CECC 2015

15th Central European Conference on Cryptology

Klagenfurt am Wörthersee, Austria

July 8-10, 2015

Book of Abstracts

The 15th Central European Conference on Cryptology is organised by the Department of Mathematics and the System Security Group of Alpen-Adria-Universität Klagenfurt, with the financial contribution of Förderverein Technische Fakultät and the City of Klagenfurt.

Organisation

Programme Chairs

Clemens Heuberger, Alpen-Adria-Universität Klagenfurt, Austria
Stefan Rass, Alpen-Adria-Universität Klagenfurt, Austria

Programme Committee

Laszlo Csirmaz, Central European University, Budapest, Hungary
Özgür Dagdelen, Technische Universität Darmstadt, Germany
Andrej Dujella, University of Zagreb, Croatia
Otokar Grosek, Slovak University of Technology in Bratislava
Marek Klonowski, Wroclaw University of Technology, Poland
Tanja Lange, Technische Universiteit Eindhoven, Netherlands
Spyros S. Magliveras, Florida Atlantic University, USA
Florian Mendel, Graz University of Technology, Austria
Karol Nemoga, Slovak Academy of Sciences
Attila Pethő, University of Debrecen, Hungary
Štefan Porubský, Academy of Sciences of the Czech Republic
Vincent Rijmen, Katholieke Universiteit Leuven, Belgium
Martin Schaffer, NXP Semiconductors, Austria
Peter Schartner, Alpen-Adria-Universität Klagenfurt, Austria

Local Organisers

Benjamin Hackl
Clemens Heuberger
Sara Kropf
Michela Mazzoli
Stefan Rass
Anita Wachter

Conference Programme

Day 1: Wednesday, July 08, 2015

08:30 – 09:15	Registration
09:15 – 09:30	Welcome session
09:30 – 10:20	**Keynote 1: Andrey Bogdanov**
	Symmetric-Key Cryptography in Untrusted Environments
10:30 – 11:00	Coffee break

Session 1 (11:00 – 12:15, Chair: Karol Nemoga)

11:00 – 11:20	Stefan Rass, Peter Schartner, Markus S. Wamser
	Oblivious Lookup Tables
11:25 – 11:45	Tomas Fabsic, Otokar Grosek, Karol Nemoga, Pavol Zajac
	On Constructing Invertible Circulant Binary $(n \times n)$*-Matrices with* $\frac{n^2}{2}$ *Ones*
11:50 – 12:10	Georg Fuchsbauer, Christian Hanser, Daniel Slamanig
	Structure-Preserving Signatures on Equivalence Classes
12:15 – 13:45	Lunch break

Session 2 (13:45 – 15:00, Chair: Otokar Grosek)

13:45 – 14:05	Noora Nieminen, Valtteri Niemi, Tommi Meskanen
	Side-Information in Garbling
14:10 – 14:30	Michala Gulasova, Matus Jokay
	Stegoanalysis of StegoStorage System
14:35 – 14:55	Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Yurii Gorbenko, Viktor Dolgov
	A New Encryption Standard of Ukraine: The Block Cipher Kalyna
15:00 – 15:30	Coffee break
15:30 – 16:20	**Keynote 2: Vincent Rijmen**
	Threshold implementations

Session 3 (16:30 – 17:20, Chair: Andrey Bogdanov)

16:30 – 16:50	Iwona Polak, Mariusz Boryczka
	Breaking RC4 Using Genetic Algorithm
16:55 – 17:15	Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer
	Ascon, a Submission to CAESAR

Day 2: Thursday, July 09, 2015

09:30 – 10:20	**Keynote 3: Eran Tromer and Daniel Genkin** *Physical Side Channel Attacks on PCs*
10:30 – 11:00	Coffee break

Session 4 (11:00 – 12:15, Chair: Vincent Rijmen)

11:00 – 11:20	Sara Kropf, Clemens Heuberger *Scalar Multiplication on Elliptic Curves Using the Binary Asymmetric Joint Sparse Form*
11:25 – 11:45	Daniel Krenn, Clemens Heuberger *Properties of τ-adic Digit Expansions for Fast Scalar Multiplication*
11:50 – 12:10	Michela Mazzoli *Non-commutative Digit Expansions for Arithmetic on Supersingular Elliptic Curves*
12:15 – 13:45	Lunch break

Session 5 (13:45 – 15:00, Chair: Christian Hanser)

13:45 – 14:05	Martin Deutschmann, Sandra Lattacher, Michael Höberl, Christina Petschnigg, Naeim Safari *Quality Limitations on the Extraction of a PUF-based Cryptographic Key*
14:10 – 14:30	László Mérai, Arne Winterhof *On the Linear Complexity Profile of Certain Sequences Derived from Elliptic Curves*
14:35 – 14:55	Raivis Bēts, Jānis Buls *WELLDOC Property in Bi-ideals*
15:00 – 15:30	Coffee break

Session 6 (15:30 – 17:10, Chair: Keith Martin)

15:30 – 15:50	Géza Horváth, Pál Dömösi, József Gáll *Statistical Analysis of a Novel Cryptosystem Based on Automata Compositions*
15:55 – 16:15	Haydar Demirhan, Nihan Bitirim *Hypothesis Testing and Multiplicity in the Evaluation of Cryptographic Randomness*
16:20 – 16:40	Mateusz Buczek *Cryptanalysis of POLAWIS*
16:45 – 17:05	Pavol Zajac, Viliam Hromada, Ladislav Ollos *A Few Notes on Algebraic Cryptanalysis*
18:30	**Conference dinner** at the restaurant “Uni-Wirt”, Nautilusweg 11

Day 3: Friday, July 10, 2015

09:30 – 10:20	**Keynote 4: Keith Martin**
	Researching Cryptography: Reflections on Theory versus Practice
10:30 – 11:00	Coffee break

Session 7 (11:00 – 12:15, Chair: Daniel Genkin)

11:00 – 11:20	Máté Horváth
	Revocation in Distributed ABE-based Secure Storage Using Indistinguishability Obfuscation
11:25 – 11:45	Renata Kawa, Mieczysław Kula
	Access Structures Induced by Uniform Polymatroids
11:50 – 12:10	Péter Ligeti
	On Complexity of Secret Sharing Schemes on Access Structures with Rank Three
12:15 – 12:30	Farewell
12:30	Lunch

Keynote Talks

Symmetric-Key Cryptography in Untrusted Environments

Andrey Bogdanov, Technical University of Denmark

Traditionally, symmetric-key algorithms have been designed under the assumption that the computational environment is trustworthy. However, in the real world, computing bases can be compromised – e.g. due to malware, hardware Trojans, physical side channels, memory leakage, etc. Among others, recent revelations by the former CIA employee and NSA contractor Edward Snowden confirm the existence of global mass surveillance programs run by the U.S. government. This much stronger adversary poses a novel challenge to cryptography and calls for countermeasures that are able to thwart such attacks or at least to limit the damage.

This talk consists of three parts. First, we give a survey on the existing countermeasures in grey-box and white-box settings, as opposed to the classical black-box setting. Second, we propose a framework for modelling the stronger attacker that can have substantial control over the execution environment, as applied to symmetric-key ciphers. Next, we analyse the residual security of existing primitives such as AES in this setting. Finally, we approach the design of new primitives that can provide more security in untrusted environments.

Threshold Implementations

Vincent Rijmen, Katholieke Universiteit Leuven

Side-channel attacks exploit weaknesses of the implementation of cryptographic transformations, rather than mathematical weaknesses of the transformations themselves. The attacks form a real threat to systems that are being used daily.

In the last two decades, several approaches have been proposed to achieve secure implementations. Almost all these approaches have been proven to be unsuccessful because they start from assumptions on hardware and software computing platforms that are too idealised. In particular transient effects have been neglected.

We proposed the Threshold Implementation approach, which takes into account the imperfections of current implementation technologies and still produces secure implementations. Since the approach is based on multiparty computation techniques, it is possible to formally prove the security.

In this talk, we first explain the threshold implementation approach. Subsequently we show its central security theorem. Finally, we present the most recent developments.

Physical Side Channel Attacks on PCs

Eran Tromer and Daniel Genkin, Tel Aviv University

Can secret information be extracted from personal computers by measuring their physical properties from the outside? What would it take to extract whole keys from such fast and complex devices? We present myriads way to do so, including:

- Acoustic key extraction, using microphones to record the high-pitched noise caused by vibration of electronic circuit components during decryption.
- Electric key extraction exploiting fluctuations in the "ground" electric potential of computers. An attacker can measure this signal by touching the computer's chassis, or the shield on the remote end of Ethernet, VGA or USB cables.

- Electromagnetic key extraction, using a cheap radio to non-intrusively attack laptop computers.

The talk will discuss the cryptanalytic, physical and signal-processing principles of the attacks, and include live demonstrations.

Joint works with Adi Shamir, Eran Tromer, Lev Pachmanov and Itamar Pipman.
For further information see `http://www.tau.ac.il/~tromer/leisec`

Researching Cryptography: Reflections on Theory versus Practice

Keith Martin, Royal Holloway, University of London

For many centuries cryptography was a practical subject which was supported by very little background theory. The rise of computer networks and their applications has seen the importance of cryptography as a practical subject rise to the point that it is now an everyday technology. Alongside this cryptography has developed and, to an extent semi-matured, as a theoretical research area. But does the theory always match the practice, and vice versa? And does it matter? In this talk we reflect on these questions, while presenting a number of current research problems that are motivated by the application of cryptography to the real world (wherever that is).

Contributed Talks

Oblivious Lookup Tables

Stefan Rass, Universität Klagenfurt, Department of Applied Informatics

Joint work with Peter Schartner (Universität Klagenfurt, Department of Applied Informatics) and Markus S. Wamser (Technical University of Munich, Institute for Security in Information Technology)

We consider the following setting: let $f : X \to Y$ be a mapping between finite sets. Assume that the sizes of X and Y are sufficiently small to permit a specification of f via a lookup table. Let $E(m, \kappa)$ denote a group-homomorphic encryption of a message m under a key κ, where E can be symmetric or asymmetric. Let E be group-homomorphic in the sense that $E(m_1 \cdot m_2, \kappa) = E(m_1, \kappa) \cdot E(m_2, \kappa)$, where $\cdot$ denotes the respective group operations within the plain- and ciphertext space.

In this setting, we consider the following question: given E and an encrypted value $c = E(x, \kappa)$, can we compute $E(f(x), \kappa)$ without decrypting c? We call any such implementation of f an *Oblivious Lookup Table (OLT)*, as it shall effectively hide the evaluation of f, or equivalently, evaluate f only on ciphertexts by virtue of conventional homomorphic encryption.

Becoming more specifically, let $p = 2q + 1$ be a safe prime (i.e., q is a prime too), and let $\mathbb{G} \subset \mathbb{Z}_p$ denote the q-order subgroup generated by some element $g \in \mathbb{Z}_p$. We first describe the lookup technique in plain form, and subsequently wrap the encryption around the necessary operations.

Let $X = \{x_1, \ldots, x_n\} \subseteq \mathbb{G}$ be an enumeration of (distinct) values to be looked up. To each such element x_i we associate a vector $\vec{v}_i = (x_i^k)_{k=0}^{n-1} = (1, x_i, x_i^2, \ldots, x_i^{n-1})$. Notice that $x_i \neq x_j$ whenever $i \neq j$ implies that the vectors $\vec{v}_1, \ldots, \vec{v}_n$ are all linearly independent, as they essentially form the rows of a Vandermonde matrix $\vec{V}$. Without loss of generality, let us assume $|X| = n = |Y|$, say, by allowing multiple occurrences of the same element in Y in case that f is not injective. Under this convention, let the (not necessarily pairwise distinct) elements of Y be enumerated as $Y = \{y_1, \ldots, y_n\}$.

We will construct the value of $f(x_i)$ by a scalar product of $\vec{v}_i$ with a vector representation of the lookup table. That is, the lookup table itself is a vector $\vec{\ell}$ with the property that $\vec{v}_i^T \cdot \vec{\ell} = f(x_i)$ for all $i = 1, 2, \ldots, n$. To this end, let us choose an arbitrary but invertible matrix $\vec{U} \in \mathbb{G}^{n \times n}$ with columns $\vec{u}_1, \ldots, \vec{u}_n$. Define the lookup table as $\vec{\ell} := \vec{U} \cdot \vec{\alpha}$ for some (yet to be determined) vector $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Now, let us look at the scalar product of $\vec{v}_i$ with $\vec{U} \cdot \vec{\alpha}$ to yield $f(x_i) \in \mathbb{Z}_p$. This results in a linear equation $\alpha_1(\vec{v}_i^T \cdot \vec{u}_1) + \alpha_2(\vec{v}_i^T \cdot \vec{u}_2) + \cdots + \alpha_n(\vec{v}_i^T \cdot \vec{u}_n) = f(x_i)$. Establishing this condition for all $i = 1, 2, \ldots, n$, we end up observing that, to find $\vec{\alpha}$, we need to solve the linear system $(\vec{V} \cdot \vec{U}) \cdot \vec{\alpha} = (f(x_1), \ldots, f(x_n))^T$ for $\vec{\alpha}$. The coefficient matrix $\vec{V} \cdot \vec{U}$ is invertible by construction, and hence we can easily look up values $f(x_i)$ by computing $f(x_i) = \vec{v}_i^T \cdot \vec{\ell}$, taking $O(n)$ multiplications and additions.

Now, let us see if we can equivalently do all the necessary steps when the pre-image is encrypted. For that matter, we take an element-wise commitment to the $\vec{v}_i$ from above to represent x_i. That is, the value x_i now comes committed and encrypted as $\tilde{E}(x_i, \kappa) := (E(1, \kappa), E(g^{x_i}, \kappa), E(g^{x_i^2}, \kappa), \ldots, E(g^{x_i^{n-1}}, \kappa)) = (c_1, \ldots, c_n)$, so that the matrix of exponents remains $\vec{V} = (v_{ij})_{i,j=1}^n$ with $v_{ij} = x_i^{j-1}$ and as such invertible. Since the order of $\mathbb{G}$ is a prime, we can – in a setup phase where the exponents are known – straightforwardly work out the values $\vec{\alpha}$ and the lookup table $\vec{\ell} = (\ell_1, \ldots, \ell_n)$, which is supplied in plain (not encrypted) form to the instance that seeks to evaluate f.

To evaluate f, let the encrypted input value x_i be given as $\tilde{E}(x_i, \kappa)$. Then, we can compute the lookup value $E(f(x_i), \kappa)$ as

$$\begin{aligned}\prod_{k=1}^{n} c_k^{\ell_k} &= \prod_{k=1}^{n} E(g^{x_i^{k-1}}, \kappa)^{\ell_k} = \prod_{k=1}^{n} E(g^{v_{ik}}, \kappa)^{\alpha_1 u_{k1} + \alpha_2 u_{k2} + \ldots \alpha_n u_{kn}} \\ &= \prod_{k=1}^{n} E(g^{\alpha_1 v_{ik} u_{k1} + \alpha_2 v_{ik} u_{k2} + \ldots + \alpha_n v_{ik} u_{kn}}, \kappa) = E(g^{f(x_i)}, \kappa). \qquad (1)\end{aligned}$$

The last equality is instantly obtained by writing out the exponents for $k = 1, 2, \ldots, n$ and rearranging terms properly when summing up.

A final remark is judicious here: the formula yields only a single value based on an input vector. To properly implement the lookup to be *repeatable*, i.e., to model iterations like $f(f(\cdots f(x)\cdots))$ or generally functions $f : X \to X$, we need to look up all the elements of the output vector via separate tables. So, the overall lookup table is no longer a n-dimensional vector, but an $(n \times n)$-matrix $\vec{L} = (\vec{\ell}_1, \ldots, \vec{\ell}_n)$. The j-th such lookup table $\vec{\ell}_j$ must then be designed to return y^{j-1}, whenever the input value x is represented by a sequence $1, x, x^2, \ldots, x^{n-1}$ in the exponents. That is, the mapping $f(x) = y$, acting on x being represented by encrypted values $1, g^x, g^{x^2}, \ldots, g^{x^{n-1}}$, requires n lookups that successively yield $1, g^y, g^{y^2}, \ldots, g^{y^{n-1}}$, each of which by (1) requires $O(n)$ exponentiations and multiplications. So, the total cost of an oblivious lookup comes to $O(n^2)$ exponentiations (subsuming multiplications as the cheaper operation here).

Security of an OLT is defined in terms of the adversaries inability to infer anything about x or $f(x)$ from $\vec{L}$ and its encrypted input $E(x, pk)$. This kind of security (against passive and active attacks) follows immediately from our construction and the security of the encryption, since x and $f(x)$ remain encrypted at all times, and the lookup table – despite being available in plain form – is independent of a particular input, thus cannot release any information about x or $f(x)$. Probabilistic encryptions like ElGamal can offer the additional appeal of enforced re-randomization of the resulting ciphertexts. That is, if a distrusted third party does several lookups, it nevertheless cannot recognize any results as being identical to previous ones.

This work closely relates to Private Function Evaluation (PFE), which provides a system where the function-to-be-evaluated f *and* the inputs are private and the evaluator learns nothing about either aside from the (encrypted) results of the evaluation of the function on the inputs. This can be realized using Secure Function Evaluation (SFE) over a universal circuit ([4, 7]), to which f has to be converted first. Another approach is to use a (non-universal) circuit representation of f and employ a Fully Homomorphic Encryption (FHE) scheme [2, 6]. However, all mentioned approaches carry complexities that are too high for practical applications. Conceptually closest to our ideas seem to be [3] and [5], both based on singly homomorphic encryption. The former realises PFE in a strict two-party setting with one party providing the function and the other providing the inputs. Evaluation is done through a common virtual machine. The latter is based on a framework that splits the task into Circuit Topology Hiding (CTH) and Private Gate Evaluation (PGE) which together enable PFE with linear complexity in all standard settings. However, both PFE protocols require an interactive setting while we are aiming for the non-interactive setting. The security implications tied to our simple scheme when being lifted to two-operand functions (if that is possible at all) are, however, far from clear and probably intricate (cf. [1]) and will be discussed along the research sketched in this abstract.

References

[1] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In *Proceedings of the 8th conference on Theory of cryptography (TCC)*, TCC'11, pages 253–273, Berlin, Heidelberg, 2011. Springer.

[2] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, STOC '09, pages 169–178, New York, NY, USA, 2009. ACM.

[3] Jonathan Katz and Lior Malka. Constant-Round private function evaluation with linear complexity. In DongHoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 556–571. Springer Berlin Heidelberg, 2011.

[4] Vladimir Kolesnikov and Thomas Schneider. A practical universal circuit construction and secure evaluation of private functions. In Gene Tsudik, editor, *Financial Cryptography and Data Security*, volume 5143 of *Lecture Notes in Computer Science*, pages 83–97. Springer Berlin Heidelberg, 2008.

[5] Payman Mohassel and Saeed Sadeghian. How to hide circuits in MPC an efficient framework for private function evaluation. In Thomas Johansson and PhongQ Nguyen, editors, *Advances in Cryptology EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 557–574. Springer Berlin Heidelberg, 2013.

[6] Alice Silverberg. Fully homomorphic encryption for mathematicians. Cryptology ePrint Archive, Report 2013/250, 2013. `http://eprint.iacr.org/`.

[7] Leslie G. Valiant. Universal circuits (preliminary report). In *Proceedings of the Eighth Annual ACM Symposium on Theory of Computing*, STOC '76, pages 196–203, New York, NY, USA, 1976. ACM.

Acronyms

OLT: Oblivious Lookup Table
CTH: Circuit Topology Hiding
FHE: Fully Homomorphic Encryption
PFE: Private Function Evaluation
PGE: Private Gate Evaluation
SFE: Secure Function Evaluation

On constructing invertible circulant binary $(n \times n)$-matrices with $\frac{n^2}{2}$ ones

Tomáš Fabšič, Slovak University of Technology in Bratislava
Joint work with Otokar Grošek, Karol Nemoga and Pavol Zajac

Circulant binary matrices are frequently employed in modern cryptology and thus the need to study circulant binary matrices with favourable additional properties arises.

An important subset of circulant binary matrices is the set of invertible circulant binary matrices. Here, and in the rest of the paper, we always mean invertibility over $GF(2)$. Invertible circulant matrices over $GF(q)$, where q is a power of a prime, were studied by e.g. Jungnickel in [3]. Among other results, Jungnickel gives a formula for the number of invertible circulant $(n \times n)$-matrices over $GF(q)$.

Another important property of circulant binary matrices is their density. The total number of ones in a circulant binary $(n \times n)$-matrix has to be a multiple of n. Since a circulant matrix is fully determined by its first row, it is easy to see that the number of circulant binary $(n \times n)$-matrices with $n \times t$ ones is $\binom{n}{t}$, for $0 \leq t \leq n$. However, it is not clear how many of these matrices are invertible.

To our knowledge, the sets of invertible circulant binary $(n \times n)$-matrices with fixed density have not been studied in the literature yet. Let $C_{inv,t}(n)$ be the set of invertible circulant binary $(n \times n)$-matrices with $n \times t$ ones. By an easy argument, presented in this paper, one can show that a necessary condition for the set $C_{inv,t}(n)$ to be nonempty is that t has to be odd:

Lemma 1. *Let $t = 0 \pmod 2$. Every circulant $(n \times n)$-matrix over $\mathbb{Z}_2$ with $n \times t$ ones is singular.*

In the present paper, we focus our attention on the set $C_{inv,\frac{n}{2}}(n)$. The study of the sets $C_{inv,t}(n)$ for $t \neq \frac{n}{2}$ is a subject of our ongoing research.

