBE, that the growth of the complexity of the access policy is not affecting the user-side computational cost. Thus we solved the bottleneck of ABC that requires much computational power both server and client-side. Considering the combination of these significant improvements in performance and key flexibility with modern and powerful technologies like WebAssembly, the model has potential in practical application. CryptID [5] provides a suitable base for this kind of future work.

References

1. Shamir, A. (1985). Identity-based Cryptosystems and Signature Schemes. Proceedings of CRYPTO 84 on Advances in Cryptology (pp. 47–53). New York, NY, USA: Springer-Verlag New York, Inc. http://dl.acm.org/citation.cfm?id=19478.19483
2. Boneh, D. & Franklin, M. K. (2001). Identity-Based Encryption from the Weil Pairing. Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (pp. 213–229). London, UK, UK: Springer-Verlag. http://dl.acm.org/citation.cfm?id=646766.704155
3. Goyal, V. & Pandey, O. & Sahai, A & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the ACM Conference on Computer and Communications Security (pp. 89-98). https://dl.acm.org/doi/10.1145/1180405.1180418.
4. Bethencourt, J. & Sahai, A. & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy (SP '07) (pp. 321-334). Berkeley, CA. https://doi.org/10.1109/SP.2007.11
5. Vécsi, Á. & Bagossy, A. & Pethő, A. (2019). Cross-platform Identity-based Cryptography using WebAssembly. Infocommunications Journal (Volume XI, Number 4) (pp. 31-38). https://doi.org/10.36244/ICJ.2019.4.5

Experimental algebraic differential cryptanalysis of SPN

Pavol Zajac * Alena Bednáriková

Slovak University of Technology in Bratislava, Slovakia

Extended Abstract

Algebraic cryptanalysis can be used to break (small versions of) block ciphers with small data complexity [1, 2]. Main principle of algebraic cryptanalysis is simple: Encryption is described by a set of equations between bits of plaintexts, ciphertexts, the unknown key, and inner states of the encryption algorithm. This set of equations is then solved by a suitable fast solver. SAT solvers can be combined with key bit guessing and massive parallel computing [3] to solve even relatively large systems.

In recent article [4], Andrzejczak and Dudzic attack smaller versions of block ciphers SIMON and SPECK. Instead of modeling whole cipher, they do not model key expansion algorithm, and instead try to find independent subkeys. This requires more plaintext-ciphertext (P-C) pairs than a standard algebraic cryptanalysis. Unfortunately, with growing number of P-C pairs, size of the system quickly increases, which increases the solving time.

If we have access to a large number of P-C pairs, algebraic cryptanalysis can be combined with differential techniques [5, 6, 7]. Attack is based on selected differential characteristic, which holds with high probability. This characteristic produces extra linear equations, which can be used to augment the original algebraic system. Based on this augmented system, algebraic solver can detect, whether the differential characteristic holds for a particular P-C pair, and to derive information about key bits.

In our research, instead of trying to break some specific cipher, we try to understand empirically the effect of having multiple P-C pairs, and of applying differential techniques on a simple Substitution Permutation Network model. In our experiments we use SAT representation and SAT solver CryptoMiniSat [8] integrated within SAGE [9].

In our experiments with algebraic differential cryptanalysis, we have developed a different technique to represent the system. Standard model produces a system of equations for each tuple of P-C pairs (supposedly connected by a differential characteristic) as a union of equations for encryption F_1, and F_2, along with linear equations describing a chosen differential. In our new method, we model a single encryption (only one of each 2 P-C pairs), but we apply the differential to restrict the equations that model active S-boxes. Suppose that differential characteristic goes through some S-box with input difference Δ_x and output difference Δ_y. We replace the original S-box equation, which has the solution set $\{(x, y); S(x) = y\}$, with the new equation with the solution set $\{(x, y); S(x) = y \wedge S(x+\Delta_x) = y+\Delta_y\}$. The number of additional clauses that express new restrictions based on differences is smaller than in the standard model. The important information about the chosen differential (equations on active S-boxes) is preserved (as well as the original solution of the whole cipher, if we use enough P-C pairs to avoid false keys).

System created with our new model is smaller, and can theoretically be solved faster. Our experiments show that the advantage depends on the overall number of P-C pairs available, and whether the chosen differential characteristic is correctly estimated. One of the advantages of the new method is that it can use a partial information from the differential, and

*This research was sponsored by Slovak Republic under grant VEGA 1/0159/17.

still determine a correct solution faster than both standard algebraic attack, and standard algebraic-differential attack.

Our experiments with CryptoMiniSAT in SAGE show an improvement over method A from [5] when increasing system size (by adding P-C pairs). However, a side effect of our model is that some of the pairs with incorrect difference are still suitable for algebraic attack, thus our attack can solve the system even in some cases when the differential is not preserved fully. When considering the overall complexity including rejection of incorrect pairs, full algebraic attack took in average 9.3s, while algebraic attack with fully determined difference 2.5s. If we apply the differential restrictions only on input and output layer of S-boxes (a truncated differential), we get the fastest attack with expected mean time 0.1s.

References

[1] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *International Conference on the Theory and Application of Cryptology and Information Security.* Springer, 2002, pp. 267–287.

[2] N. T. Courtois and G. V. Bard, "Algebraic cryptanalysis of the data encryption standard," in *IMA International Conference on Cryptography and Coding.* Springer, 2007, pp. 152–169.

[3] V. Hromada, L. Öllős, and P. Zajac, "Using sat solvers in large scale distributed algebraic attacks against low entropy keys," *Tatra Mountains Mathematical Publications*, vol. 64, no. 1, pp. 187–203, 2015.

[4] M. Andrzejczak and W. Dudzic, "Sat attacks on arx ciphers with automated equations generation," *Infocommunications*, vol. 9, no. 4, pp. 2–7, 2019.

[5] M. Albrecht and C. Cid, "Algebraic techniques in differential cryptanalysis," in *International Workshop on Fast Software Encryption.* Springer, 2009, pp. 193–208.

[6] J.-C. Faugère, L. Perret, and P.-J. Spaenlehauer, "Algebraic-differential cryptanalysis of des," in *Western European Workshop on Research in Cryptology-WEWoRC*, vol. 2009. Citeseer, 2009, pp. 1–5.

[7] M. Wang, Y. Sun, N. Mouha, and B. Preneel, "Algebraic techniques in differential cryptanalysis revisited," in *Australasian Conference on Information Security and Privacy.* Springer, 2011, pp. 120–141.

[8] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings*, ser. Lecture Notes in Computer Science, O. Kullmann, Ed., vol. 5584. Springer, 2009, pp. 244–257. [Online]. Available: https://doi.org/10.1007/978-3-642-02777-2_24

[9] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020, `https://www.sagemath.org`.