The set $C_{inv,\frac{n}{2}}(n)$ is ill-defined for odd n and, by Lemma 1, is empty for $n = 0 \pmod 4$. Hence, we can only hope to find invertible circulant binary $(n \times n)$-matrices with $\frac{n^2}{2}$ ones when $n = 2 \pmod 4$. The main result of the present paper is a construction of a large set of matrices belonging to $C_{inv,\frac{n}{2}}(n)$, for $n = 2 \pmod 4$. To this end, we use the following facts from [3]:

Fact 1 (Proposition 1.7.1 in [3])**.** *Consider the mapping τ which sends the circulant binary $(n \times n)$-matrix with the first row $(c_0, c_1, c_2, \ldots, c_{n-1})$ onto the coset of the polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$. Then the mapping τ is an isomorphism between the ring of circulant binary $(n \times n)$-matrices and the ring $\mathbb{Z}_2[x]/(x^n + 1)$.*

Fact 2. *A circulant $(n \times n)$-matrix C over $\mathbb{Z}_2$ is invertible if and only if $\tau(C)$ is relatively prime to $x^n + 1$.*

These facts tell us that in order to find an invertible circulant binary $(n \times n)$-matrix with $\frac{n^2}{2}$ ones, it suffices to look for a polynomial of weight $\frac{n}{2}$ in $\mathbb{Z}_2[x]/(x^n+1)$ which is relatively prime to x^n+1. In the main theorem presented in our paper, we construct a large class of such polynomials for every $n = 2 \pmod 4$. The idea behind our construction is as follows:

(1) We observe that for $n = 2 \pmod 4$ we have:

$$x^n + 1 = (x+1)^2 \cdot q(x),$$

where $q(x) = x^{n-2} + x^{n-4} + \cdots + x^2 + 1$, and that $q(x)$ has weight $\frac{n}{2}$.

(2) We alter the polynomial $q(x)$ to produce polynomials of weight $\frac{n}{2}$, which are relatively prime to $x^n + 1$.

Thus, we arrive at:

Theorem 1. *Let $n = 2 \pmod 4$. Let $q(x) = x^{n-2} + x^{n-4} + \cdots + x^2 + 1$. Consider the set:*

$$\begin{aligned}\mathbb{A}_n = \{c(x) \in \mathbb{Z}_2[x]/(x^n+1) \quad : \quad & c(x) = x^t \cdot (q(x) + a^2(x) + x^k \cdot a^2(x)),\\ & a(x) \in \mathbb{Z}_2[x]/(x^n+1),\\ & \gcd(a(x), q(x)) = 1,\\ & t, k \in \mathbb{Z}_n, \quad \gcd(k, n) = 1 \quad \}.\end{aligned}$$

Then:

(1) *Every $c(x) \in \mathbb{A}_n$ has $\frac{n}{2}$ terms and is relatively prime to $x^n + 1$ in $\mathbb{Z}_2[x]$.*

(2) *Every $c(x) \in \mathbb{A}_n$ can be uniquely expressed in the form:*

$$c(x) = q(x) + b^2(x) + x^s b^2(x),$$

where:

- $b(x) \in \mathbb{Z}_2[x]/(x^n+1)$, $\deg(b(x)) < n/2$,
- $\gcd(b(x), q(x)) = 1$,
- $s \in \mathbb{Z}_n^*$.

(3) $|\mathbb{A}_n| = 2 \times \psi(x^{\frac{n}{2}} + 1) \times \phi(n)$.

The theorem gives a recipe to construct the set $\tau^{-1}(\mathbb{A}_n) = \{\tau^{-1}(c(x)) \, : \, c(x) \in \mathbb{A}_n\}$ of invertible circulant binary $(n \times n)$-matrices containing $\frac{n^2}{2}$ ones with cardinality:

$$\left|\tau^{-1}(\mathbb{A}_n)\right| = 2 \times \psi(x^{\frac{n}{2}} + 1) \times \phi(n).$$

Here $\phi(n)$ denotes the Euler function, and $\psi(x^{\frac{n}{2}}+1)$ denotes the number of polynomials of smaller degree which are relatively prime to $x^{\frac{n}{2}} + 1$ in $\mathbb{Z}_2[x]$. In [3], Jungnickel presents the following formula for $\psi(x^{\frac{n}{2}} + 1)$, when $n = 2 \pmod 4$:

$$\psi(x^{\frac{n}{2}} + 1) = 2^{\frac{n}{2}} \prod_{d \mid \frac{n}{2}} \left(1 - 2^{-o_d(2)}\right)^{\phi(d)/o_d(2)}.$$

In the formula, $o_d(2)$ denotes the order of 2 in the group $\mathbb{Z}_d^*$.

In order to make the dependance of $\left|\tau^{-1}(\mathbb{A}_n)\right|$ on n more explicit, we also present some estimates of $\left|\tau^{-1}(\mathbb{A}_n)\right|$. Using the estimates from [2] (Thm. 2.1) and [1] (Thm. 8.8.7) for ψ and ϕ respectively, we obtain a lower bound for $\left|\tau^{-1}(\mathbb{A}_n)\right|$:

$$\left|\tau^{-1}(\mathbb{A}_n)\right| \geq 2 \times \frac{2^{n/2}}{e^{\gamma + 1/2(1+\log_2(n/2))}\,(1 + \log_2(n/2))} \times \frac{n}{e^{\gamma} \log\log n + \frac{3}{\log\log n}} \quad \text{for } n > 2.$$

where $\gamma = 0.577216\ldots$ is the Euler constant. We also have a trivial upper bound for $\left|\tau^{-1}(\mathbb{A}_n)\right|$:

$$\left|\tau^{-1}(\mathbb{A}_n)\right| \leq 2 \times 2^{n/2} \times (n-1).$$

Our experiments, however, suggest that the number of all invertible circulant binary $(n \times n)$-matrices with $\frac{n^2}{2}$ ones is significantly larger than $\left|\tau^{-1}(\mathbb{A}_n)\right|$. Thus, it remains an open problem to determine the cardinality of $C_{inv,\frac{n}{2}}(n)$.

It is easy to observe that a circulant binary $(n \times n)$-matrix with $\frac{n^2}{2}$ ones contains $\frac{n}{2}$ ones in every row and every column. In applications, one might need to construct invertible binary $(n \times n)$-matrices with row and column sums $\frac{n}{2}$, not insisting on matrices being circulant. Matrices of the form $P \times C \times Q$, where P and Q are $(n \times n)$ permutation matrices and $C \in \tau^{-1}(\mathbb{A}_n)$, satisfy these conditions. Thus the set $\tau^{-1}(\mathbb{A}_n)$ can be used to construct a large set of invertible binary $(n \times n)$-matrices with row and column sums $\frac{n}{2}$. Let us denote this set by $\mathbb{B}_n$:

$$\begin{aligned}\mathbb{B}_n = \{B = P \times C \times Q \quad : \quad & C \in \tau^{-1}(\mathbb{A}_n), \\ & P, Q \in (\mathbb{Z}_2)^{n \times n} \text{ are permutation matrices}\}.\end{aligned}$$

We also consider the following subset $\mathbb{D}_n$ of the set $\mathbb{B}_n$:

$$\begin{aligned}\mathbb{D}_n = \{D = P \times C \quad : \quad & C \in \tau^{-1}(\mathbb{A}_n), \\ & P \in (\mathbb{Z}_2)^{n \times n} \text{ is a permutation matrix}\}.\end{aligned}$$

We prove:

Lemma 2. $|\mathbb{D}_n| = (n-1)! \times |\mathbb{A}_n|$.

Thus, at least $(n-1)! \times |\mathbb{A}_n|$ invertible binary $(n \times n)$-matrices with row and column sums $\frac{n}{2}$ can be constructed from the matrices in $\tau^{-1}(\mathbb{A}_n)$.

References

[1] Eric Bach, Jeffrey Shallit, *Algorithmic Number Theory: Efficient Algorithms, Vol. 1.*, MIT press, (1996).

[2] Shuhong Gao, Daniel Panario, *Density of Normal Elements*, Finite Fields and Their Applications **3(2)**, (1997), 141–150.

[3] Dieter Jungnickel, *Finite Fields: Structure and Arithmetics*, BI Wissenschaftsverlag, (1993).

[4] Rudolf Lidl, Harald Niederreiter, *Finite Fields*, Cambridge University Press, (1997).

Structure-Preserving Signatures on Equivalence Classes

Christian Hanser, Graz University of Technology

Joint work with Georg Fuchsbauer (IST Austria) and Daniel Slamanig (Graz University of Technology)

Structure-preserving signature (SPS) schemes [1] are signature schemes whose message space are (vectors of) elements of a bilinear group without requiring any prior encoding of messages to group elements. In such schemes, one operates in a group setting equipped with a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, and public keys, messages and signatures consist only of group elements and the verification algorithm evaluates a signature by deciding group membership of signature elements and by evaluating pairing-product equations (PPEs). SPS are particularily attractive for numerous privacy-related applications such as (delegatable) anonymous credentials, group signatures and blind signatures, as they are compatible with the Groth-Sahai (GS) proof framework [11] (the latter yielding non-interactive zero-knowledge proofs that do not require random oracles). Over the last years various lower bounds and impossibility results have been shown and different (optimal) constructions with respect to number of group elements or number of pairing product equations have been proposed [2, 3, 7, 4, 5].

SPS schemes on equivalence classes (SPS-EQ-$\mathcal{R}$) are a specific variant of SPS and have been proposed by Hanser and Slamanig [12]. The idea behind SPS-EQ-$\mathcal{R}$ is as follows. For a prime p, $\mathbb{Z}_p^\ell$ is a vector space. Thus, if $\ell > 1$ one can define a projective equivalence relation on it, which propagates to $\mathbb{G}_i^\ell$ and partitions $\mathbb{G}_i^\ell$ into equivalence classes. Let $\sim_{\mathcal{R}}$ be this relation, i.e., $M \sim_{\mathcal{R}} N \Leftrightarrow \exists\, s \in \mathbb{Z}_p^* : M = sN$ where $M, N \in \mathbb{G}_i^\ell$. An SPS-EQ-$\mathcal{R}$ scheme signs an equivalence class $[M]_{\mathcal{R}}$ for $M \in (\mathbb{G}_i^*)^\ell$ by actually signing a representative M of $[M]_{\mathcal{R}}$. It, then, allows to switch to other representatives of $[M]_{\mathcal{R}}$ and to update the corresponding signature without having access to the secret key. An important property of SPS-EQ-$\mathcal{R}$ is that two message-signature pairs corresponding to the same class should be unlinkable. Although there are various types of linearly homomorphic SPS schemes [13, 6], none of them provides this unlinkability property (they are either trivially linkable or forgeable otherwise) and it turns out that this is not easy to achieve. The first instantiation of SPS-EQ-$\mathcal{R}$ only provides security against random message attacks (RMA) (cf. [8] and the updated version of [12]), but together with Fuchsbauer [9] they subsequently presented the first scheme that provides security under adaptively chosen message attacks (EUF-CMA), which is proven secure in the generic group model.

SPS-EQ-$\mathcal{R}$ turned out to be an interesting concept. Besides their applicability to efficient attribute-based multi-show anonymous credential systems (cf. [12]), they can be used to efficiently construct other well-known cryptographic primitives such as very efficient round-optimal blind signatures (without GS proofs) and in the standard model [10] or standard model instantations of verifiably encrypted signatures. Moreover, it can be shown that any SPS-EQ-$\mathcal{R}$ scheme that signs equivalence classes of $(\mathbb{G}_i^*)^{\ell+1}$ with $\ell > 1$ can be turned into a corresponding SPS scheme signing vectors of $(\mathbb{G}_i^*)^\ell$.

In this talk we first introduce the concept of SPS-EQ-$\mathcal{R}$, present existing instantiations and present several recent results on their application as well as limitations.

References

[1] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, *Structure-Preserving Signatures and Commitments to Group Elements*, CRYPTO 2010, LNCS, vol. 6223, Springer, 2010, pp. 209–236.

[2] Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, *Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups*, CRYPTO 2011, LNCS, vol. 6841, Springer, 2011, pp. 649–666.

[3] Masayuki Abe, Jens Groth, and Miyako Ohkubo, *Separating Short Structure-Preserving Signatures from Non-interactive Assumptions*, ASIACRYPT 2011, LNCS, vol. 7073, Springer, 2011, pp. 628–646.

[4] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi, *Structure-Preserving Signatures from Type II Pairings*, CRYPTO 2014, LNCS, vol. 8616, Springer, 2014, pp. 390–407.

[5] ———, *Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures*, TCC 2014, LNCS, vol. 8349, Springer, 2014, pp. 688–712.

[6] Nuttapong Attrapadung, Benoît Libert, and Thomas Peters, *Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures*, Public Key Cryptography 2013, LNCS, vol. 7778, Springer, 2013, pp. 386–404.

[7] Jan Camenisch, Maria Dubovitskaya, and Kristiyan Haralambiev, *Efficient Structure-Preserving Signature Scheme from Standard Assumptions*, SCN 2012, LNCS, vol. 7485, Springer, 2012, pp. 76–94.

[8] Georg Fuchsbauer, *Breaking Existential Unforgeability of a Signature Scheme from Asiacrypt 2014*, Cryptology ePrint Archive, Report 2014/892, 2014, `http://eprint.iacr.org/`.

[9] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig, *EUF-CMA-Secure Structure-Preserving Signatures on Equivalence Classes*, Cryptology ePrint Archive, Report 2014/944, 2014, `http://eprint.iacr.org/`.

[10] ———, *Practical Round-Optimal Blind Signatures in the Standard Model*, CRYPTO 2015, LNCS, Springer, 2015, to appear.

[11] Jens Groth and Amit Sahai, *Efficient Non-interactive Proof Systems for Bilinear Groups*, EUROCRYPT 2008, LNCS, vol. 4965, Springer, 2008, pp. 415–432.

[12] Christian Hanser and Daniel Slamanig, *Structure-Preserving Signatures on Equivalence Classes and their Application to Anonymous Credentials*, ASIACRYPT 2014, LNCS, vol. 8873, Springer, 2014, Full version: Cryptology ePrint Archive, Report 2014/705, pp. 491–511.

[13] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung, *Linearly Homomorphic Structure-Preserving Signatures and Their Applications*, CRYPTO 2013, LNCS, vol. 8043, Springer, 2013, pp. 289–307.

Side-information in Garbling

Noora Nieminen, University of Turku and Turku Centre for Computer Science (TUCS)
Joint work with Tommi Meskanen and Valtteri Niemi

1. Brief introduction to garbling schemes

Garbling techniques have been studied since Yao proposed his circuit-garbling technique in [11]. Since then, similar techniques have been used to develop further protocols for secure multiparty computation. Recently, the various garbling techniques have been formalized by Bellare et al. to *garbling schemes* [2]. According to [2], the syntactic framework of garbling scheme is independent of the representation of the computation method which is garbled. Using other words, the same framework would fit not only circuits but also Turing machines (TM), random-access machines (RAM), deterministic finite automata (DFA) and beyond. Many different computational models have been used in context of garbling – methods to garble Turing machines (garbled TM [4] and RAM's [6, 3]) among others have recently been developed.

The security of a garbling scheme is an important concept from practical and theoretical point of view. Several security definitions for garbling schemes have been introduced in [2, 1, 7, 8, 9]. These definitions also include different levels of security thus providing flexibility to the use and implementation of garbling schemes. A central concept in defining the security of garbling schemes is the concept of *side-information*, modelling the information that is allowed to be leaked during the garbled evaluation of the private functions. It is important to define the side-information correctly, since it plays a central role in security. It is obvious that the model of side-information is dependent on the computation model – circuits can leak different information than Turing machines.

Side-information is used to parametrize the security of garbling schemes. Since there is a wide variety of different side-information functions, the choice of an appropriate side-information function is important from the practical point of view. The application in which garbling is used determines what kind of side-information functions can be chosen, because the information allowed to be leaked varies in different applications. In some situations, nothing about the function should be leaked, whereas in some situations it is acceptable that the function is totally leaked (in which case the function would not be private anymore). As an example, Bellare et al. have implemented two efficient garbling schemes `Garble1` and `Garble2`. The former hides the function and the argument but the topology of the circuit is allowed to be leaked.

Generalizing the side-information function has also further advantages. Recently, Ishai and Wee have introduced the concept of *partial garbling scheme* [5]. A partial garbling scheme is designed for a situation in which the argument x contains partly public and partly private information. According to [5], the term *public* means information that is allowed to be leaked about x during the garbled evaluation. It is hard to imagine that this feature would be reached using Bellare et al.'s model of side-information function that is based on information deducible from f solely.

Moreover, Meskanen et al. have proposed a new way to perform the garbling. In *reverse order* garbling, first the argument is garbled and only then the function is garbled [8]. In this model, the side-information about the argument should be leaked when the argument is garbled. In the case of circuits, this can be achieved by fixing the lengths of argument x, the final value y and the length of function f beforehand as was done in [8]. In the case of Turing machines, it is not reasonable to restrict the length of argument x in the computation. Hence, the length of x should be leaked in another way. This is modelled by a side-information function which depends only on x and usually reveals only the length of x (but may also reveal other information about the argument, e.g. how many zeros and ones there are in the bit representation of x).

To summarize, there are several reasons to improve the concept of side-information function. The current side-information depends only on f even though, according to the above reasoning, it should depend on both the function f and argument x. In this paper we introduce a generalized model in which the side-information may depend on argument x, in addition to dependence of

f. Our side-information function can be used to define security of partial garbling schemes. In addition, our new model supports better the other computation models in garbling.

2. Issues in current definitions of side-information

Since the side-information plays a central role in the security definitions of garbling schemes, the side-information must be defined in an appropriate way. A garbling scheme is not tied to any specific model of computation, hence the definition of side-information cannot rely on specific features of a computation model. Unfortunately, the definition of side-information used in [2] is not fully supporting other computation models than circuits.

One reason why the definition of side-information function does not fully support for example Turing machines is the following. In the case of logical circuits, the argument x does not affect how the function f is evaluated. For example, the running time of a circuit is constant and does not depend on the chosen argument. Therefore, it is acceptable for circuits that the model of side-information function in [2] depends only on the function f. However, Turing machines do not have this same property.

Another reason is that, according to [2], the side-information always leaks at least the length of the representations of f, x and y. Since the side-information function in the model of Bellare et al. depends only on f, the lengths of x and y must be derivable from the function f alone. This is another property that does not fit Turing machines.

Thirdly, the model as in [1] does not fully take into account all the security threats during the garbled evaluation. Different types of attacks can reveal information about f, x and y. Following only the execution of encryption algorithm and capturing X may reveal something about the argument x. If the adversary can follow the execution of garbling algorithm and capture F then the adversary finds something about function f only. Thirdly, if the adversary possesses F and X and is able to follow the execution of decryption algorithm, then the adversary finds out something about the evaluation $\texttt{ev}(f, x)$. The different targets of attacks also suggest that there are different components modelling the information available to the adversary: information about x solely, information about f solely and information based on both f and x. Figure 2 illustrates the possible attacks of an adversary during the garbled evaluation process.

3. Generalizing side-information and security definitions in garbling

In this paper, we show how the side-information function should be generalized so that the independence from the model of computation would be truly achieved. In the current model, the side-information function depends only on f. In our new model the side-information function depends also on the argument x. The rationale for defining the side-information as a function of (f, x) is the following. An adversary attacking the security of a garbling scheme can get information from any of the algorithms $\texttt{Gb}$, $\texttt{En}$, $\texttt{De}$ and $\texttt{Ev}$. The total side-information depending on (f, x) represents the maximum information that is allowed to be leaked about the garbling process. For technical reasons, the side-information $\Psi(f, x)$ is divided into three components. The first component consists of information related only to the argument x, the second component leaks information about f only and the third component consists of information that depends on both f and x. It might be that some of these components are missing.

Even though we have changed the model, this is not the case for the generalized model of side-information and the security classes that are defined by the new side-information function. We have proven that the old security classes are exactly the same classes as the new ones when the side-information function Ψ is chosen in an appropriate manner and the model of computation for f is restricted to circuits.

We also prove that the hierarchy for classes of garbling schemes remains the same even though the model of side-information is changed. This applies to all garbling schemes in [7, 8, 9, 10].

To conclude, we have been able to create a generic model of side-information function that does not restrict the model of computation used for representing f. Moreover, we have obtained simple and practical security definitions for garbling schemes. In other words, we have now generic definitions

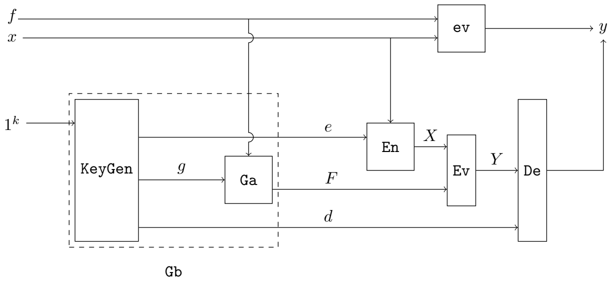


FIGURE 1. The idea of garbling. The value y must be the same despite of the way of evaluation, i.e. $\mathtt{ev}(f, x) = y = \mathtt{De}(d, \mathtt{Ev}(F, X))$.

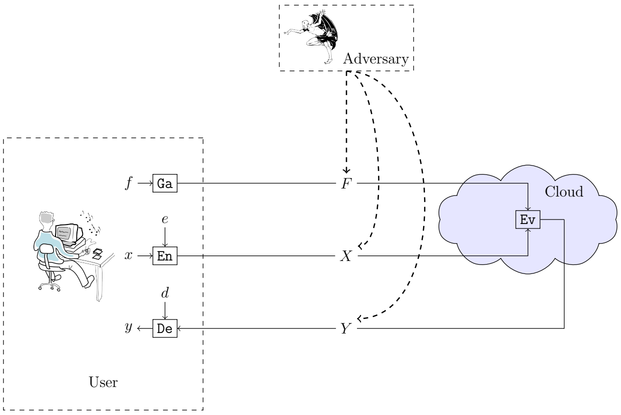


FIGURE 2. Diagram illustrating the possible attacks for an adversary. The dotted lines show possible targets for side-channel attacks. The dashed lines illustrate the attacks to directly retrieve information.

that can be used to design secure garbled circuits, secure garbled Turing machines and secure garbled versions of other computation models.

REFERENCES

[1] M. Bellare, V. T. Hoang, and P. Rogaway, *Adaptively secure garbling scheme with applications to one-time programs and secure outsourcing*, Proc. of Asiacrypt 2012, vol. 7685 of LNCS, Springer, 2012, pp. 134–153.

[2] ———, *Foundations of garbled circuits*, Proc. of ACM Computer and Communications Security (CCS'12), ACM, 2012, pp. 784–796.

[3] C. Gentry, S. Halevi, S. Lu, R. Ostrovsky, M. Raykova, and D. Wichs, *Garbled ram revisited*, Proc. of 33^{rd} Eurocrypt, vol. 8441 of LNCS, 2014, pp. 405–422.

[4] S. Goldwasser, Y. Kalai, R. Popa, V. Vaikuntanathan, and N. Zeldovich, *How to run turing machines on encrypted data*, Proc. of 33^{rd} CRYPTO, vol. 8043 of LNCS, 2013, pp. 536–553.

[5] Yuval Ishai and Hoeteck Wee, *Partial garbling schemes and their applications*, Automata, Languages, and Programming (Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, eds.), Lecture Notes in Computer Science, vol. 8572, Springer Berlin Heidelberg, 2014, pp. 650–662.

[6] S. Lu and R. Ostrovsky, *How to garble ram programs*, Proc. of 32^{nd} Eurocrypt, vol. 7881 of LNCS, 2013, pp. 719–734.

[7] T. Meskanen, V. Niemi, and N. Nieminen, *Classes of garbled schemes*, Infocommunications Journal **V** (2013), no. 3, 8–16.

[8] ———, *Garbling in reverse order*, The 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-14), 2014.

[9] ———, *Hierarchy for classes of garbling schemes*, Proc. of Central European Conference on Cryptology (CECC'14), 2014.

[10] ———, *On reusable projective garbling schemes*, 2014 IEEE International Conference on Computer and Information Technology (CIT 2014), 2014.

[11] A. Yao, *How to generate and exchange secrets*, Proc. of 27^{th} FOCS, 1986., IEEE, 1986, pp. 162–167.

Steganalysis of Stegostorage System[1]

Michala Gulášová, Slovak University of Technology
Joint work with Matúš Jókay

1. Introduction

The need for encrypted communication is still growing. With the raise in importance of cryptography, "invisible" encrypted information becomes a more important issue, too. Only steganography can provide this "masking". It allows to hide any ongoing communication, whether encrypted or not. The opposite pole of steganography is steganalysis. Its main objective is to detect such a stealth communication. Therefore, we consider this other side of steganography as an interesting object of study.

The main focus of this contribution is the detection of messages possibly present in JPEG images, specifically the messages inserted through a system called StegoStorage. This system is able to hide a single message into hundreds or thousands of images, making the detection more difficult. It makes use of embedding into the least significant bit of DCT coefficients, which can be sequential, pseudo-random but can also make use of Hamming codes [3]. Our aim is to achieve detectability of sequential embedding with the full capacity of filling a carrier medium.

This contribution is divided into three sections. In the first section, we present our mathematical model, which is necessary for expressing the dependency of pairs of values. In the second section, we explain the importance of calibration method. In the last section, we take a look at the reached results.

2. Mathematical Model

This section has been written in compliance with [1] and [2].

Let $h_{kl}(d)$ be the total number of AC DCT coefficients in the cover image corresponding to the frequency (k, l), $1 \leq k,\ l \leq 8$, whose value is equal to $d \in \{-2, -1, 2, 3\}$. The corresponding histogram values for the stego image will be denoted using the capital letter H_{kl}. Let us assume that the LSB embedding process changes n AC coefficients. The probability that a non-zero AC coefficient will be modified is $\beta = n/P$, where P is the total number of non-zero AC coefficients. Because the selection of the coefficients is pseudorandom in the StegoStorage system (due to the utilization of pseudorandomly permuted coefficients in Hamming coding embedding scheme), the expected values of the histograms H_{kl} of the stego image are

$$\begin{aligned} H_{kl}(d) &= (1-\beta)h_{kl}(d) + \beta h_{kl}(d+1), \quad \text{for } d = 2m \text{ (even number)}, \\ H_{kl}(d) &= (1-\beta)h_{kl}(d) + \beta h_{kl}(d-1), \quad \text{for } d = 2m+1 \text{ (odd number)}. \end{aligned} \tag{1}$$

This equation expresses the dependency of pairs of values, which originated from LSB embedding.

3. Calibration Process

The next assumption is that we have an estimate $\hat{h}_{kl}(d)$ of the cover image histogram (acquired from the process of calibration). Now, we can calculate $\hat{H}_{kl}$ using Eq. (1) and replace $h_{kl}(d)$ by $\hat{h}_{kl}(d)$. In our calculation, we only consider four values of $d \in \{-2, -1, 2, 3\}$, because these are the most numerous. In [1], experiments have been carried out on how to get the value (denoted β), which should give the best agreement with the cover image histogram. The best results of the experiments were for the formula of β which minimizes the square error between the stego image histogram H_{kl} and the expected value of $\hat{H}_{kl}$:

$$\begin{aligned} \beta_{kl} = \arg\min_{\beta} \{ &(H_{kl}(-2) - \hat{H}_{kl}(-2))^2 + (H_{kl}(-1) - \hat{H}_{kl}(-1))^2 + \\ &+ (H_{kl}(2) - \hat{H}_{kl}(2))^2 + (H_{kl}(3) - \hat{H}_{kl}(3))^2 \}. \end{aligned} \tag{2}$$

[1] This work was supported by projects VEGA 1/0173/13 and VEGA 1/0529/13.

The least square approximation in Eq. (2) (differentiation with respect to β and searching for minimum) leads to the following formula for β:

$$\begin{aligned}\beta_{kl} = {} & \frac{[\hat{h}_{kl}(-2)-\hat{h}_{kl}(-1)]^2 - [\hat{h}_{kl}(-2)-\hat{h}_{kl}(-1)][H_{kl}(-2)-H_{kl}(-1)]}{2(\hat{h}_{kl}(-2)-\hat{h}_{kl}(-1))^2 + 2(\hat{h}_{kl}(3)-\hat{h}_{kl}(2))^2} + \\ & + \frac{[\hat{h}_{kl}(3)-\hat{h}_{kl}(2)]^2 - [\hat{h}_{kl}(3)-\hat{h}_{kl}(2)][H_{kl}(3)-H_{kl}(2)]}{2(\hat{h}_{kl}(-2)-\hat{h}_{kl}(-1))^2 + 2(\hat{h}_{kl}(3)-\hat{h}_{kl}(2))^2}\end{aligned} \tag{3}$$

The final value of the parameter β is calculated as the average of selected low-frequency DCT coefficients $(k,l) \in \{(1,2),(2,1),(2,2)\}$.

4. Results

Analogously to the basic Chi-square attack, the results of this test indicate detectability through the entire image database consisting of 1450 files. But in contrast to the Chi-square attack, the situation when we embedded the information into the files and re-compressed them, was different. The detectability of such steganographic files decreased only slightly. This fact means that this steganalysis framework should be a more suitable approach to the detection of various types of LSB embedding than the classical Chi-square approach.

References

[1] J. Fridrich, M. Goljan, and D. Hogea, *Steganalysis of JPEG Images: Breaking the F5 Algorithm*, Information Hiding: 5th International Workshop, IH '02 Noordwijkerhout, The Netherlands, October 7-9, 2002 Revised Papers, ISBN 978-3-540-00421-9. Springer Berlin Heidelberg (2003), 310–323.

[2] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, ISBN 978 0 521 19019 0 (2010).

[3] M. Košdy, *Steganographic File System based on JPEG Files*, Master's thesis, Bratislava: FEI STU (2013).

A New Encryption Standard of Ukraine: The Block Cipher "Kalyna"

Roman Oliynykov, JSC Institute of Information Technologies (Ukraine)

Joint work with Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Yurii Gorbenko, Viktor Dolgov

1. Introducton

Since 1990 GOST 28147-89 [1] has been the official standard for block encryption in Ukraine. Even now this cipher still provides an acceptable level of practical security. However, its software implementation is significantly slower and less effective on modern platforms comparing to newer solutions like AES [2]. In addititon, more effective theoretical attacks than brute force search were discovered [3].

Based on the experience of international cryptographic competitions, like AES [4] or NESSIE [5], the State Service of Special Communication and Information Protection of Ukraine organized the National Public Cryptographic Competition [6] to select a block cipher that could become a prototype of the new national standard. Main requirements to candidates were a high level of cryptographic security, variable block size and key length (128, 256, 512), and an acceptable performance of encryption in software implementation. There were no restrictions concerning lightweight (hardware) implementations.

The block cipher Kalyna was selected among other candidates [7] and its slight modification (aimed to performance improvement and more compact implementation) was approved as the national standard DSTU 7624:2014 [8]. It describes both the block cipher and nine modes of operation.

2. Cipher description

2.1. **Encryption.** The base encryption transformation of Kalyna cipher is defined as:

$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ {\pi'}_l \circ \prod_{\nu=1}^{t-1} \left(\kappa_l^{(K_\nu)} \circ \psi_l \circ \tau_l \circ {\pi'}_l \right) \circ \eta_l^{(K_0)},$$

where:
l – the block size of Kalyna, $l \in \{128, 256, 512\}$,
k – the key length of Kalyna, $k \in \{128, 256, 512\}$ ($k = l$ or $k = 2 \cdot l$),
t – the number of rounds, $t \in \{10, 14, 18\}$ depending on the key length,
K – the encryption key,
$\eta_l^{(K_\nu)}$ – the function of addition of the internal state with the round key K_ν modulo 2^{64},
${\pi'}_l$ – the layer of non-linear bijective mapping (S-box layer) that process byte (i.e., elements of V_8) vectors,
τ_l – permutation of elements $g_{i,j} \in GF(2^8)$ of the cipher internal state (right circular shift),
ψ_l – the linear transformation of the internal state elements over the finite field,
$\kappa_l^{(K_\nu)}$ – the function of modulo 2 addition of the round key K_ν and the state matrix.

2.2. **Round keys generation.** Round keys K_i with even indexes ($i \in \{0, 2, ..., t\}$) are obtained with the $\Xi^{(K,K_\sigma,i)}$ transformation:

$$\Xi^{(K,K_\sigma,i)} = \eta_l^{(\varphi_i^{(K_\sigma)})} \circ \psi_l \circ \tau_l \circ {\pi'}_l \circ \kappa_l^{(\varphi_i^{(K_\sigma)})} \circ \psi_l \circ \tau_l \circ {\pi'}_l \circ \eta_l^{(\varphi_i^{(K_\sigma)})},$$

where $\eta_l^{(\cdot)}$, ${\pi'}_l$, τ_l, ψ_l, $\kappa^{(\cdot)}$ are functions used in the encryption procedure; $\varphi_i^{(K_\sigma)}$ returns K_σ added modulo 2^{64} with the constant shifted by the round key index. Input to the $\Xi^{(K,K_\sigma,i)}$ transformation is the shifted value of the encryption key K.
The intermediate key K_σ used by $\Xi^{(K,K_\sigma,i)}$ is generated by the following transformation:

$$\Theta^{(K)} = \psi_l \circ \tau_l \circ {\pi'}_l \circ \eta_l^{(K_\alpha)} \circ \psi_l \circ \tau_l \circ {\pi'}_l \circ \kappa_l^{(K_\omega)} \circ \psi_l \circ \tau_l \circ {\pi'}_l \circ \eta_l^{(K_\alpha)},$$

where $K_\alpha = K_\omega = K$ or $K_\alpha || K_\omega = K$ depending on block size and key length ratio. A constant depending on the cipher parameters is taken as input for the $\Theta^{(K)}$ transformation.
Rotated value of round key with even index forms the next round key having odd index.

3. Resistance against cryptanalytic attacks

The security level of the block cipher Kalyna was evaluated. It was shown that Kalyna is resistant against known cryptanalytic attacks (differential, linear, integral, boomerang, truncated differentials, algebraic, etc.). The minimum number of rounds when the cipher is resistant against all considered attacks is:

- 128-bit block: 6 rounds (of 10 or 14, depending on the key length);
- 256-bit block: 7 rounds (of 14 or 18);
- 512-bit block: 9 rounds (of 18).

4. Performance comparison

Comparison of encryption performance in software implementation (without hardware acceleration) of Kalyna with all combinations of block size and key length, AES and GOST 28147-89 is given in Fig. 1. The results were obtained by running a program implemented in C (gcc v4.9.2 for x86_64) on Intel Core i7-3770K@3.50GHz.

References

[1] Government Committee of the USSR for Standards. *GOST 28147-89. State Standard of the USSR. Information Processing Systems. Cryptographic protection. Algorithm of cryptographic transformation.* Government Committee of the USSR for Standards, 1990 (in Russian).

[2] National Institute of Standards and Technology (NIST). *Advanced Encryption Standard (AES).* Federal Information Processing Standards (FIPS) Publication 197, Nov. 2001.

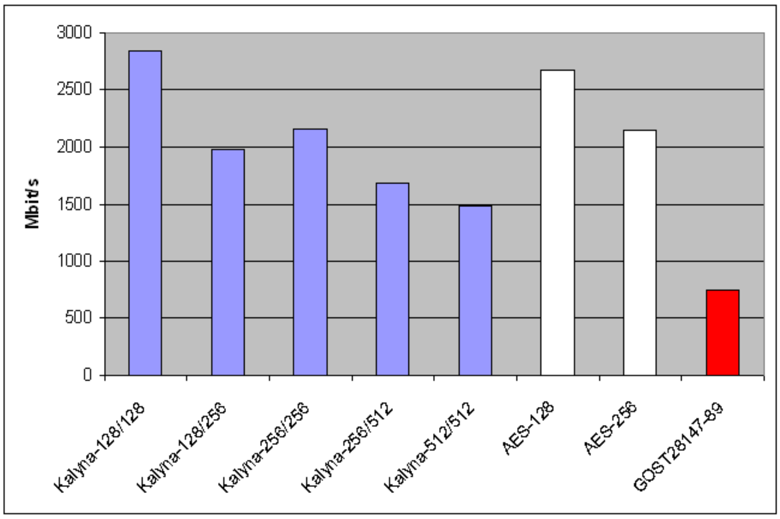


Figure 1. The performance comparison of block ciphers.

[3] Courtois, Nicolas T. *Security evaluation of GOST 28147-89 in view of international standardisation.* Cryptologia 36.1 (2012): 2-13.

[4] National Institute of Standards and Technology (NIST). *Announcing Development Of A Federal Information Processing Standard For Advanced Encryption Standard.* http://csrc.nist.gov/archive/aes/pre-round1/aes_9701.txt. Jan. 1997.

[5] NESSIE *New European Schemes for Signatures, Integrity, and Encryption.* https://www.cosic.esat.kuleuven.be/nessie, 2004.

[6] State Service of Special Communication and Information Protection of Ukraine. *Statement on Public Competition of Cryptographic Algorithms* (in Ukrainian). http://www.dstszi.gov.ua/dstszi/control/ua/publish/printable_article?art_id=48387, 2006.

[7] Oliynykov Roman, Gorbenko Ivan, Dolgov Victor, Ruzhentsev Victor. *Results of Ukrainian National Public Cryptographic Competition.* Tatra Mountains Mathematical Publications, 47(1), 99-113. 2009.

[8] Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Yurii Gorbenko, et al. *DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm.* Ministry of Economical Development and Trade of Ukraine, 2015 (in Ukrainian).

Breaking RC4 using Genetic Algorithm

Iwona Polak, University of Silesia
Joint work with Mariusz Boryczka

Cryptography is ubiquitous nowadays. It protects information of private people and big corporations, it has civil, political and martial applications. Everyone wants to have strong and safe ciphers. The field of examining the strength of ciphers is cryptanalysis.

One of the branches of modern cryptography are stream ciphers, which belong to symmetric-key cryptography [8]. Symmetric ciphers are used in data transmission in payment cards and other types of smart cards, in voice transmission in mobile phones and also in other guided or wireless types of data transmission.

In this work cryptanalysis of a stream cipher using genetic algorithm is shown. Attacking bit streams with genetic algorithms was already tested in [2]. Authors look for the shortest equivalent linear system which approximate given key stream with linear shift feedback register (LFSR). Authors study registers of length 5 to 8. In our work also approximation using LFSR is calculated, but for RC4. Previous research were conducted on LFSR itself [6] and A5/1 and A5/2 [7].

LFSR is a n-bits length register, which acts as follows:

- right-most bit is added to the generated stream,
- all other bits are shifted for one position to the right,
- left-most bit is calculated as XOR of chosen bits, called taps.

LFSRs are described by equations of the form $x^a + x^b + ... + 1$, where every power of x shows places where taps occur. The highest power is the length of the LFSR. LFSRs appear in many cryptographic constructions and pseudorandom number generators. LFSRs are common because they are very easy for hardware implementation. Breaking component LFSR could be the first step in breaking the whole stream cipher.

RC4 is a stream cipher [1] with variable key length implemented, among others, in SSL/TLS (protecting Internet traffic) and WEP (securing wireless networks). It was designed by Ron Rivest in RSA Security. The keystream is the same length as plaintext and it is independent of the plaintext.

Genetic Algorithm (GA) is one of metaheuristic techniques [3, 5]. It was for the first time introduced by John Holland in 1975 [4]. His work is based on the phenomenon of natural evolution. There are basic evolutionary mechanisms implemented: crossover, mutation and selection. The metaheuristic techniques (and thus also GA) are algorithms with randomized processes, so every run can give different final results. For this research basic version of GA was used, which acts as follows:

Algorithm: Genetic Algorithm

```
• randomly generate initial population
• evaluate the fitness function for every individual
• While termination condition has not been reached {
    – apply for chosen individuals: {
        ∗ crossover
        ∗ mutation
      }
    – replace old population with new one using selection and reproduction
    – evaluate the fitness function for every individual
  }
• Return the best solution found
```

The tests are based on known plaintext attack. We have particular amount of keystream bits and the aim of the research is to approximate the following bits with some LFSR. This work focuses on possibility of RC4 cryptanalysis using Genetic Algorithm. But we assume that there is no knowledge neither about the value of the key nor about cipher used, so we could generalise this attack to other stream ciphers. The only thing given are the bits of keystream of limited length (in this case 100 bits).

In this research to produce the attacked keystreams the following RC4 keys were used: “Key”, “Secret”, 0x0102030405, 0x1910833222772a [9]. Every individual from GA is a single LFSR, represented as binary string, where ones stand for taps. The length of individuals can be variable.

The fitness function was:

$$f_{fit} = \frac{H(a[n+1..l], b[n+1..l])}{l-n} \tag{1}$$

where:
$H(a,b)$ – Hamming distance between strings a and b,
a – output string of attacked system (here: RC4),
b – output string of an individual,
l – output length,
n – length of an individual.

The fitness function was normalized to the interval $[0, 1]$ so the results produced by different length individuals could be compared. The higher value of the fitness function, the better is the result achieved, e.g. $f_{fit} = 0.75$ means that 75% of the output bits match the attacked stream.

There were two types of crossover considered. Both types of crossover are one-point crossover – one was right-aligned, the second one was left-aligned. Individuals may vary in length so the crossover had to be adapted to such situation as this is not a classical approach. Right-aligned crossover guarantees to produce only correct individuals. With left-aligned crossover sometimes the repair process needs to be activated, because some new individuals could be invalid LFSRs.

There were also two types of mutation considered. The first one was random swap – one tap is chosen and moved to some other free place. The second one affected individual's length – it stretched the LFSR for one bit. Both mutation types were chosen among others during preliminary studies.

The probability of crossover and mutation were respectively 0.5 and 0.05. Tests without any mutation were also performed. There were 40 individuals for each generation and 100 generations as termination condition was set. For every key and for every type of crossover and mutation there were 30 runs of GA performed. Average and median values were calculated and together with best and worst cases are shown in Table 1.

Table 1. Results for RC4 cryptanalysis

k	best	worst without mutation	worst with mutation	avg	median
"*Key*"	0.750	0.628	0.644	0.679	0.679
"*Secret*"	0.766	0.614	0.639	0.676	0.674
0x0102030405	0.771	0.614	0.624	0.676	0.673
0x1910833222772a	0.754	0.600	0.621	0.672	0.671
altogether	0.771	0.600	0.621	0.676	0.675

Conclusions of the research are the following. Mutation improves the performance. The best found individuals agree in 62-77% with attacked keystream, with average and median value at 67-68%. This means we can decrypt 67-68% of the message correctly, which can be enough information to decrypt the whole message. This method is effective for not only A5/1 and A5/2, but also for RC4. Further research will focus on generalising this method to other stream ciphers. It is also planned to compare genetic algorithms with other metaheuristic technique, namely tabu search.

References

[1] RC4 Source Code. Cypherpunks http://cypherpunks.venona.com/archive/1994/09/msg00304.html 1994

[2] Abd A. A., Younis H. A., Awad W. S.: Attacking of stream Cipher Systems Using a Genetic Algorithm. Journal of the University of Thi Qar, Volume 6, pp.1-6. 2011

[3] Goldberg D. E.: Genetic algorithms in search, optimization, and machine learning (in Polish). Third edition. Warszawa, Wydawnictwa Naukowo-Techniczne. 2003

[4] Holland J. H.: Adaptation in Natural and Artificial Systems University of Michigan Press, USA. 1975

[5] Michalewicz Z., Fogel D. B.: How to Solve It: Modern Heuristics (in Polish). Second Edition, Warszawa, Wydawnictwa Naukowo-Techniczne. 2006

[6] Polak I., Boryczka M.: Breaking LFSR Using Genetic Algorithm. Computational Collective Intelligence. Technologies and Applications, pp. 731-738. 2013

[7] Polak I., Boryczka M.: Cryptanalysis of A5/1 and A5/2 using Genetic Algorithm (in Polish). Systemy Inteligencji Obliczeniowej, pp. 145-153. 2014

[8] Schneier B.: Applied Cryptography (in Polish). Second Edition, Warszawa, Wydawnictwa Naukowo-Techniczne. 2002

[9] Strombergson J., Josefsson S.: Test Vectors for the Stream Cipher RC4. 2011

Ascon – A submission to CAESAR

Christoph Dobraunig, IAIK, Graz University of Technology
Joint work with Maria Eichlseder, Florian Mendel, Martin Schläffer

C I A — the three big letters in cryptography — stand for confidentiality, integrity and availability. These are the three main attributes one wants to achieve by using symmetric cryptography. In most use cases, it is desirable to achieve all three attributes together. For example, if a message is exchanged between two parties, these parties might want no other third party to be able to read the content. Neither do they want this message to be modified accidentally or intentionally, nor do they want this to generate much computational overhead.

In the past, often two different schemes have been used to achieve confidentiality and integrity/authenticity. For instance, a block cipher like AES [10] in CBC mode is used to encrypt a message, afterwards HMAC-SHA1 [11] is used to ensure authenticity. Although such composed constructions might fulfill all needed security requirements, dedicated solutions have the potential to achieve higher performance while also require less implementation overhead in terms of chip area or code size. This talk deals with such a dedicated scheme, Ascon-128. Ascon-128 is the primary candidate of a family of authenticated encryption schemes taking part in the ongoing CAESAR competition [12]. The mission of CAESAR is to identify a portfolio of authenticated encryption schemes out of more than 50 submissions, which is suitable for widespread adoption.

Since no strict design requirements have been stated in the CAESAR call, the candidates differ significantly. For instance some candidates are optimized for high performance in a software environment, while other designs target low area hardware implementations. The design of Ascon is more balanced. This is also reflected by the design goals of Ascon, which are a very low footprint in hardware and software, while still being fast, and providing a simple analysis and good bounds for security [7].

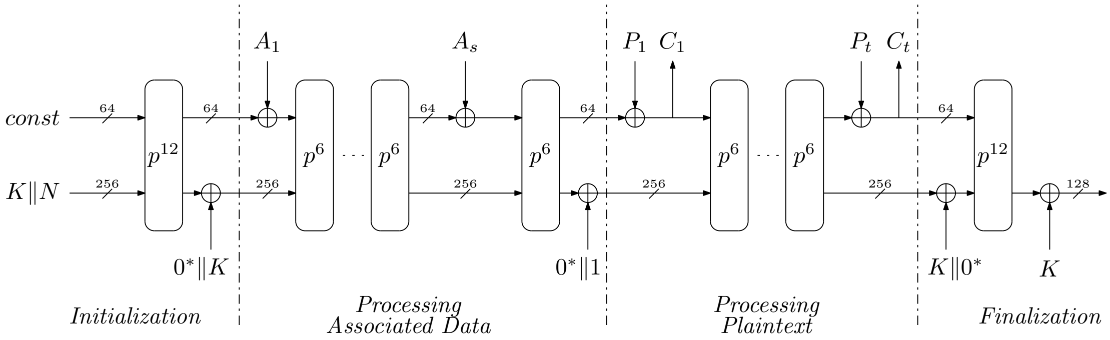


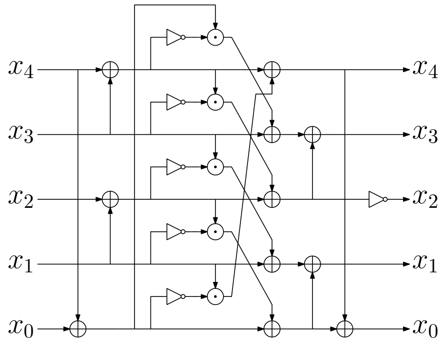
Figure 1. The encryption of Ascon-128 (taken from [7]).

Ascon-128 is sponge based [2, 3] and uses a MonkeyDuplex [6] like mode of operation. The encryption is shown in Figure 1. In the case of Ascon-128, the key K, the nonce N and the tag T have a size of 128-bit. The associated data A (not encrypted, just authenticated) and the plaintext P (both encrypted and authenticated) are separately padded using a 10^* padding until they reach a multiple of the 64-bit blocksize. Then, they are split into 64-bit blocks which are absorbed blockwise. Ascon uses two different permutations p^{12} and p^6. Those two permutations use the same round function and differ only in the number of rounds, which are 6 and 12.

The round transformation p consists of the following three steps:

- Addition of a round constant.
- Parallel application of 64 identical 5-bit S-boxes.
- Parallel application of 5 different 64-bit linear transformations.

The round constants differ for every round and are defined in the design document [7]. The linear layer and the S-box are shown in Figure 2. The S-box is an affine transformation of the χ mapping of Keccak [4]. The linear layer uses Σ of SHA-2 with 5 different sets of rotation values.



$$x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41) \to x_4$$
$$x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) \to x_3$$
$$x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) \to x_2$$
$$x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39) \to x_1$$
$$x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) \to x_0$$

Figure 2. Substitution layer with 5-bit S-box (left) and linear layer (right) (taken from [7]).

Several design features of Ascon help to allow fast and lightweight implementations in hardware and fast implementations in software for different CPU architectures.

- The S-box is designed for fast bitsliced implementation, with relatively few, well pipelinable instructions.
- Up to 5 instructions can be carried out in parallel in nearly every phase of the permutation.
- This parallelism can be achieved using only 2-operand instructions and 5 temporary registers.
- To scale for smaller implementations, the permutation can also be computed using only 2 temporary registers.
- Ascon is intuitively defined using only the common bitwise Boolean functions AND, OR, XOR, NOT, and bitwise rotation.
- The performance of Ascon can benefit from platform-specific features and combined instructions like ANDNOT.
- The design is optimized for hardware and modern CPUs using 64-bit instructions.

Besides performance and other implementation specific characteristics, the security of Ascon is of capital importance. The security of the mode of operation has been analyzed by Jovanovic et al. [9]. Furthermore, the resistance of Ascon against various state-of-the-art cryptanalysis techniques has been evaluated [7, 8]. Besides the analytical aspect, Ascon has been designed with side-channel attacks in mind. For instance the choice of the S-box facilitates similar threshold implementations as already used for Keccak [5]. Moreover, implementations of Ascon do not need look-up tables. This precludes cache-timing attacks like Bernstein's attack on AES [1].

To sum up, this talk is about the CAESAR candidate Ascon. We present its design and explain the main design goals. Furthermore, we will give an overview about the most recent implementation and cryptanalysis results available at the time of the presentation.

Acknowledgments. The work has been supported in part by the Austrian Science Fund (project P26494-N15) and by the Austrian Research Promotion Agency (FFG) and the Styrian Business Promotion Agency (SFG) under grant number 836628 (SeCoS).

References

[1] Daniel J. Bernstein, *Cache-timing attacks on AES*, `http://cr.yp.to/antiforgery/cachetiming-20050414.pdf`, 2005

[2] Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche, *Sponge Functions*, ECRYPT Hash Workshop 2007

[3] Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche, *On the Indifferentiability of the Sponge Construction*, In Nigel P. Smart, editor, Advances in Cryptology - EUROCRYPT 2008, volume 4965 of LNCS, pages 181–197. Springer, 2008

[4] Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche, *Keccak Specification*, Submission to NIST SHA-3 competition (Round 3)

[5] Begül Bilgin, Joan Daemen, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen and Gilles Van Assche, *Efficient and First-Order DPA Resistant Implementations of Keccak*, In Aurélien Francillon and Pankaj Rohatgi, editors, CARDIS, volume 8419 of LNCS, pages 187–199. Springer, 2013

[6] Joan Daemen, *Permutation-based Encryption, Authentication and Authenticated Encryption*, DIAC – Directions in Authenticated Ciphers 2012

[7] Christoph Dobraunig, Maria Eichlseder, Florian Mendel and Martin Schläffer, *Ascon*, Submission to the CAESAR competition: http://ascon.iaik.tugraz.at, 2014

[8] Christoph Dobraunig, Maria Eichlseder, Florian Mendel and Martin Schläffer, *Cryptanalysis of Ascon*, In Kaisa Nyberg, editor, Topics in Cryptology - CT-RSA 2015, volume 9048 of LNCS, pages 371–387. Springer, 2015

[9] Philipp Jovanovic, Atul Luykx and Bart Mennink, *Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes*, In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology - ASIACRYPT 2014, volume 8873 of LNCS, pages 85–104. Springer, 2014

[10] National Institute of Standards and Technology, *FIPS PUB 197: Advanced Encryption Standard (AES)*, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[11] National Institute of Standards and Technology, *FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC)*, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=901614

[12] The CAESAR committee, *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness*, http://competitions.cr.yp.to/caesar.html

Scalar multiplication on elliptic curves using the binary asymmetric joint sparse form

Sara Kropf, Institut für Mathematik, Alpen-Adria-Universität Klagenfurt
Joint work with Clemens Heuberger

In public-key cryptography the computation of scalar multiples nP of an element P in some Abelian group is a common example of a one-way-function. One possibility to compute nP efficiently uses the binary digit expansion of n and computes nP by Horner's scheme. This method is called *double-and-add* method. For every nonzero digit in the digit expansion of n an addition has to be processed. Since these are expensive, we want to minimize the number of nonzero digits. Therefore we define the *Hamming weight* $h(n)$ of a digit expansion of n as the number of nonzero digits in this digit expansion. We are interested in digit expansions with a minimal Hamming weight (with respect to a fixed digit set).

If the additive inverse of any element in the Abelian group can be computed essentially for free, then one can also use negative digits in the digit expansion of n to decrease the Hamming weight. An example for such a group is the additive group of points on an elliptic curve.

Example. *An expansion of* 27 *with base* 2 *and digit set* $\{-1,0,1\}$ *is* $(100\bar{1}0\bar{1})$ *where* $\bar{1}$ *is* -1. *To compute* $27P$ *for a point* P *on the elliptic curve, we write*

$$27P = 2\,(2\,(2\,(2\,(2\,(1\cdot P)+0\cdot P)+0\cdot P)+\bar{1}\cdot P)+0\cdot P)+\bar{1}\cdot P.$$

The Hamming weight of $27 = (100\bar{1}0\bar{1})$ *is* 3.

Joint representations of several integers can be used for computing a linear combination $n_1P_1 + \cdots + n_dP_d$ of points P_i of an elliptic curve, or more generally an abelian group (cf. [10]).

Example. *A digit expansion of* $(11,4,17)^T$ *with digit set* $\{0,1,2\}$ *is*

$$\begin{pmatrix}1011\\0020\\2001\end{pmatrix}.$$

It has Hamming weight 3. *This expansion can be used to compute* $11P_1 + 4P_2 + 17P_3$ *by the double-and-add method.*

Digit expansions with a minimal Hamming weight among all digit expansions with the same digit set and base are of special interest as the Hamming weight corresponds to the number of elliptic curve additions. Examples for such optimal digit expansions in base 2 are

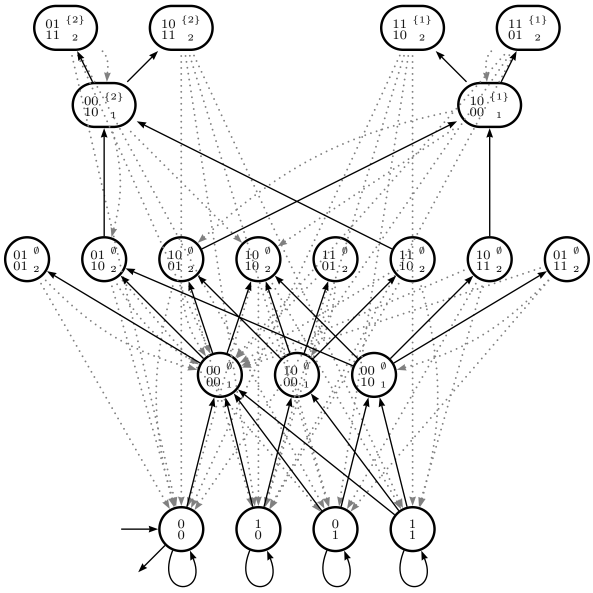


FIGURE 1. Transducer for $D_{-2,3}$ and $d = 2$.

(1) the *nonadjacent form* [8, 5]: It has digit set $\{-1, 0, 1\}$ and the syntactical rule that at least one of any two adjacent digits has to be zero.
(2) the *width-w nonadjacent form* [1, 6]: It has digit set $\{0, \pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)\}$ and the syntactical rule that at least $w - 1$ of any w consecutive digits have to be zero.
(3) the *simple joint sparse form* [2]: It has digit set $\{-1, 0, 1\}$ and is a 2-dimensional joint digit expansion. The syntactical rules are given in [2]. A different optimal expansion with the same digit set is given in [9].
(4) the *asymmetric joint sparse form* (AJSF) [4]: It has digit set $D_{\ell,u} = \{a \in \mathbb{Z} : \ell \leq a \leq u\}$ with $\ell \leq 0$ and $u \geq 1$ and is a d-dimensional joint digit expansion. The syntactical rules are given in [4]. For extensions to bases other than 2, see [7].

These digit expansions exist and are unique for all integer vectors n. The AJSF is a generalization of all other three optimal digit expansions.

The colexicographic order sorts digit expansions by lexicographically comparing the positions of nonzero digits from right to left. For example for the integer 14, the digit expansion (1102) is colexicographically less than the expansion (62): The positions of nonzero digits are 1101 and 11. If these two strings are lexicographically compared from right to left, then the first one is less than the second one.

Theorem (Heuberger–Muir [4]). *The AJSF is colexicographically minimal and has minimal Hamming weight among all digit expansions of an integer vector n with base 2 and digit set $D_{\ell,u}$.*

We consider the algorithm to compute the AJSF presented in [4]. By transforming this algorithm into a transducer, we can asymptotically analyze the Hamming weight of the AJSF.

The transducer in Figure 1, computes the Hamming weight of the 2-dimensional AJSF with digit set $D_{-2,3}$. The input and output labels are omitted and transitions going back are gray. We give a general construction of this transducer for arbitrary values of l, u and d.

Theorem (Heuberger–Kropf [3]). *The Hamming weight $h(n_1, \ldots, n_d)$ of the AJSF of an integer vector $(n_1, \ldots, n_d)^T$ over the digit set $D_{l,u}$ in dimension d with equidistribution of all vectors $(n_1, \ldots, n_d)^T$ with $0 \leq n_i < N$ for an integer N is asymptotically normally distributed. There exist constants $e_{\ell,u,d}$, $v_{\ell,u,d} \in \mathbb{R}$ and $\delta > 0$, depending on u, l and d, such that the expected value is*

$$e_{\ell,u,d} \log_2 N + \Psi_1(\log_2 N) + \mathcal{O}(N^{-\delta} \log N)$$

l	u	d	$e_{l,u,d}$	$v_{l,u,d}$	Name
0	2	1	$1/2$	$1/4$	binary standard expansion
-1	1	1	$1/3$	$2/27$	non-adjacent form
$-2^{w-1}+1$	$2^{w-1}-1$	1	$1/(w+1)$	$2/(w+1)^3$	width-w non-adjacent form
-1	1	2	$1/2$	$1/16$	simple joint sparse form
-3	11	1	$1/5$	$2/125$	
-2	3	2	$32/89$	$63200/2114907$	

Table 1. Special values of $e_{l,u,d}$ and $v_{l,u,d}$.

and the variance is

$$v_{\ell,u,d}\log_2 N - \Psi_1^2(\log_2 N) + \Psi_2(\log_2 N) + \mathcal{O}(N^{-\delta}\log^2 N),$$

where Ψ_1 and Ψ_2 are continuous, 1-periodic functions on $\mathbb{R}$.

The constants $e_{l,u,d}$ and $v_{l,u,d}$ can be computed for any fixed digit set.

Because of the central limit theorem, we obtain that a Hamming weight of the AJSF is concentrated around its mean. This mean is the constant $e_{l,u,d}$ times the length of the digit expansion $\log_2 N$. This implies that scalar multiplication on elliptic curves using the AJSF is efficient for many integer vectors n. Special values of the constants $e_{l,u,d}$ and $v_{l,u,d}$ are given in Table 1.

References

[1] Roberto Avanzi, *A note on the signed sliding window integer recoding and a left-to-right analogue*, Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers (H. Handschuh and A. Hasan, eds.), Lecture Notes in Comput. Sci., vol. 3357, Springer-Verlag, Berlin, 2005, pp. 130–143.

[2] Peter J. Grabner, Clemens Heuberger, and Helmut Prodinger, *Distribution results for low-weight binary representations for pairs of integers*, Theoret. Comput. Sci. **319** (2004), 307–331.

[3] Clemens Heuberger and Sara Kropf, *Analysis of the binary asymmetric joint sparse form*, Combin. Probab. Comput. **23** (2014), 1087–1113.

[4] Clemens Heuberger and James A. Muir, *Minimal weight and colexicographically minimal integer representations*, J. Math. Cryptol. **1** (2007), 297–328.

[5] François Morain and Jorge Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.

[6] James A. Muir and Douglas R. Stinson, *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. **75** (2006), 369–384.

[7] Braden Phillips and Neil Burgess, *Minimal weight digit set conversions*, IEEE Trans. Comput. **53** (2004), 666–677.

[8] George W. Reitwiesner, *Binary arithmetic*, Advances in Computers, vol. 1, Academic Press, New York, 1960, pp. 231–308.

[9] Jerome A. Solinas, *Low-weight binary representations for pairs of integers*, Tech. Report CORR 2001-41, Centre for Applied Cryptographic Research, University of Waterloo, 2001, available at `http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps`.

[10] Ernst G. Straus, *Addition chains of vectors (Problem 5125)*, Amer. Math. Monthly **71** (1964), 806–808.

Properties of τ-adic Digit Expansions for Fast Scalar Multiplication

Daniel Krenn, TU Graz, Austria

Joint work with Clemens Heuberger

One main operation in (hyper-)elliptic curve cryptography is building multiples of a point on a (hyper-)elliptic curve over a finite field. Clearly, we want to perform this scalar multiplication as efficiently as possible. A standard method are double-and-add algorithms. But if the (hyper-)elliptic curve is defined over a field with q elements and we are working in the point group in an extension (i.e., working over a field with q^m elements), then one can use a Frobenius-and-add method instead, for example, see [11], [12] for Koblitz curves or [10], [15], [16]. There the (expensive) doublings are replaced by the (cheap) evaluation of the Frobenius endomorphism in the point group. To use this method we need to understand digit expansions with base τ, where τ is an algebraic integer whose conjugates all have the same absolute value. In the case of elliptic curves, this is an imaginary-quadratic integer.

So let's consider digit expansions with a base as above, i.e., we write a number $z \in \mathbb{Z}[\tau]$ as a finite sum

$$z = \sum_{\ell=0}^{L-1} d_\ell \tau^\ell,$$

where the d_ℓ are out of a finite digit set $\mathcal{D}$. Let w be a positive integer. Our digit set $\mathcal{D}$ should consist of 0 and one representative of every residue class modulo τ^w which is not divisible by τ. That choice of the digit set yields redundancy, i.e., each element z of $\mathbb{Z}[\tau]$ has more than one representation. Thus we can choose a "good" representation, which leads to a fast evaluation scheme.

The width-w non-adjacent form [14], w-NAF for short, is a special representation: Every block of w consecutive digits contains at most one non-zero digit. The choice of the digit set guarantees that the w-NAF-expansion of any number z is unique. The low weight (number of non-zero digits) of this expansion makes the arithmetic on the (hyper-)elliptic curves efficient.

In this talk the following properties of these digit expansions are discussed.

Existence

A quite natural first question is, whether each possible multiple of a curve point in the scalar multiplication algorithm can be calculated, or, translated into the language of digit expansions, whether each element of $\mathbb{Z}[\tau]$ admits a unique w-NAF (for all w). Of course, this depends on the choice of the digit set.

Various results exists, cf. [12], [15], [16], [1], [3] and [2]. Here, results for imaginary-quadratic bases with an minimal norm digit set, cf. [6] are presented. The higher-dimensional case and other digit sets are also discussed, see [7].

Occurrences of Digits

The next part deals with analyzing the number of occurrences of a fixed non-zero digit. This property corresponds to the average running time of the scalar multiplication algorithm.

Again we take a minimal norm digit set. We give an explicit expression for the expectation and the variance of the occurrence of such a digit in all expansions of a fixed length, cf. [6]. Further a central limit theorem is proved in this setting. Moreover, we found an asymptotic formula for the number of occurrence of a digit in the w-NAFs of all elements of $\mathbb{Z}[\tau]$ in some region (e.g. a disc). The main term coincides with the full block length analysis mentioned above, but a periodic fluctuation in the second order term is also exhibited. This is a frequent behaviour of digit expansions, see, for example, [9] or [5]. The proof of the presented result follows Delange's method [4], but several technical problems have to be taken into account. Generalizations to higher dimensions (coming from hyperelliptic curves) are also mentioned, cf. [13]

Minimality of Digit Expansions

Another interesting question is the following: Is the w-NAF-expansion optimal, where optimal means minimizing Hamming-weight, i.e., the number of non-zero digits? These minimal expansions correspond to the fastest evaluation schemes for the scalar multiplication.

The answer to the posed question is affirmative for most of the cases coming from elliptic curves. More precisely, suppose τ is a solution of $\tau^2 - p\tau + q = 0$, where p and q are integers, then we could show optimality if $|p| \geq 3$ and $w \geq 4$ or if $|p| \geq 5$ and $w = 3$. Moreover, optimality and non-optimality results were shown for some special configurations, see [8]. Again, generalizations are discussed, cf. [7]

References

[1] Ian F. Blake, V. Kumar Murty, and Guangwu Xu, *Efficient algorithms for Koblitz curves over fields of characteristic three*, J. Discrete Algorithms **3** (2005), no. 1, 113–124. MR MR2167767 (2006f:11069)

[2] ———, *A note on window τ-NAF algorithm*, Inform. Process. Lett. **95** (2005), 496–502.

[3] ———, *Nonadjacent radix-τ expansions of integers in Euclidean imaginary quadratic number fields*, Canad. J. Math. **60** (2008), no. 6, 1267–1282.

[4] Hubert Delange, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, Enseignement Math. (2) **21** (1975), 31–47.

[5] Peter J. Grabner, Clemens Heuberger, and Helmut Prodinger, *Distribution results for low-weight binary representations for pairs of integers*, Theoret. Comput. Sci. **319** (2004), 307–331. MR 2074958 (2005h:11018)

[6] Clemens Heuberger and Daniel Krenn, *Analysis of width-w non-adjacent forms to imaginary quadratic bases*, J. Number Theory **133** (2013), no. 5, 1752–1808. MR 3007130

[7] ———, *Existence and optimality of w-non-adjacent forms with an algebraic integer base*, Acta Math. Hungar. **140** (2013), no. 1–2, 90–104. MR 3123865

[8] ———, *Optimality of the width-w non-adjacent form: General characterisation and the case of imaginary quadratic bases*, J. Théor. Nombres Bordeaux **25** (2013), no. 2, 353–386. MR 3228312

[9] Clemens Heuberger and Helmut Prodinger, *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248. MR 2215565 (2007g:11010)

[10] Neal Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), no. 3, 139–150. MR 1007215 (90k:11165)

[11] ———, *CM-curves with good cryptographic properties*, Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991) (J. Feigenbaum, ed.), Lecture Notes in Comput. Sci., vol. 576, Springer, Berlin, 1992, pp. 279–287. MR 94e:11134

[12] ———, *An elliptic curve implementation of the finite field digital signature algorithm*, Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, 1998, pp. 327–337. MR MR1670960 (99j:94052)

[13] Daniel Krenn, *Analysis of the width-w non-adjacent form in conjunction with hyperelliptic curve cryptography and with lattices*, Theoret. Comput. Sci. **491** (2013), 47–70.

[14] George W. Reitwiesner, *Binary arithmetic*, Advances in Computers, Vol. 1, Academic Press, New York, 1960, pp. 231–308. MR 0122018 (22 #12745)

[15] Jerome A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology — CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings (B. S. Kaliski, jun., ed.), Lecture Notes in Comput. Sci., vol. 1294, Springer, Berlin, 1997, pp. 357–371.

[16] ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249. MR 2002k:14039

Non-commutative Digit Expansions for Arithmetic on Supersingular Elliptic Curves

Michela Mazzoli, Alpen-Adria-Universität Klagenfurt, Austria

In this talk we shall consider non-commutative digit expansions in a subring of a quaternion algebra to the basis of a quadratic algebraic integer τ. These digit expansions can be used in a τ-and-add method to speed up arithmetic (scalar multiplication and pairing) on certain families of supersingular elliptic curves in characteristic $p \geq 5$. The basis τ represents the Frobenius endomorphism of the curve, that is $\tau(x, y) = (x^p, y^p)$.

Arithmetic of elliptic curves is in general rather time-consuming. The scalar multiplication, i.e. $nP = P + \cdots + P$ with P point on the curve and $n \in \mathbb{Z}$, is especially important as it occurs in elliptic curve cryptosystems. One of the possible speed-up methods to calculate nP is to expand the integer n to the basis τ, i.e. $n = \sum_{j=0}^{l-1} d_j \tau^j$, with d_j belonging to some suitable digit set. Then one can compute nP with a τ-and-add method:

$$nP = \sum_{j=0}^{l-1} d_j \tau^j(P) = d_0 P + \tau(d_1 P + \tau(d_2 P + \tau(\cdots + \tau(d_{l-1}P)\cdots))) ,$$

possibly precomputing and storing the values dP for all non-zero digits. This τ-and-add scheme requires $\mathrm{wt}_\tau(n) - 1$ point additions (where $\mathrm{wt}_\tau(n)$ is the number of non-zero digits in the τ-adic expansion of n) and $\mathrm{len}_\tau(n) - 1 = l - 1$ evaluations of τ, which is very efficient, as it requires only two p-powers in $\mathbb{F}_{p^m}$, i.e. two cyclic shifts if the field $\mathbb{F}_{p^m}$ is represented in normal base. Further syntactical constraints, such as the NAF property (see below), can be imposed on the digit expansion in order to reduce the number of additions and/or the precomputation effort.

Moreover, in the pairing-based setting, computation of Weil and Tate-Lichtenbaum pairings is achieved with a double-and-add scheme, i.e. by means of the binary expansion of integers. Also in this case extra operations have to be performed when a non-zero digit occurs (see [1, Alg. 16.8] for the detailed algorithm). Substitution of the binary expansion with a τ-adic expansion is not only possible but also desirable in the pairing computation as well.

Let $E/\mathbb{F}_p$ be an elliptic curve over the finite field $\mathbb{F}_p$ with $p \geq 5$ prime. It is well-known ([3, Ch. 13, § 7]) that E is *supersingular* if and only if its endomorphism ring $\mathrm{End}(E)$ is an order in a quaternion algebra; in particular, $\mathrm{End}(E)$ is not commutative. In this case the characteristic polynomial of the Frobenius endomorphism τ of E is $x^2 + p$, and thus $\tau^2 = -p$.

Furthermore, the elliptic curves $E_a : y^2 = x^3 + ax$ and $E_b : y^2 = x^3 + b$ have automorphism groups $\mathrm{Aut}(E_a) \cong \mathcal{U}_4$ and $\mathrm{Aut}(E_b) \cong \mathcal{U}_6$ respectively, where $\mathcal{U}_m$ is the cyclic group of the m-th roots of unity ([5, III § 10]). From the computational perspective, this fact is important because automorphisms turn out to be very cheap to evaluate. More precisely, if ζ is an automorphism of order m, then the action of ζ on the points of the curve is $\zeta(x, y) = (u^2x, u^3y)$, where $u \in \overline{\mathbb{F}}_p$ is an element of order m and $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$.

In addition, E_a is supersingular if and only if $p \equiv 3 \mod 4$, while E_b is supersingular if and only if $p \equiv 2 \mod 3$. These two families of curves have been already studied for fast scalar multiplication methods, for instance in [2], but only in the ordinary case.

When E_a and E_b are supersingular, their automorphisms are defined in $\mathbb{F}_{p^2}$, but not in $\mathbb{F}_p$. For instance, consider the curve of type E_a in characteristic $p \equiv 3 \mod 4$. Then $i(x, y) = (-x, -uy) \in \mathrm{Aut}(E_a)$ and $u \in \overline{\mathbb{F}}_p$ has order 4. Since $4 \nmid p - 1$ but $4 \mid p^2 - 1$, we have $u \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

The endomorphisms that commute with τ are precisely those defined in the base field $\mathbb{F}_p$ (cf. [4]). Therefore, when we compute the τ-adic digit expansions by including the automorphisms in the digit set, as well as in the τ-and-add algorithm, we must pay attention to the order of operations and keep track of any non-commutative switch.

In this work we shall focus on curves of equation $E_a : y^2 = x^3 + ax$ in characteristic $p \equiv 3 \mod 4$ (the case of E_b is analogous). If $i(x, y) = (-x, -uy)$ is an automorphism of E_a of order 4, then

$$\begin{aligned}\tau \circ i\,(x, y) &= (-x^p, -u^p y^p)\ ,\\ i \circ \tau\,(x, y) &= (-x^p, -uy^p)\ .\end{aligned}$$

As said before, $\tau \circ i \neq i \circ \tau$ because $u \notin \mathbb{F}_p$. However, u^p is the other element of order 4 in $\mathbb{F}_{p^2}$, which means that $-i(x, y) = (-x, -u^p y)$ is the other automorphism of E_a of order 4. Hence

$$i \circ \tau = -\tau \circ i\ . \tag{1}$$

Consider the free $\mathbb{Z}$-module $\mathbb{Z}[i, \tau] = \{a + bi + c\tau + d(i\tau) \mid a, b, c, d \in \mathbb{Z}\}$ equipped with the following multiplication rules:

$$\tau i = -i\tau, \quad i^2 = -1, \quad \tau^2 = -p\ .$$

The first rule is justified by (1). In particular, we have $(i\tau)^2 = -p$. Since i and τ are $\mathbb{Z}$-linearly independent, $\mathbb{Z}[i, \tau]$ has rank 4. It is clear that $\mathbb{Z}[i, \tau]$ is a subring of the algebra of Hamilton quaternions.

We want to find digit expansions to the basis τ of elements of $\mathbb{Z}[i, \tau]$. In order to construct a digit set in $\mathbb{Z}[i, \tau]$, we have to choose a representative of each residue class modulo τ. We show that

$$\mathbb{Z}[i, \tau]/\langle\tau\rangle \cong \mathrm{GF}(p^2)\ .$$

Given $\eta \in \mathbb{Z}[i,\tau]$, we consider the existence of a *right* τ-adic expansion $\eta = \sum_{j=0}^{l-1}(a_j, b_j)\tau^j$, with (a_j, b_j) belonging to the digit set

$$\Delta = \left\{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid -\frac{p-1}{2} \leq n, m \leq \frac{p-1}{2}\right\}.$$

We prove the following:

- Every element of $\mathbb{Z}[i,\tau]$ admits a finite right Δ-τ-adic expansion.
- The digit set Δ provides a NAF (Non-Adjacent Form) expansion of *integers*, i.e. if $n = \sum_{j=0}^{l-1}\delta_j\tau^j$ is a τ-adic expansion of $n \in \mathbb{Z}$ with digits $\delta_j \in \Delta$, then $\delta_j\delta_{j+1} = 0$ for all $j = 0 \dots l-2$, or equivalently there is at least one 0 every two digits.

The NAF property allows us to reduce the weight of the expansion and consequently the computational cost of arithmetic on the elliptic curve.

Finally, we show that any *right* Δ-τ-adic expansion can be easily derived from a *left* Δ-τ-adic expansion (i.e. the basis τ is placed right, resp. left, to the digit) and viceversa, with the obvious consequence that the statements above hold for left expansions as well.

References

[1] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and its Applications, Chapman & Hall/CRC, 2006.

[2] C. Heuberger and M. Mazzoli, *Symmetric digit sets for elliptic curve scalar multiplication without precomputation*, Theoretical Computer Science **547** (2014), no. 100, 18–33.

[3] D. Husemöller, *Elliptic curves*, 2 ed., GTM 111, Springer-Verlag, 2004.

[4] H. W. Lenstra Jr., *Complex multiplication structure of elliptic curves*, Journal of Number Theory **56** (1996), no. 2, 227–241.

[5] J. H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.

Quality Limitations on the Extraction of a PUF-based Cryptographic Key

Sandra L. Lattacher, TECHNIKON Forschungs- und Planungsgesellschaft mbH
Joint work with Martin Deutschmann, Michael Höberl, Christina Petschnigg and Naeim Safari

1. Introduction

An indispensable demand for the majority of cryptographic implementations is the ability to securely generate and store cryptographic keys. Physically Unclonable Functions (PUFs) prove to be a suitable primitive to comply these requirements. PUFs can be understood as physical systems which, when measured, provide unique and unpredictable responses. The responses are depending on the physical structure of the device and are out of the control of the manufacturer. As PUFs are physical objects they are prone to errors, i.e. the responses will always include some degree of noise. Further the distribution of the responses does not necessarily have to be uniform. In other words, when designing key generation or protection schemes based on PUF measurements, one has to make sure that suitable error correcting mechanisms are put in place. Further entropy extraction is crucial, to ensure the generation of keys with high entropy.

In this work we are exposing the limits in the design of a key generation framework by taking into account relevant properties of PUF instantiations, such as entropy or the mutual information. Our attempt is to present a tool to evaluate if and how a cryptographic key of a certain length can be extracted with the demanded reliability for a given PUF source. The solutions presented are evaluated against concrete PUF parameters. The PUF source are 65nm TSMC ASICs, which were developed in the course of the FP7 research project UNIQUE [2].

[2] www.unique-project.eu

2. The PUF Framework

By challenging the PUF twice consecutively with identical conditions, we expect an unreliability of the two responses R and R' reflected by the so-called intra distance. Moreover, when comparing two different instances of a PUF type, an inter distance of about 50% is desired.

To reliably generate cryptographic keys, the PUF response has to be processed within a specific framework that can cope with the noise cancellation and the entropy extraction. This is where so called Helper Data Algorithms (HDAs) come into play. Most HDAs follow a two-step approach: the key is derived by querying the PUF in a secure environment during an enrollment phase. During the so called reconstruction phase the key is recovered in the field. A HDA can additionally be divided into three sub-components. The first is bit selection, aiming at discarding the least reliable bits within a PUF response. This step can significantly lower the number of expected errors within the response and thus allowing the application of shorter and simpler error correcting codes. Applying bit selection as well as error correction measures allow the assumption of a negligible low failure rate during reconstruction. However, the remaining bits have non-maximum entropy due to leakage during the former two steps. Therefore, the third step comprises entropy compression. [5]

3. Quality Aspects of a Key

Generally speaking there are two main areas that might affect the quality level of a key: the property of the raw data, and the helper data leakage, including the choice of the error correction and the randomness extraction. A rough assessment on the quality of the data is the Hamming weight of the response which gives a first indication of the randomness, since it is a measure of the distribution of ones and zeros within a binary bit string:

$$W(x) = \sum_{i=1}^{n} x_{\mathrm{i}}. \tag{1}$$

When designing key generation frameworks, a high level of unpredictability and robustness is claimed. Entropy estimation, which is the measure of uncertainty of a random variable, comprises in fact all relevant parameters.

The Shannon entropy which is commonly used in information theory is defined as

$$H_1(x) = -\sum_{i=1}^{n} p_{\mathrm{i}} \log_2 p_{\mathrm{i}}, \tag{2}$$

where x defines the binary random variable and p_{i} the probability that x takes on zero or one. The limit of H_1 converges to the min-entropy:

$$H_\infty(x) = -\log \max_i p_{\mathrm{i}}. \tag{3}$$

When transmitting information, it is assumed to be correct on the receiver side, but in fact, the signal will be superimposed by noise with a specific bit error probability p_b. Assuming a given bit error probability we claim a failure rate of $P_{\mathrm{fail}} \leq 10^{-6}$. For simple codes, an estimation of the probability that a string of n bits has more than t errors is given by:

$$P_{\mathrm{fail}} = \sum_{i=t+1}^{n} \binom{n}{i} p_b^i (1-p_b)^{n-i} \tag{4}$$

With the use of a HDA, a key is derived from the raw PUF source bits by compressing the bits with a hash function. The amount of source bits that are needed to achieve a secret of a specific size is expressed in the so-called secrecy rate. The maximum achievable secrecy rate depends on the mutual information

$$I(x, y) = H(x) - H(x|y) \tag{5}$$

between the measurement done at enrolment x and reconstruction y, where $H(x|y)$ describes the remaining entropy of x when y is known. In more detail, $\lceil K/I(x, y)\rceil$ gives the number of required source bits to derive a secret of size K. [8] [18]

Given any $C[n, k, d]$ code the entropy loss within a practical realization of a HDA can be stated as $n - k$. It follows that the leftover entropy ℓ in the PUF response is given by $\ell = m + k - n$, relying on the commonly used Random Oracle model [2] [12], where the loss during the entropy extraction is assumed as 0.

4. Evaluation and Limitations

In the following, our aim is to show the limitations and boundary conditions when generating a 128-bit binary key based on different PUF instantiations, when having the quality aspects of Section 3 in mind. The used ASICs containing different PUF types are mounted on a customized evaluation board, that is connected via a ribbon cable to a Xilinx KC705 FPGA evaluation board. The ASICs are controlled via a dedicated IP block on the FPGA and the measurements are forwarded via a serial interface to a PC. We focused during the evaluation of raw PUF data on memory based PUFs, namely SRAM, Latch and DFF PUFs.

Type	p_b	N	$H_1(x)$	H_∞	$I(x,y)$	$W(x)$
SRAM	5.2%	65536	1.00	0.99	0.70	0.49
DFF	3.1%	8192	0.84	0.45	0.64	0.73
Latch	2.5%	8192	0.79	0.39	0.63	0.76

Table 1. Quality measures of memory-based PUFs at room temperature.

Table 1 lists in addition to the bit error rate, also the maximum number of source bits N as well as the entropy $H_1(x)$, the min-entropy $H_\infty(x)$, the mutual information $I(x, y)$ and the Hamming weight $W(x)$ for SRAM, DFF and Latch PUFs. The SRAM PUF behaves worst regarding the bit error rate with a value of 5.2%. In contrast, the other parameters such as the entropy values or the Hamming weight come close to an optimum. The biased output of DFF and the Latch PUF expressed by the Hamming weight influences the entropy and the min-entropy, which is significantly lower for these two PUF types. Figure 1 depicts the dependency between the code parameters n and d with respect to a failure rate $P_{\text{fail}} \leq 10^{-6}$ for the evaluated PUF types.

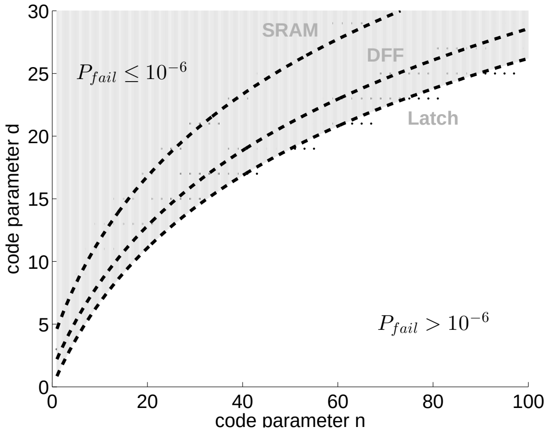


Figure 1. Dependency of the code parameters n and d regarding the failure rate P_{fail} for SRAM, DFF and Latch PUFs.

Targeting secure key generation, the leftover entropy is the second point that has to be considered. It is common practice to process the PUF response in blocks of equal length n. With a given entropy, the mutual information and a desired key length of 128 bit, a lower bound of the block numbers $l_{\min}$ is derived. Depending on the number of available source bits N, an upper bound $l_{\max}$ can be determined. As long as $l_{\max} > l_{\min}$, the key generation will be successful with maximum achievable entropy. Based on these assumptions, all free parameters can be combined to a threshold function

$$f_T(k,n) = k - sn - o, \tag{6}$$

where s is the slope, o the offset of the function and k, n are the variable code parameters. In Table 2 the fixed parameters of f_T are shown for a changing number of source bits and for the different PUF types. Generally, the slope of the threshold function tends to increase, when the entropy decreases at the same time. The key can be derived with maximum achievable entropy with a specific code when $f(k,n) \geq 0$.

	1024		2048		4096		8192	
Type	s	o	s	o	s	o	s	o
SRAM	0.19	0.32	0.09	0.46	0.04	0.55	0.02	0.59
DFF	0.68	0.39	0.61	0.50	0.58	0.47	0.57	0.50
Latch	0.74	0.43	0.67	0.53	0.64	0.48	0.63	0.56

Table 2. Parameters of the threshold function for the feasibility of key generation given the slope s and the offset o.

5. Conclusion

The aim of this paper was to present a hands-on guide on how to design tailored PUF-based key generation frameworks, taking into account the limitations given by the PUF source and the HDA. With the implementation of a threshold function, we are able to expose the limits of reliable key generation while considering the relevant quality aspects at the same time. There are a couple of published papers that describe the design of HDAs, the choice of the error correcting code, the consideration of entropy loss or statistical analysis of different PUF sources. To our best knowledge, however, there is no paper that tries to draw a complete picture, reaching from statistical investigation on the PUF source to the actual HDA design.

Acknowledgment. This work was supported in part by the European Commission through the ICT programme under contract FP7-ICT-2011-317930 HINT.

References

[1] Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Berk Sunar, and Pim Tuyls, *Memory leakage-resilient encryption based on physically unclonable functions*, Towards Hardware-Intrinsic Security, Springer, 2010, pp. 135–164.

[2] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, Francois-Xavier Standaert, and Yu Yu, *Leftover hash lemma, revisited*, Cryptology ePrint Archive, Report 2011/088, 2011, `http://eprint.iacr.org/`.

[3] Christoph Boesch, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, and Pim Tuyls, *Efficient Helper Data Key Extractor on FPGAs*, Proceedings of the 10^{th} International Workshop on Cryptographic Hardware and Embedded Systems CHES 2008, Lecture Notes in Computer Science, vol. 5154, Springer Berlin Heidelberg, 2008, pp. 181–197 (English).

[4] J. Delvaux and I. Verbauwhede, *Key-recovery attacks on various RO PUF constructions via helper data manipulation*, Proceedings of the Conference on Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014, March 2014, pp. 1–6.

[5] Jeroen Delvaux, Dawu Gu, Dries Schellekens, and Ingrid Verbauwhede, *Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **PP** (2014), no. 99, 1–1.

[6] Jeroen Delvaux and Ingrid Verbauwhede, *Fault Injection Modeling Attacks on 65nm Arbiter and RO Sum PUFs via Environmental Changes*, IACR Cryptology ePrint Archive **2013** (2013), 619.

[7] Jeroen Delvaux and Ingrid Verbauwhede, *Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation*, Topics in Cryptology CT-RSA 2014, Lecture Notes in Computer Science, vol. 8366, Springer International Publishing, 2014, pp. 106–131 (English).

[8] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls, *FPGA Intrinsic PUFs and Their Use for IP Protection*, Proceedings of the 9^{th} International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727, Springer Berlin Heidelberg, 2007, pp. 63–80 (English).

[9] Maximilian Hofer and Christoph Boehm, *An Alternative to Error Correction for SRAM-Like PUFs*, Proceedings of the 12^{th} Internatinal Workshop on Cryptographic Hardware and Embedded Systems, CHES 2010, Lecture Notes in Computer Science, vol. 6225, Springer Berlin / Heidelberg, 2011, pp. 335–350.

[10] Stefan Katzenbeisser, Ünal Kocabaş, Vladimir Rožić, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann, *PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions(PUFs) Cast in Silicon*, Proceedings of the 14^{th} Internatinal Workshop on Cryptographic Hardware and Embedded Systems CHES 2012, Lecture Notes in Computer Science, vol. 7428, Springer Berlin Heidelberg, 2012, pp. 283–301 (English).

[11] P. Koeberl, Jiangtao Li, A. Rajan, and Wei Wu, *Entropy loss in puf-based key generation schemes: The repetition code pitfall*, Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on, May 2014, pp. 44–49.

[12] Roel Maes, *Physically unclonable functions - constructions, properties and applications*, Springer, 2013.

[13] Roel Maes, Pim Tuyls, and Ingrid Verbauwhede, *Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs*, Proceedings of the 11^{th} International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2009, Lecture Notes in Computer Science, vol. 5747, Springer Berlin Heidelberg, 2009, pp. 332–347 (English).

[14] Roel Maes, Anthony Van Herrewege, and Ingrid Verbauwhede, *PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator*, Proceedings of the 14^{th} International Workshop on Cryptographic Hardware and Embedded Systems CHES 2012, Lecture Notes in Computer Science, vol. 7428, Springer Berlin Heidelberg, 2012, pp. 302–319 (English).

[15] Roel Maes and Ingrid Verbauwhede, *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions*, Towards Hardware-Intrinsic Security, Springer Berlin Heidelberg, 2010, pp. 3–37 (English).

[16] R.S. Pappu, *Physical one-way functions*, Massachusetts Institut of Technology, 2001.

[17] Ying Su, J. Holleman, and B.P. Otis, *A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations*, IEEE Journal of Solid-State Circuits **43** (2008), no. 1, 69–77.

[18] Robbert van den Berg, Boris Skoric, and Vincent van der Leest, *Bias-based Modeling and Entropy Analysis of PUFs*, Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices (New York, NY, USA), TrustED '13, ACM, 2013, pp. 13–20.

[19] Vincent van der Leest, Bart Preneel, and Erik van der Sluis, *Soft Decision Error Correction for Compact Memory-Based PUFs Using a Single Enrollment*, Proceedings of the 14^{th} International Workshop on Cryptographic Hardware and Embedded SystemsCHES 2012, Lecture Notes in Computer Science, vol. 7428, Springer Berlin Heidelberg, 2012, pp. 268–282.

On the linear complexity profile of certain sequences derived from elliptic curves

László Mérai, Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria

Joint work with Arne Winterhof

Let $\mathbb{F}_q$ be the finite field of q elements with a prime power q satisfying $\gcd(q, 6) = 1$ and let $\mathbf{E}$ be an elliptic curve defined by the *short Weierstrass equation*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{F}_q$$

over $\mathbb{F}_q$ with non-zero discriminant.

The $\mathbb{F}_q$-rational points $\mathbf{E}(\mathbb{F}_q)$ of $\mathbf{E}$ form an Abelian group (with respect to the usual addition which we denote by $\oplus$) with the point at infinity $\mathcal{O}$ as the neutral element.

Let $\mathbb{F}_q(\mathbf{E})$ be the function field of $\mathbf{E}$ over $\mathbb{F}_q$. For an $f \in \mathbb{F}_q(\mathbf{E})$ we define the *elliptic curve generator for pseudorandom numbers* (r_n) *with respect to* f as the sequence

$$r_n = f(W_n) = f(G \oplus W_{n-1}) = f(nG \oplus W_0), \quad n = 1, 2, \dots,$$

with $G, W_0 \in \mathbf{E}(\mathbb{F}_q)$.

The *elliptic curve power generator* (s_n) *with respect to* f is defined as

$$s_n = f(e^n G), \quad n = 1, 2, \dots$$

where the integer $e \geq 2$ is co-prime to the order $|G|$ of the point G.

In this talk we present several results concerning the linear complexity of the sequences (r_n) and (s_n).

The *linear complexity profile* $L(s_n, N)$, $N = 1, 2, \dots$, of a sequence (s_n) over $\mathbb{F}_q$ is a non-decreasing sequence where the N-th term is defined as the length L of a shortest linear recurrence relation

$$s_{n+L} = c_{L-1}s_{n+L-1} + \dots + c_1 s_{n+1} + c_0 s_n, \quad 1 \leq n \leq N - L$$

where $c_0, \dots, c_{L-1} \in \mathbb{F}_q$, that s_n satisfies. The value

$$L(s_n) = \sup_{N \geq 1} L(s_n, N)$$

is called the *linear complexity* of the sequence (s_n);

$$L(s_n) = L(s_n, 2t) \leq t.$$

Elliptic curve generator. The linear complexity profile $L(r_n, N)$ of the sequence (r_n) was already studied earlier for some special function f. For example, Hess and Shparlinski [1] obtained non-trivial bounds for a large family of functions, namely if the pole divisor of f is a multiple of a single place. We extend this family using Edwards coordinates.

An Edwards curve $\mathbf{C}$ over $\mathbb{F}_q$ is defined by

$$u^2 + v^2 = c(1 + du^2v^2),$$

where $c, d \in \mathbb{F}_q$, $d \neq 0, 1$, $c \neq 0$. For a non-square d over $\mathbb{F}_q$ the addition is defined by

$$(u_1, v_1) \oplus (u_2, v_2) = \left(\frac{u_1v_2 + u_2v_1}{c(1 + du_1u_2v_1v_2)}, \frac{v_1v_2 - u_1u_2}{c(1 - du_1u_2v_1v_2)} \right).$$

The points of the curve form a group with respect to this addition, with $(0, c)$ as the neutral element. We remark that every Edwards curve is birationally equivalent to an elliptic curve. On the other hand, if $\mathbf{E}(\mathbb{F}_q)$ has a unique point of order two, then $\mathbf{E}$ is birationally equivalent to an Edwards curve.

Theorem. *Let* $\mathbf{C}$ *be an Edwards curve and* $f \in \mathbb{F}_q(\mathbf{C})$ *such that the ideal points are poles. If* $G \in \mathbf{C}$ *of order* t *and* $w_n = f(nG)$*, then we have*

$$L(w_n, N) \geq \min \left\{ \frac{t - \deg f}{4 \deg f}, \frac{N - \deg f}{4 \deg f + 1} \right\}, \quad N \geq \deg f.$$

For example, if $f \in \mathbb{F}_q(\mathbf{C})$ is the sum of the coordinate functions: $f(u, v) = u + v$, then the theorem says, that the linear complexity profile of the corresponding sequence is large. However, if we use the birationally correspondence, we get a function which does not fulfill the requirement of the Hess-Shparlinski theorem.

Elliptic curve power generator. The computation of an element of the elliptic curve power generator from the previous ones is highly related to the generalized Diffie-Hellman problem thus it is thought to be 'secure'. In the next theorem we give an unconditionally result on the linear complexity of the sequences.

Theorem. *Let* $f \in \mathbb{F}_q(\mathbf{E})$ *be a non-constant function. If the order* $|G|$ *of* G *is a prime number and the multiplicative order of* e *mod* $|G|$ *is* t*, then*

$$L(r_n) \gg \frac{t}{|G|^{2/3}(\deg f)^{1/3}}.$$

References

[1] Florian Hess, Igor E. Shparlinski, *On the linear complexity and multidimensional distribution of congruential generators over elliptic curves*, Des. Codes Cryptogr. **35** (2005), 111–117.

WELLDOC property in bi-ideals

Raivis Bēts[3], University of Latvia, Institute of Mathematics and Computer Science
Joint work with Jānis Buls

A combinatorial condition called well distributed occurrences, or WELLDOC for short, has been introduced in [1] and [2]. The WELLDOC property for an infinite word u over an alphabet A means that for any integer m and any factor w of u, the set of Parikh vectors reduced by modulo m of prefixes of u preceding the occurrences of w equals $\mathbb{Z}_m^{|A|}$. The main aim of our work is the investigation of possible application of aperiodic infinite words in development and production aperiodic pseudorandom number generators (PRNGs) with good statistical behavior [3].

The proofs that WELLDOC property holds for the family of Sturmian words, and more generally, for Arnoux-Rauzy words are given in [1] and [2]. In our paper we analyse the WELLDOC property for bounded bi-ideals, a subclass of recurrent words, and prove the existence of a 2-bounded bi-ideal over the alphabet $A = \{0, 1\}$ that satisfies the WELLDOC property.

Let $A = \{a_0, \ldots, a_k\}$ be a finite, non-empty set of elements (letters), called an *alphabet.* An n-tuple $(u_0, \ldots, u_n)$ of a set A is called a *finite word* and is denoted $u = u_0u_1 \ldots u_n$. The set of all non-empty words of A is denoted A^+. An *empty word* of A is denoted by λ and we define $A^* = A^+ \cup \{\lambda\}$. Number $n+1$ is called the *length* of a finite word $u = u_0u_1 \ldots u_n$ and is denoted $|u| = n + 1$. A total map $x : \mathbb{N} \to A$ is called an *infinite word*, and the set of all infinite words is denoted by A^ω. Let $a\#b$, or simply ab, denote the word *concatenation.*

A word w is called a *factor* of a word u if there exist words x, y such that $u = xwy$. If $x = \lambda$, then w is said to be a prefix of u, but if $y = \lambda$, then w is a suffix of u. By $u[p, l]$ we denote the factor of the word u that starts in the position p and ends in the position l, i.e., $u[p, l] = u_pu_{p+1} \ldots u_l$. If the factor is a single letter, it is denoted $u[l]$ instead of $u[l, l]$. For any factor w of the infinite word u, every index i such that w is a prefix of the infinite word $u_iu_{i+1}u_{i+2} \ldots$ is called an *occurrence* of w in u.

An infinite word $x \in A^\omega$ is called *periodic* if it is of the form $x = u^\omega$, where $u \in A^+$ and ω denotes an infinite repetition. An infinite word x is called *eventually periodic* if it is of the form $x = vu^\omega$, where $u, v \in A^+$. An infinite word is called *aperiodic* if it is not eventually periodic. A sequence of finite words

$$v_0, v_1, \ldots, v_n, \ldots \tag{1}$$

is called a bi-ideal sequence if $v_0 \in A^+$, and

$$\forall i \geq 0 : v_{i+1} \in v_iA^*v_i \tag{2}$$

Let $\{u_i\}_{i\in\mathbb{N}}$ be an infinite sequence of finite words with $u_0 \neq \lambda$. Let us define a sequence of words $\{v_i\}_{i\in\mathbb{N}}$ by induction, so that:

$$\begin{gathered} v_0 = u_0, \\ v_{i+1} = v_iu_{i+1}v_i \end{gathered} \tag{3}$$

The limit of this sequence $x = \lim_{i\to\infty} v_i$ is called a *bi-ideal.*

A bi-ideal x is called a *finitely generated bi-ideal* if the sequence $\{u_i\}_{i\in N}$ is periodic. A bi-ideal x is called a *μ-bounded bi-ideal*, if there $\exists\mu$ such that

$$\forall i \in \mathbb{N} : |u_i| \leq \mu. \tag{4}$$

[3] Funded by ESF project 2013/0024/1DP/1.1.1.2.0/13/APIA/VIAA/045

The *Parikh vector* of a finite word over an alphabet $\{0,1,\dots,d-1\}$ is defined as

$$(|w|_0,|w|_1,\dots,|w|_{d-1}).$$

For a finite or infinite word $u=u_0u_1u_2\dots$, $Pref_n u$ will denote the prefix of length n of u, i.e., $Pref_n u = u_0u_1\dots u_{n-1}$.

Let $i_0, i_1, \dots$ denote the occurrences of w in an aperiodic infinite word u over the alphabet $\{0,1,\dots,d-1\}$. According to the definition, if for any $m\in\mathbb{N}$ and any factor w of u,

$$\{(|Pref_{i_j}u|_0,\dots,|Pref_{i_j}u|_{d-1}) \bmod m | j\in\mathbb{N}\} = \mathbb{Z}_m^d;$$

that is, the Parikh vectors of $Pref_{i_j}u$ for $j\in\mathbb{N}$, when reduced by modulo m, give the complete set $\mathbb{Z}_m^d$, then u has well distributed occurrences (that is, has the WELLDOC property).

As infinite words, which contain all finite words over an alphabet A as its factors, satisfy the WELLDOC property, it follows that there exists a bi-ideal with WELLDOC property. The main result of this paper is proof that there exists a 2-bounded bi-ideal in alphabet $\{0,1\}$.

The next goal is to find a good algorithm that generates a basis sequence $\{u_i\}_{i\in N}$ of a 2-bounded bi-ideal such that the bounded bi-ideal, generated by this basis sequence, satisfies the WELLDOC property. Having such algorithm would help us to produce aperiodic PRNGs with good statistical behavior.

References

[1] L. Balkova, M. Bucci, A. de Luca, J.Hladky, *Aperiodic pseudorandom number generators based on infinite words*, arXiv:1311.6002 [math.CO], 2013.

[2] L. Balkova, M. Bucci, A. de Luca, S.Puzynina, *Infinite Words with Well Distributed Occurrences*, In: J. Karhumaki, A. Lepisto, L. Zamboni (EDS.), *Combinatorics on Words,* LNCS 8079 (2013), 46-57, Springer.

[3] L.-S. Guimond, Jan Patera, Jiri Patera, *Statistical properties and implementation of aperiodic pseudorandom number generators*, Applied Numerical Mathematics 46(3-4), (2003), 295-318.

[4] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its applications, Vol.90, Cambridge University Press, 2002.

Statistical Analysis of a Novel Cryptosystem Based on Automata Compositions

Géza Horváth, University of Debrecen

Joint work with Pál Dömösi and József Gáll

Modern block cyphers are symmetric cryptosystems operating on fixed-length groups of bits, called blocks. These blocks contains at least 128 bits. The cryptosystem transforms the plaintext blocks into cyphertext blocks one by one. In [1] the authors introduced a novel block cypher based on abstract automata and Latin cubes. The basic idea of this novel cryptosystem is to use a giant size finite automaton and a pseudorandom generator. The set of states of the automaton consists of all possible plaintext/cyphertext blocks, and the input set of the automaton contains all possible pseudorandom blocks. The size of the pseudorandom blocks are the same as the size of the plaintext/cyphertext blocks: 128 bits. For each plaintext block the pseudorandom generator generates the next pseudorandom block, and the automaton transforms the plaintext block into a cyphertext block by the effect of the pseudorandom block. The key is the transformation matrix of the automaton. The problem with this idea is the following. The size of the transition matrix of the automaton is huge, namely $2^{128}\times 2^{128}\times 16$ bytes, which is impossible to store in the memory or on a hard disk. The solution is to use an automata network. Automata network consists of smaller automata, and it is able to simulate the work of a huge automaton [2].

A block cypher should have an appropriate avalanche effect, and a protection against differential cryptanalysis. This means, one bit change in the plaintext block should effect significant change in the cyphertext block, and one bit change in the cyphertext block should effect significant change in the corresponding plaintext block. To test our system, we calculated the number of the identical bytes in two 16 bytes long independent random strings. We have tested 1.000.000 pairs, and saved the result. We also compared 1.000.000 ciphertext block pairs, where the corresponding plaintext blocks had just 1 bit difference. Finally we compared 1.000.000 plaintext block pairs, where the corresponding ciphertext blocks had just 1 bit difference.

Based on the generated samples we considered three different statistical questions to analyse the distribution of the number of different blocks in the pairs. Clearly, in an ideal situation –where we have an appropriate avalanche effect– one should get a binomial distribution with parameters $n = 16$ and $p = 1 - 1/256$, which we shall call "reference distribution". Firstly, we simply estimated the 16 atoms of the distribution separately and calculated the corresponding (99.9 %) confidence intervals to see the difference of the probabilities from the ones of the reference binomial distribution mentioned above. Secondly, we certainly analised the goodness-of-fit of the distribution by a χ^2-test with binomial test distribution. Thirdly, assuming that the sample comes from a binomial distribution (based on the results obtained to the previous questions) we calculated the maximum likelihood estimation of the parameters and compared it to the parameters of the reference distribution.

The results from the statistical estimations and tests show that the distributions of the 3 samples are the same with the same parameters, their distribution coincides with the theoretical binomial distribution, which means that the cryptosystem has an appropriate avalanche effect, and it is protected against differential cryptanalysis.

References

[1] Pál Dömösi and Géza Horváth: *A novel cryptosystem based on abstract automata and Latin cubes*, Studia Scientiarum Mathematicarum Hungarica (2015), accepted for publication.

[2] Pál Dömösi and Chrystopher L. Nehaniv: *Algebraic theory of automata networks: An introduction*, ser. SIAM monographs on Discrete Mathematics and Applications **11**, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, (2005), doi 10.1137/1.9780898718492.

Hypothesis Testing and Multiplicity in the Evaluation of Cryptographic Randomness

Haydar Demirhan, Hacettepe University
Joint work with Nihan Bitirim

Security of a cryptographic application is highly related to the quality of randomness of the mechanism used to cipher a message. A ciphering process used to encrypt a message is mainly based on random numbers that have some special characteristics. In cryptographic applications, a special subset of pseudo-random numbers, namely cryptographic random numbers, is employed. Because pseudo-random numbers require a starting number sequence, which is called seed, they are reproducible. Although cryptographic random numbers have the same weakness, they satisfy very strong statistical requirements to be unpredictable. For a sequence of random variables, no autocorrelation and independence both imply randomness. A strong randomness is the key requirement for suitability of a random number generator (RNG) for use in cryptographic applications.

Because the quality of randomness constitutes the hearth of a ciphering process, it is very important to apprehend the mechanism behind the statistical testing of randomness. The quality of randomness of an RNG is evaluated and tested to confirm its suitability for use in encryption processes. This evaluation is done by statistical randomness tests. Randomness test of an RNG is conducted at two stages. First, empirical distribution of a test statistic is obtained and then goodness-of-fit of the empirical distribution to a theoretical distribution is statistically tested. For instance, it is possible to generate 2^m different sequences with a set of m zeros and ones. In a randomness test, whether these 2^m sequences occur with equal probability or not is tested under the null hypothesis "H_0 : Sequences generated by the RNG of interest are random". In the test of this null hypothesis, probabilities of making both true and false decisions are controlled. In the cryptography context, if we decide non-randomness of an RNG while it is actually generating random numbers, we commit a Type-I error, which is also called false positive decision. If we decide randomness of an RNG while it is not generating random numbers, we commit a Type-II error, which is called false negative decision and denoted by β. For a randomness hypothesis, power $(1-\beta)$ is the probability of deciding non-randomness of an RNG while it is actually non-random. The power measures the chance of identifying a non-random RNG correctly. Related with the Type-I error, significance level constitutes a pre-determined value for the Type-I error. For an appropriate and scientific way of testing randomness of an RNG, these concepts should be used properly. However, we identified misuses of these contexts in the literature of cryptography. In this study, we mention two examples from Alani [1] and L'Ecuyer and Simard [5] and criticize their use of hypothesis testing notions. Attracting attention to these issues is beneficial for a more reliable testing of RNGs.

There are more than a hundred statistical tests that can be used to test randomness of a sequence of numbers [4]. Because having tests with different characteristics is effectual in identification of deviations from randomness in different cases, use of collections of tests as test batteries is proposed in the literature [5, 6]. Each test in a test battery is applied separately to the RNG under consideration at α level of significance. If all or a predetermined portion of tests conclude that the RNG of interest generates random numbers, it is deduced that the degree of positive belief on randomness of the RNG is strong [2, 3, 7].

Although this manner of testing seems to be reasonable, it causes a severe problem called multiple testing problem in statistics. Multiple testing problem, also called multiplicity problem, is one of the basic problems seen in multiple hypothesis testing. Let us have k tests in a test battery and suppose that tests in the battery are conducted at a significance level of α. We have the following result on the probability of having at least one significant result:

$$\mathbb{P}(\{\text{at least one significant result}\}) = 1 - \mathbb{P}(\{\text{no significant results}\}) = 1 - (1-\alpha)^k \,.$$

For example, with $k = 7$ and $\alpha = 0.05$, we have a 30% chance of deciding that sequences generated by an RNG of interest is not random in at least one of the tests, even if all the tests actually indicate that the sequences are random. When we simultaneously use more than one test to evaluate randomness of an RNG, the probability of rejecting the null hypothesis simply due to chance increases with increasing values of k. It is apparently seen that one should regard the multiple testing problem in statistical testing of cryptographic randomness. However, to the best of our knowledge, there is no article in the cryptography literature focusing on the test of cryptographic randomness under multiplicity. In this study, we discuss multiplicity problem in terms of test batteries used to evaluate cryptographic randomness and figure impact of multiplicity on the decisions reached by the use of test batteries.

Consequently, for a reliable and scientifically suitable hypothesis testing in such an important and critical field, proper use of hypothesis testing notions and the problem of multiplicity in test batteries should be regarded. With this motivation, we focus on statistical randomness tests, test batteries, and use of basic statistical hypothesis testing context in testing the cryptographic randomness. We review the literature on the cryptographic randomness tests and provide basic information on test batteries as a whole. We focus on selection and interpretation of significance level and multiple testing problem in detail, evaluate each test battery according to the impact of conducting more than one statistical randomness test simultaneously and present some approaches for the solution of multiple testing problem for test batteries.

Acknowledgements

This work was supported by The Scientific and Technological Council of Turkey (TUBITAK) under the project 114F249 of ARDEB-3001 programme.

References

[1] Mohammed M. Alani, *Testing randomness in ciphertext of block-ciphers using diehard tests*, International Journal of Computer Science and Network Security **10** (2010), 53–57.

[2] Pedro M. Alcover, Antonio Guillamon, Maria C. Ruiz, *A new randomness test for bit sequences*, Informatica **24** (2013), 339–356.

[3] Charmaine Kenny, *Random number generators: An evaluation and comparison of random.org and some commonly used generators*, Trinity College Dublin Management Science and Information Systems Studies Project Report. URL: https://www.random.org/ analysis/Analysis2005.pdf, 2005. [Online; accessed 24-February-2014].

[4] Pierre L'Ecuyer, Peter Hellekalek, *Random number generators: Selection criteria and testing*, Random and Quasi-Random Point Sets Lecture Notes in Statistics **138** (1998), 223–265.

[5] Pierre L'Ecuyer, Richard Simard, *Testu01: A C library for empirical testing of random number generators*, ACM Transactions on Mathematical Software **33** (2007), Article 22.

[6] George Marsaglia, Wai W. Tsang, *Some difficult-to-pass tests of randomness*, Journal of Statistical Software **7** (2002), 3.

[7] Kinga Marton, Alin Suciu, Christian Sacarea, Octavian Cret, *Generation and testing of random numbers for cryptographic applications*, The Publishing House of the Romanian Academy **4** (2012), 368–377.

Cryptanalysis of POLAWIS

Mateusz Buczek, Enamor International

Abstract

POLAWIS is a family of block ciphers submitted for the CAESAR Competition by Arkadiusz Wysokiski and Ireneusz Sikora. The algorithm is based on non-commutative quaternion field and comes in two variants – one based on computations over finite field modulo prime number p and the second in the field of real numbers.

In this paper I'll propose some attacks on the first variant of the algorithm, which should be able to break a full 8-round version or a reduced round version depending on key scheme with just one known ciphertext/plaintext pair. I'll also show an improved attack that will break any key scheme (even with increased number of rounds) but will require more pairs of data. Some concerning features of the algorithm will also be addressed that may deem it unusable if not resolved.
Keywords: POLAWIS, block cipher, cryptology, cryptanalysis, authenticated encryption.

1. Overview

POLAWIS is a family of block ciphers with variable block and key sizes. It has a rather atypical construction, similar to ECB (Electronic Code Book). It uses some of the intermediate data from one function call to modify the key used in the next call.

The algorithm has two modes of operation one based on computations over finite field modulo prime number p and the second in the field of real numbers. Due to the fact that computation over the field of real numbers are much more complicated and can be biased by implementation/architecture/system issues I'll concentrate on the variant modulo p (though all the attacks presented below should also work in the field of real numbers).

2. Block size and key size

As stated above POLAWIS uses computations modulo prime number p (or in the field of real numbers with some degree of precision). The size n is the highest integer exponent of 2, such that $2n < p$ will determine the size of the block (or in the case of the other variant number of bits used to hold the real number, for instance 64 – double precision number).
Message is divided into blocks of $6n$ bits consisting of six numbers modulo p designated as $a_1, a_2, a_3, a_4, b_2, b_3$. The output block from the function call is slightly larger (to compensate for numbers between $2n$ and p) and consists of $6n + 6$ bits.
Authors suggest that the prime p shouldn't be smaller then 2^{256} and $p = 2^{256} + 297$ is proposed as the base of operation in the function which sets the block size at 1536 bits.

There are two key schemes available:

- Short-key scheme – key consists of two n-bit integers c_1 and c_4 which will be used in every round
- Long-key scheme – key consists of $2k$ n-bit integers, where k is the number of rounds in one POLAWIS function call (default number of rounds is 8 with 16 n-bit integers as key). Every value is used only once, hence two times the number of rounds.

Long-key scheme is deemed as more secure by authors and suggested as the basic mode of operation of POLAWIS. Key space is limited so that the first part of every round key is non-zero. With the proposed p the size of the key varies from 512 bits to 4096 bits depending on number of rounds.

3. Unresolved issues and assumptions

Unfortunately the biggest problem with the algorithm is the lack of precise specification. Some variables are unspecified or there are non described transitions between them.

For the rest of this paper I'll work under some assumptions for non resolved issues in the paper describing POLAWIS. Wherever there is a missing information or some degree of uncertainty I'll use best (security-wise) or the most possible explanation. This include:

- passing round output data to the input of next round,
- b_4 variable will be chosen in a deterministic way, based on supplied a_4,
- criteria $(c_1^2 + c_2^2 + c_3^2 + c_4^2) \neq 0 \pmod{p}$ from paper is passed and if not, algorithm uses next b_4 to guarantee that this will be true.

We will also show all the further operations assuming $p = 2^{256} + 297$ and computations over finite field modulo p.

4. Trivial attack on long-key scheme

First I'll present a trivial attack on the "more secure" version of the algorithm using long key scheme. For the attack we will need three pairs of one block message M and corresponding ciphertext C encrypted under secret key K.

The idea is quite trivial: we simply iterate through all possible values of 14 first integers used in the key which will require $2^{14 \cdot 256} = 2^{3584}$ operations. With every set of values we run the first seven rounds to get the input to the last one and, as we know the output – ciphertext C, we get a system of six linear congruence equations (from the decoding algorithm). By solving it we get the missing values of the key or if there is no solution, we assume that that the previous 14 numbers are incorrect and move to the next. Of course this method will generate many possible keys as the key space is larger then the block size by ratio of approximately $2^{4096}/2^{1536} = 2^{2560}$. This means we will need at least 3 pairs of plaintext/ciphertext to get, with a rather good degree of probability, the correct 4096-bit key K.

5. Attacks on short-key scheme

5.1. **One round.**

First let's look on the one round version of POLAWIS. The authors clearly stated in the paper that with one pair of plaintext and ciphertext it is easy to get the key. It's easy to show that to acquire the correct key one doesn't need a full input block. If we have a ciphertext that has nonzero values of at least for example first and second element we can get the key faster then with a full search with only first two elements of plaintext. We simply need to solve a trivial system of equations.

5.2. **Multiple rounds.**

Now let's look at the multiple round variant of the algorithm with short-key scheme. First attack described above won't work if the algorithm uses only one key – we cannot iterate through a part of it to single out the second one as they get intertwined really fast. Still we can try to build a system of congruence equations to get the rest of the key while iterating through all the possible values in second part.

After eight rounds we will get 6 equations with highest degree of monomials equal to $2^7 = 128$ which will consist of at max 8256 monomials each. Of course even though we got only two variables, solving this kind of system would be extremely hard. But there is a method to do so that will require more plaintext/ciphertext pairs. Let's designate every distinct monomial as new variable for the system. Now we got system of 6 linear equations with about 8256 variables and solving this kind of system is trivial, but we will get at least 8250 free variables (parameters). The question is how to eliminate them. And the answer is quite easy – get some more equations. The easiest way to get them is to go through more pairs of plaintext/ciphertext. Every pair generates 6 new equations, but some of them might not contribute to solving the system by being linearly dependent on previous equations. We will need at least 1375 pairs (most likely a bit more) to get a Cramer's system of equations which can be easily solved – we only need to get the values of two variables corresponding to c_1 and c_4. What can one do when not enough pairs are available? There is a tradeoff that will simplify the equations but at a great computation cost. We simply iterate through all possible values of for instance c_1 and treat them as known, which will make the equations dependent on only one variable. Number of monomials will drop to 128 so we will need only about 22 pairs to solve the system.

5.3. **Chosen Ciphertext Attack (CCA).** The attacks described in previous chapter can be further improved by changing the attacking model from Known Plaintext Attack (KPA) to Chosen Ciphertext Attack (CCA). We can build such a message that only two equations remain and they have much lower number of monomials in them – less then 30, so the attack is possible with only about 15 pairs of plaintext/ciphertext.

This attack also raises another concern with POLAWIS – if all input variables other then a_1 and a_4 are set to 0 then only output variables x_1 and x_4 will be nonzero, no matter how many rounds there will be and what key scheme we'll use. This may lead to some new attacks on the scheme and is a flaw of the construction (we can easily distinguish POLAWIS from a random function generator). Another effect of this is that our attack not only falls into CCA category but also can be described as Chosen Plaintext Attack (CPA).

6. Padding

As stated above the padding function works like this: "if the string is shorter, it must be supplemented by selected constants". Let's name the constants $pad_1, pad_2, ..., pad_6$ and assume that each of them is of length n. If the message misses t-bits to fill a full block we simply take them from as many pad_i as we require in ascending order. First we take the bits from pad_1, then pad_2 and so on starting from the most significant bit in every constant.

Now let's look at two messages one consisting of four 256-bit values: a, b, c, d and the other consisting of six: a, b, c, d, pad_1, pad_2. As we can easily see the first message is too short so the padding algorithm will append it with first two constants pad_1, pad_2. Second message has an ideal size so no padding is needed. Now we input two identical values into POLAWIS function and for the same key we get the same result. This means it is impossible to unambiguously decrypt the value.

7. Summary

As I showed above POLAWIS is susceptible to several kinds of attacks, that can reclaim key with effort much lower then exhaustive search. Attacks work for full version of algorithm with both long-key scheme and short-key scheme even with increased number of rounds. Further work may show a better attack using advanced numerical methods but might require more effort in building correct ciphertext for CCA. I also showed some issues concerning ambiguity of decryption of certain set of messages, which if unresolved, results in algorithm being unusable in any protocols. I strongly recommend that both problems should be resolved before moving using POLAWIS in any kind of cryptographic protocol.

References

[1] Arkadiusz Wysokinski and Ireneusz Sikora *POLAWIS*, CAESAR Competition Entry (2014).

A few notes on algebraic cryptanalysis

Pavol Zajac, Slovak University of Technology
Joint work with Viliam Hromada and Ladislav Öllös

1. Introduction

The algebraic cryptanalysis tries to solve cryptanalytic problems directly through their algebraic representation. One of the basic types of algebraic attacks is just to model an encryption with Boolean formula in conjunctive normal form (CNF). The unknown literals are mapped to internal state of the cipher during the encryption process, inputs, outputs and potential key bits. Then a SAT solver is applied to the CNF. The attacker can extract the key bits from the positive proof found by the solver (if it exists). Although the SAT problem is hard in general, there are some instances [1] when algebraic cryptanalysis using SAT solvers was found to be more efficient than brute force attacks.

In our contribution we focus on three particular practical issues arising when using SAT solvers (and other algebraic cryptanalytic tools in general). In the first part, we remark on the improvements we can get when keys are not taken from a uniform random distribution, but are "password based". In the second part, we focus on issues that are involved in distributing the algebraic attacks to many computational nodes. In the final part, we remark on attacks in multiple key scenario in which the attacker wants to recover just one out of many keys used for different encryptions.

All experiments are concluded on the simple example of round reduced DES. We remark that basic algebraic attacks are typically successful only against already weak ciphers. However, we can apply many of these basic techniques for more advanced scenarios involving algebraic complexity reduction [2], or in combination with other types of attacks [4, 5].

2. Password based keys

A basic algebraic attack encodes individual key bits as literals in some CNF formula. The proof of satisfiability for the CNF formula representing an individual encryption is provided by the SAT solver. Attacker can then determine values of the key bits according to the encoding used. E.g., a positive literal in the proof means that the corresponding key bit must have value 1.

Now let us suppose that a simple cipher is used for password storage in some custom "security" module. We can make an assumption on key space, such as that each key is chosen as a string of eight lowercase letters 'a'–'z', ASCII encoded into 56 DES key bits. The assumption can be then encoded as a CNF formula, and added to the encryption formula (with AND operator). If the password is indeed a string of lowercase letters, SAT solver provides a proof with the key bits. Otherwise, it provides the answer that formula is unsatisfiable.

Our experiments show that estimated complexity of the attack for reduced key space scenario in proportion to the brute force attack on reduced key space is similar to the ratio of estimated complexity of the attack on the whole cipher to the brute force attack on the whole key space. However, for very simple cases, such as 4-round DES and lowercase letters, we get additional reduction in complexity from very weak key diffusion.

This work was supported by project VEGA 1/0173/13. Part of the experiments were run on Slovak infrastructure for high performance computing under project Algebraic cryptanalysis.

3. Distributed computing

A basic algebraic attacks can be combined with partial key guessing. We can e.g., guess 28 bits of the DES key, and try to find the rest with a SAT solver. If the guess was incorrect the SAT solver provides answer "unsatisfiable", otherwise it provides the proof containing the rest of the key bits. In a distributed computing environment we can use individual guesses as a basis for distributing parallel tasks.

We have realised a series of experiments with six-round DES and MiniSat solver in distributed computing cluster. Our goal was to check the effects of task distribution on the (estimated) total time of algebraic attack. The experiments confirm the intuition that splitting the total computation to many tasks by guessing more individual bits increases the overall complexity of the attack, even excluding communication overhead. We suspect that this is mainly caused by reducing the efficiency of heuristics and learning methods in the solver by limiting the key space. Further experiments confirm that deterioration in efficiency caused by task distribution can be reduced by better selection of key bits that are being guessed. Moreover, in the large experiment, a good selection of individual bits to guess is much more important than the number of key bits guessed.

4. Multiple key scenario

In some instances, an attacker can have access to many individual P-C pairs $(P_1, C_1) \ldots (P_n, C_n)$, encrypted by potentially different keys $K_1, \ldots, K_n$. In multikey scenario the attacker wants to find any one of the keys $K_1, \ldots, K_n$. In our work, we do not use some specific properties of the cipher to provide one suitable pair with algebraic weakness such as in [3]. Instead, we encode the problem in a different way: We add formulas that encode I/O relations $(P_1 \wedge C_1) \vee \cdots \vee (P_n \wedge C_n)$, a single formula for internal state and key. Now, the SAT solver can produce a proof using any of the keys $K_1, \ldots, K_n$. This has an advantage over brute force attack, when we need to check each pair and each candidate key, until at least one suitable pair is found.

References

[1] Courtois, Nicolas T., and Gregory V. Bard. "Algebraic cryptanalysis of the data encryption standard." Cryptography and Coding. Springer Berlin Heidelberg, 2007. 152-169.

[2] Courtois, Nicolas. "Algebraic Complexity Reduction and Cryptanalysis of GOST." IACR Cryptology ePrint Archive 2011 (2011): 626.

[3] Courtois, Nicolas T. "CRYPTANALYSIS OF GOST IN THE MULTIPLE-KEY SCENARIO." Tatra Mountains Math. Pub. 57.1 (2013): 45-63.

[4] Gsecki, Arkadiusz. "LOW DATA COMPLEXITY DIFFERENTIAL-ALGEBRAIC ATTACK ON REDUCED ROUND DES." Tatra Mountains Math. Pub. 57.1 (2013): 35-43.

[5] Renauld, Mathieu, and Standaert, Franois-Xavier. "Algebraic side-channel attacks." Information Security and Cryptology. Springer Berlin Heidelberg, 2010.

Revocation in Distributed ABE-based Secure Storage using Indistinguishability Obfuscation

Máté Horváth[5], Laboratory of Cryptography and System Security (CrySyS Lab), Budapest University of Technology and Economics

Secure storage in clouds. Cloud computing is an emerging paradigm of information technology, by which computer resources are provided dynamically via Internet. Besides cost savings, flexibility is the main driving force of outsourcing for instance data storage, although on the other hand it raises the issue of security, which leads us to the necessity of encryption. In order to fulfil the new requirements of the cloud environment, that traditional cryptographic protocols handle inflexibly, new schemes have appeared.

Attribute-Based Encryption (ABE) was proposed by Sahai and Waters [SW05] as the generalization of Identity-Based Encryption. Contrary to traditional public-key cryptography, ABE is intended for one-to-many encryption in which ciphertexts are not necessarily encrypted to one particular user, but for those who fulfil certain requirements. These requirements are related to attributes and access policies, namely decryption is possible if and only if the attributes satisfy the access policy. Ciphertext-policy ABE, one of its two basic types, embeds the access policy into the ciphertext, which means that the encryptor can define requirements that the decryptor needs to fulfil in order to decrypt the ciphertext. By its design, it is a useful tool for access control to data, stored in the cloud, although it must be adjusted to some specific requirements.

One such requirement is the need for a tool for changing user's rights, which is essential when unexpected events occur. An occasion when someone' rights has to be revoked can be dismissal or the revealing of malicious activity. However, revocation is especially hard problem in ABE-based schemes, because different users may hold the same functional secret keys related to the same attribute set.

User revocation in CP-ABE. Indirect user revocation, based on the attributes, has multiple drawbacks. As different users might be identified by the same attributes, the keys of all those users have to be updated, who had any common attributes with the malicious user. In case of re-encryption, the drawback is similar: all ciphertext that used any of the affected attributes in the access policy must be re-encrypted, even if the revoked user could not decrypt that specific ciphertext before. This results in computational and communicational burden which can easily lead to a performance bottleneck.

Another approach avoids these inefficiencies by identifying malicious users directly, based on a unique "identity attribute" owned by each user. A list of revoked user's "global IDs" (GID) is also embedded in the ciphertext, besides the access policy and negation of theses specific attributes is provided. As a result, a potential decryptor must satisfy the access policy, but also needs to compare his GID with the revoked ones in the ciphertext. Decryption is possible only if no correspondence was found and the policy is satisfied by the owned attributes. Instead of putting extra burden of key regeneration on authorities, the extra computation caused by revocation is distributed between the largest set of parties, the users, during encryption and decryption. Another benefit is that lazy re-encryption is achievable only by extending the revoked user list (RL) and using the fresh list for encryption, after data was edited. However long revocation lists and immediate re-encryption still can cause a serious burden.

Indistinguishability obfuscation. The intuitive goal of obfuscation is to make programs "unintelligible" while preserving their functionality. One possible approach to capture the unintelligibility property was proposed by Barak et al. in their seminal work [BGI+01]. The definition of indistinguishability obfuscation ($i\mathcal{O}$) requires that if two programs of similar size compute the same function, then their obfuscations should be indistinguishable. This notion not just evades the negative results of the same paper, but in 2013 Garg et al. [GGH+13] managed to give the first candidate construction for general purpose obfuscation, according to this definition (about

[5] mhorvath@crysys.hu

the latter development of the $i\mathcal{O}$ constructions see the survey of [Hor15b]). Since then, $i\mathcal{O}$ turned out to be an extremely useful cryptographic primitive, that already was used for solving long-standing open problems such as the constructions of functional encryption [GGH+13], witness encryption [GGSW13] or deniable encryption [SW14]. However, the breakthrough also posed a bunch of further questions about the security guarantees, efficiency and application approaches. The difficulty, from the point of view of the last, is that $i\mathcal{O}$ does not give an intuitive guarantee that the obfuscated version practically "hides information". In our application we partly use the so called "punctured programming" approach of Sahai and Waters [SW14] to bridge this gap.

Contribution. We concentrate on access control for data, stored in the cloud thus we are going to make use of the results of [Hor15a], that allows multiple, independent attribute authorities and ID-based user revocation. Such systems that use a centrally controlled revocation list, the ciphertexts will embed a growing sequence of revocation sets. Thus the decryptor is always forced to prove that his GID is not identical with some other GIDs. However the revocation list will always contain partly the same GIDs, the "proof" must be prepared separately for each ciphertexts in order to decrypt them. Although it is obviously a waste of computation, this property is common in the list-based revocation systems like [LSW10, LXZ13, Hor15a]. The reason is that in order to avoid the need for multiple proofs, some kind of coordination between different encryptors would be necessary. We use a developing new cryptographic primitive, indistinguishability obfuscation, to *reduce* both the *ciphertext length* (in case of large number of revoked users) and the necessary computation for decryption by allowing the reuse of proofs of not being a specific user.
Our main contribution is that we *avoid parallelisms* by securely delegating computation of some revocation related parameters of ciphertexts to the cloud service provider (CSP), thus the *extra burden is divided between all parties*, not only between the users or the authorities, as before.

Theorem (informal)**.** *In multi-authority CP-ABE with identity-based user revocation, it is possible to securely delegate the revocation related computation of encryption to a third party.*

It not just solves the above mentioned problem of coordination, but also *allows immediate partial re-encryption* of ciphertext parameters with an extended RL, in such a way that after re-encryption no user from the refreshed list can retrieve the data, who did not decrypted it previously. This approach has the additional benefits, that the CSP who re-encrypts, cannot gain any information from the process, as the ciphertext is not decrypted and the *attribute related parameters do not even have to be modified.*
Although these results aim to increase efficiency, at the moment they are far more inefficient than other methods, because of $i\mathcal{O}$, the used underlying primitive, which is a promising new tool that still faces initial difficulties. Regarding these, our work stands in the line of recent studies that motivate further research on $i\mathcal{O}$ by representing its extreme usefulness, now also in the field of user revocation in ABE-based access control.

Our technique. Here we only highlight the main ideas and refer to the scheme in [Hor15a] as our starting point, furthermore we use the same notions for the ease of expression. The original ABE ciphertext there, contains functionally three kinds of parameters. The hidden data, blinded with a random $s \in \mathbb{Z}_p$, the secret shares of s, that can be extracted using a satisfying attribute set, although the reconstruction of the secret will also reconstruct an other value $s^* \in \mathbb{Z}_p$, that will still hide s. This redundant value can be recovered from the last two parameters, if there is no correspondence between the elements of RL an the decryptor's GID and used to gain s in order to recover the data:

$$CT = (\underbrace{C_0}_{\text{Data hidden with } s}, \{\overbrace{C_{1,x}, C_{2,x}, \underbrace{C_{3,x}}_{\text{Shares of } s^*}}^{\text{Shares of } s}\}_{x=1\ldots n}, \{\underbrace{C^*_{1,k}, C^*_{2,k}}_{\text{Shares of } s^*=\sum_1^r s_k}\}_{k=1\ldots r}),$$

where x runs on the rows of the access matrix and k on the indexes of RL. It can be seen that a revocation event affects $C^*_{1,k}, C^*_{2,k}$ and $C_{3,x}$. As the s^* secret must be refreshed, $C_{3,x}$ has to be updated for all $x = 1 \ldots n$. However if the other two parameters could be somehow computed centrally and used in all ciphertexts then only the values corresponding to the newly revoked users ought to be generated. Based on this observation, we introduce a dummy revoked user with GID_0^* and divide the previous ciphertext into two parts:

$$CT_{user} = (\underbrace{C_0}_{\text{Blinding with } s}, \{\overbrace{C_{1,x}, C_{2,x}, \underbrace{C_{3,x}, C'_{3,x}, C''_{3,x}}_{\text{Shares of } s^*}}^{\text{Shares of } s}\}_{x=1\ldots n}, \underbrace{C^*_{1,0}, C^*_{2,0}}_{\text{Share of } s^* - \sum_1^r s_k}), \quad CT_{cloud} = \{\overbrace{C^*_{1,k}, C^*_{2,k}}^{s_k \text{ shares for revoked } GID_k^*}\}_{k=1\ldots r}$$

after which for $k \geq 1$ it is enough to compute $C^*_{1,k}, C^*_{2,k}$ once and use them in each ciphertexts (e.g. as a part of the revocation list), so the decryptor also have to extract s_k-s only once and later can reuse them. As it can be obtained only in a blinded form (with a secret identifier of the user), only minor modifications on the security proof of [Hor15a] are needed in order to prove security of this modification in the random oracle and generic bilinear group models.

To enable re-encryption by the CSP without information leakage, the CSP need to use s^* and its secret shares, during the computation of parameters without gaining their values. To achieve this, we construct three algorithms, the $i\mathcal{O}$ obfuscated versions of which will be given to the the CSP. The first creates $C^*_{1,r+1}, C^*_{2,r+1}$ parameters for a newly revoked GID^*_{r+1}. The second generates a new s^* for a specific ciphertext, together with the dummy share of GID_0^*, that is adjusted to be $s_0 = s^* - \sum_1^{r+1} s_i$. Finally the last one updates $C_{3,x}, C'_{3,x}, C''_{3,x}$ to contain the shares of the fresh s^*.

When constructing these algorithms we merge two approaches. With the "two key" encryption technique (in spirit similar to the one used in the bootstrapping of $i\mathcal{O}$ in [GGH+13]), we ensure the secrecy of those values that must be transmitted between the algorithms or between encryptor and the CSP. The generated pseudo-random values, like secret exponents are hidden using the "punctured programming approach" of Sahai and Waters [SW14]. With the help of these, we construct alternative, functionally equivalent programs, which either use different keys or which simply does not contain the interesting information. Equivalence is proved through a hybrid argument after which, from the properties of $i\mathcal{O}$, security of the algorithms follows.

The encryption in this scheme is partly done by the CSP. First the user chooses a random s^* and s_0 for the dummy GID_0^*, so decryption is not possible as s_0 is not a share of s^*. However in the cloud, the ciphertext can be "re-encrypted" (or completed) by the CSP, using the two algorithms for re-encryption, that creates the correct parameters such that $s^* = \sum_0^r s_k$. The decryptor then always need to obtain s_0 (that is always possible as GID_0^* is not a real user, only a dummy one), and further GID comparisons are necessary only when a new element was added to the revocation list since the last decryption of any ciphertext.

References

[BGI+01] Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im) possibility of obfuscating programs. In *Advances in Cryptology-CRYPTO 2001*, pages 1–18. Springer, 2001.

[GGH+13] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 40–49. IEEE, 2013.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 467–476. ACM, 2013.

[Hor15a] Máté Horváth. Attribute-Based Encryption Optimized for Cloud Computing. In G.F. Italiano et al., editor, *SOFSEM 2015: Theory and Practice of Computer Science*, number 8939 in LNCS, pages 566–577. Springer, 2015.

[Hor15b] Máté Horváth. Survey on Cryptographic Obfuscation. Cryptology ePrint Archive, Report 2015/412, 2015. `http://eprint.iacr.org/`.

[LSW10] Allison Lewko, Amit Sahai, and Brent Waters. Revocation systems with very small private keys. In *IEEE Symposium on Security and Privacy*, pages 273–285, 2010.

[LXZ13] Qinyi Li, Hu Xiong, and Fengli Zhang. Broadcast revocation scheme in composite-order bilinear group and its application to attribute-based encryption. *International Journal of Security and Networks*, 8(1):1–12, 2013.

[SW05] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005*, pages 457–473. Springer, 2005.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: Deniable encryption, and more. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 475–484, New York, NY, USA, 2014. ACM.

Access structures induced by uniform polymatroids

Renata Kawa, University of Silesia
Joint work with Mieczysław Kula

A secret sharing scheme, introduced by Shamir [1], is a method of dividing a secret data s among a finite set $P = \{p_1, \ldots, p_n\}$ of participants in such a way that only certain subsets of participants, called the *authorized subsets*, can reconstruct the secret by pooling together their private shares of information. The collection Γ of authorized subsets is called the *access structure* of the secret sharing scheme. It is natural to require that Γ is monotone, that is, if $A \in \Gamma$ and $A \subseteq B \subseteq P$, then $B \in \Gamma$. Let the set of minimal elements of an arbitrary family $\Lambda \subseteq 2^P$ be denoted as $\min \Lambda$.

It is clear that if P is fixed and a secret sharing scheme for P is given, then its access structure is uniquely determined. However, investigations concerning secret sharing scheme problems also refer to the situation in which a monotone family of sets of P is given and a goal is to find a scheme realizing it.

A secret sharing scheme is called *perfect* if

(1) every authorized set of participants can reconstruct the secret by pooling together their private shares of information,

(2) every unauthorized set of participants cannot reveal any information about the secret by pooling together their private shares.

A secret sharing scheme is called *ideal* if it is perfect and $|U_i| = |S|$, where S is the set of all possible values of the secret s and U_i is the set of all possible values of the share u_i of i-th participant.

An access structure Γ is called *ideal* if there exists an ideal secret sharing scheme such that Γ is its access structure.

The most desired schemes are ideal. It is proven in [2] and [3] that for every monotone family of sets of participants there exists a perfect scheme realizing it. Unfortunately, perfect schemes constructed by the authors of this statement are not ideal, each share is a vector with many entries. It is also known that there exist monotone families of sets of participants which are not realized by any secret sharing scheme that is both ideal and perfect (see [3], p. 33, Theorem 3).

From now on we consider only perfect secret sharing schemes. One of many branches of investigations concerning secret sharing schemes is studying a hierarchy introduced by an access structure. When we have fixed an access structure Γ, we say that the participant p is *hierarchically superior or equivalent* to the participant q, and we write $q \preceq_\Gamma p$, if

$$\bigwedge_{A \subseteq P \setminus \{p,q\}} A \cup \{q\} \in \Gamma \Rightarrow A \ \cup \{p\} \in \Gamma.$$

If $q \preceq_\Gamma p$ and $p \preceq_\Gamma q$, then we say that p and q are *hierarchically equivalent* and we write $p \sim_\Gamma q$.

For a partition $\Pi = \{P_1, \ldots, P_m\}$ of the set P, an access structure Γ on P is said to be Π-*partite* if every two participants in the same block P_i are hierarchically equivalent. In the set Π we can define the following relation:

$$P_i \preceq_\Gamma P_j \iff \bigvee_{q \in P_i} \bigvee_{p \in P_j} q \preceq_\Gamma p.$$

In such a situation we say that block P_j is *hierarchically superior or equivalent* to the block P_i. This relation is reflexive and transitive, but it does not have to be antisymmetric. Such a relation is called *pre-order*. If $P_i \preceq_\Gamma P_j$ and $P_j \preceq_\Gamma P_i$, then the blocks P_i and P_j are called *hierarchically equivalent* and we write $P_i \sim_\Gamma P_j$. If $P_i \preceq_\Gamma P_j$ or $P_j \preceq_\Gamma P_i$, then the blocks P_i and P_j are said to be *comparable.* If $P_i \preceq_\Gamma P_j$ and $P_i \not\succeq_\Gamma P_j$, then we say that the block P_j is *hierarchically superior* to the block P_i and we write $P_i \prec_\Gamma P_j$. We say that P_i is a *maximal element* in $\Phi \subseteq \Pi$ if for all $P_j \in \Phi$ such that $P_i \preceq_\Gamma P_j$ we have $P_i = P_j$. We say that P_i is a *minimal element* in $\Phi \subseteq \Pi$ if for all $P_j \in \Phi$ such that $P_j \preceq_\Gamma P_i$ we have $P_i = P_j$.

Generally Π-partite access structures are called *multipartite.* A Π-partite access structure Γ is said to be *hierarchical* if P_i and P_j are comparable for every $i, j \in \{1, \dots, m\}$. A Π-partite access structure Γ is said to be *compartment* if P_i and P_j are not comparable for every $i, j \in \{1, \dots, m\}$. Hierarchical ideal access structures are completely characterized in [8]. As far as compartment ideal access structures are concerned, only some specific families are analyzed and classified. There are also some results for Π-partite access structures with small number of blocks. Notice that hierarchical and compartment access structures are two extreme cases of a wide range of access structures in which we consider partial hierarchy in a set of blocks. In our investigations we are particularly interested in studying multipartite access structures such that are different from hierarchical and compartment.

Let us remind the connection between matroids and access structures presented in [4]:

Theorem 1. *Each ideal access structure is a port of uniquely determined matroid $\mathcal{M} = (E, r)$.*

In the above theorem a *port of a matroid* is a family described as follows:

$$\Gamma_{p_0}(\mathcal{M}) = \{X \subseteq E \setminus \{p_0\} : r(X \cup \{p_0\}) = r(X)\},$$

where p_0 is a fixed element of E.

We should also remember that generally a port of an arbitrary matroid is an access structure, but it does not have to be ideal.

It is very convenient to present sets in Π-partite access structure as vectors. For a partition $\Pi = \{P_1, \dots, P_m\}$ of a set P and for every $A \subseteq P$ we define a mapping $\pi : 2^P \to \mathbb{N}_0^m$ given by

$$\pi(A) = (|A \cap P_1|, \dots, |A \cap P_m|).$$

It is easily seen that if $\pi(A) = \pi(B)$ and $A \in \Gamma$, then $B \in \Gamma$. That is, Γ is completely determined by the partition Π and the set of vectors $\pi(A), A \in \Gamma$.

To present our main tool and results, we need to introduce more definitions.

Definition 2. *A polymatroid $\mathcal{Z}$ is an ordered pair (Q, h) consisting of a finite set Q and function $h \colon 2^Q \to \mathbb{N}_0$ which fulfils the following conditions:*

(1) *$h(\emptyset) = 0$.*
(2) *If $X \subseteq Y \subseteq Q$, then $h(X) \leq h(Y)$.*
(3) *If $X, Y \in Q$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$.*

Notice that if we replace condition (1) by $h(X) \leq |X|$ for all $X \subseteq Q$, then $\mathcal{Z}$ is a matroid.

Let us adopt the following notations: $J_m = \{1, \dots, m\}, J'_m = \{0, 1, \dots, m\}$.

Definition 3. *A completion of a polymatroid $\mathcal{Z} = (J_m, h)$ is a polymatroid $\mathcal{Z}' = (J'_m, h')$ such that $h'\big|_{J_m} = h$ and $h'(\{0\}) = 1$.*

It is important to notice that a completion of a polymatroid is not determined uniquely. It is also easy to check that

$$\Delta(\mathcal{Z}') := \{X \subseteq J_m : h'(X \cup \{0\}) = h'(X)\}$$

is a monotone family of subsets of J_m.

If $\mathcal{Z} = (J_m, h)$ is a polymatroid and $X \subseteq J_m$, then we define the following family:

$$\mathcal{B}(\mathcal{Z}, X) = \{\bar{v} \in \mathbb{N}_0^m : \operatorname{supp}(\bar{v}) \subseteq X, \forall_{Y \subseteq X} |\bar{v}_Y| \leq h(Y), |\bar{v}_X| = h(X)\},$$

where $|\bar{v}_Y| = \sum_{i \in Y} \bar{v}_i$.

The following theorem, proved in [7], is crucial for our purposes and shows the connection between polymatroids and access structures.

Theorem 4. *Let $\Pi = \{P_1, \ldots, P_m\}$ be a partition of a set P and let $\mathit{\Gamma}$ be a Π-partite access structure. Then $\mathit{\Gamma}$ is a matroid port if and only if there exist a polymatroid $\mathcal{Z} = (J_m, h)$ such that $h(\{i\}) \leq |P_i|$ for every $i \in J_m$, and a completion $\mathcal{Z}'$ such that*

$$\min \mathit{\Gamma} = \min\{\bar{u} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta(\mathcal{Z}')\}.$$

We wish to use this theorem to investigate the partial hierarchy in the set of blocks of a multipartite access structure determined by a matriod port.

It is known that tripartite access structures that are matroid ports, are ideal (see [7]). Combining this statement with our results we can obtain an ideal access structure which is neither hierarchical nor compartment (see the table at the end of the abstract).

Our investigations are restricted to uniform polymatroids.

Definition 5. *A polymatroid (Q, h) is called uniform if $|A| = |B| \implies h(A) = h(B)$ for all $A, B \subseteq Q$.*

For simplicity of notation, we write $h_i = h(A)$ if $A \subseteq Q,\ |A| = i$. It follows from monotonicity that a sequence $(h_i)_{i=0,1,\ldots,|Q|}$ is not decreasing. Let us denote $g_i = h_{i+1} - h_i$. From submodularity it occurs that a sequence $(g_i)_{i=0,1,\ldots,|Q|-1}$ is not increasing. We managed to prove a simple characterization of uniform polymatroids.

Lemma 6. *Let $(g_i)_{i=0,1,\ldots,m-1}$ be a not increasing sequence of non-negative integers.*

Let $(h_i)_{i=1,2,\ldots,m}$ be a sequence such that $h_0 = 0$ and $h_i = h_{i-1} + g_{i-1}$ for $i = 1, \ldots, m$. Then (J_m, h), where the function $h : 2^{J_m} \longrightarrow \mathbb{N}_0$ is defined by $h(A) = h_{|A|}$, is a uniform polymatroid.

The following theorems summarize our current results. They have a common set of assumptions: Let $\Pi = \{P_1, \ldots, P_m\}$ be a partition of a set P. Let $\mathcal{Z} = (J_m, h)$ be a uniform polymatroid such that $h_m \leq |P_i|$ for every $i \in J_m$ and let $\mathcal{Z}'$ be its completion. Let $\mathit{\Gamma}$ be an access structure such that

$$\min \mathit{\Gamma} = \min\{\bar{u} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta(\mathcal{Z}')\}.$$

Theorem 7. *If $A \in \min \Delta(\mathcal{Z}')$, $|A| = k$, $h_1 > 1$ and $g_k > 0$, then the block P_j is not hierarchically superior or equivalent to the block P_i for all $i \in A$ and $j \in J_m \setminus A$.*

Corollary 8. *If $1 < h_1 < h_2$ and $\{i\} \in \Delta(\mathcal{Z}')$ for some $i \in J_m$, then P_i is a maximal element in the set $(\Pi, \preceq_{\mathit{\Gamma}})$.*

Corollary 9. *If $A \in \min \Delta(\mathcal{Z}')$, $j \in J_m \setminus A$, $h_1 > 1$, $g_k \neq 0$, then P_j is minimal in the set $(\{P_j\} \cup \{P_i \colon i \in A\}, \preceq_{\mathit{\Gamma}})$.*

Theorem 10. *Assume that there exist $A \in \min \Delta(\mathcal{Z}')$, $|A| \geq 2$, and elements $i \in A$, $j \in J_m \setminus A$ such that P_j and P_i are comparable. If $g_{m-1} > 0$, then $g_1 = \cdots = g_{m-1}$.*

Theorem 11. *Assume that there exist $A \in \min \Delta(\mathcal{Z}')$ and elements $i \in A$, $j \in J_m \setminus A$ such that P_j and P_i are comparable. If $g_{m-1} > 0$, then $h_1 = g_1 = \cdots = g_{m-1}$.*

Corollary 12. *If $h_1 = g_1 = \cdots = g_{m-1}$, then $\{A\} = \min \Delta(\mathcal{Z}')$, for a suitable $A \subseteq J_m$. If $A \neq J_m$, then P_i is hierarchically superior to P_j for all $i \in A$ and $j \in J_m \setminus A$. Otherwise the access structure is compartment.*

Theorem 13. *If $g_{m-1} > 0$ and $\mathit{\Gamma}$ is not compartment, then $\min \Delta(\mathcal{Z}') = \{k\}$ for some $k \in J_m$ or $h_1 = g_1 = \cdots = g_{m-1}$.*

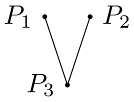
Corollary 14. *If a Π-partite access structure is determined by a uniform polymatroid, then the length of every chain in Π is not greater than 1.*

In order to illustrate applications of the above results, we enclose the following table. It presents partial hierarchy among blocks of tripartite access structures.

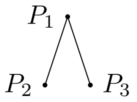
		1	2	3	4	5	6	7
		$g_1 = 0$ $g_2 = 0$	$1 \leq g_1 < h_1$ $g_2 = 0$	$1 \leq g_1 = h_1$ $g_2 = 0$	$1 \leq g_1 < h_1$ $1 \leq g_2 < g_1$	$1 \leq g_1 < h_1$ $1 \leq g_2 = g_1$	$1 \leq g_1 = h_1$ $1 \leq g_2 < g_1$	$1 \leq g_1 = h_1$ $1 \leq g_2 = g_1$
1	$\min \Delta = \{\{1\}\}$	–	–	–	G	G	G	g
2	$\min \Delta = \{\{1\}, \{2\}\}$	–	D	–	A	–	–	–
3	$\min \Delta = \{\{1\}, \{2\}, \{3\}\}$	p	A	–	A	A	–	–
4	$\min \Delta = \{\{1\}, \{2, 3\}\}$	–	G	G	A	–	A	–
5	$\min \Delta = \{\{1, 2\}\}$	–	–	–	A	D	A	D
6	$\min \Delta = \{\{1, 2\}, \{1, 3\}\}$	–	–	–	A	–	A	–
7	$\min \Delta = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$	–	A	A	A	–	A	–
8	$\min \Delta = \{\{1, 2, 3\}\}$	–	–	–	A	A	A	A

The legend:

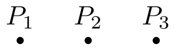
D



G



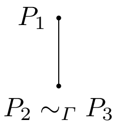
A



p

$P_1 \sim_\Gamma P_2 \sim_\Gamma P_3$

g



.

References

[1] Shamir A., *How to share a secret*, Communications of the ACM 22 (11), 612-613, 1979.

[2] Ito M., Saito A., Nishizeki T., *Secret Sharing Scheme Realizing General Access Structure*, Proceedings of the IEEE Global Telecommunications Conference, 99-102, 1987.

[3] Benaloh J., Leichter J., *Generalized Secret Sharing and Monotone Functions*, Proceedings of the Annual International Cryptology Conference on Advances in Cryptology, 27-35, 1988.

[4] Brickell E., Davenport D., *On the Classification of Ideal Secret Sharing Schemes*, Journal of Cryptology, 123-134, 1991.

[5] Padro C., Saez G., *Secret Sharing Schemes with Bipartite Access Structure*, IEEE Transactions on Information Theory 46 (7), 2596 - 2604, 2000.

[6] Farras O., Marti-Farre J., Padro C., *Ideal Multipartite Secret Sharing Schemes*, Lecture Notes in Computer Science 4515, 448 - 465, 2007.

[7] Farras O., Multipartite Secret Sharing Schemes, Doctoral dissertation, 2010.

[8] Farras O., Padro C.,*Ideal Hierarchical Secret Sharing Schemes*, Information Theory, IEEE Transactions on Information Theory 58 (5), 3273 - 3286, 2012.

On complexity of secret sharing schemes on access structures with rank three

Péter Ligeti, Eötvös Loránd University, Department of Computer Algebra

In a secret sharing scheme a piece of information – the secret – is distributed among a finite set of participants, such that only some predefined coalitions can recover it. This set of subsets is called access structure, which is supposed to be monotone, hence the system can be characterized by its minimal elements. Within this paper we consider access structures with rank three, i.e. with minimal subsets of size at most three and compare them with rank two or graph based schemes.

The efficiency of a scheme is measured by the amount of information the most heavily loaded participant must remember. For a given system, one of the most interesting problem of this topic is the exact determination or at least the estimation of this amount, called complexity. Secret sharing schemes with complexity 1 are called ideal schemes.

In contrast to the case of graph-based schemes, very little is known about the complexity of higher rank access structures. Within this paper we outline the known estimation methods for graph-based schemes and review the possible generalizations. Furthermore, we present several ideal schemes of rank three using tools from matroid theory and determine the complexity of small access structures. Especially, we determine the complexity of a large family of graphs by using star-covering and the entropy method.

Information

Lunch. Participants of CECC 2015 will be given vouchers for the university canteen “Mensa”, which is located in Universitätsstraße 90, opposite to Café Pazzo and Raiffeisenlandesbank; it is open Mon–Fri from 11:30 to 14:00.

Places to eat, shops and other useful locations around the university.

- University Cafeteria
  Central hall of the main building, Mon–Fri 8:00–14:00
- Bakery “Wienerroither”
  Universitätsstraße 98, Mon–Fri 6:30–18:30, Sat–Sun 6:30–14:00
- Restaurant “Mittagstisch”
  Lakeside Park B06, Mon–Fri 11:00–14:00
- Restaurant “Alles Gute”
  Lakeside Park B01, Mon–Fri 07:30–13:00
- Restaurant “Uni-Wirt”
  Nautilusweg 11, Tel.: +43 463 218905, Mon–Sat 8:00–24:00
- Café “Como”
  Nautilusweg 12, Mon–Fri 7:00–19:00, Sat 8:00–18:00
- Café and Bar “Pazzo”
  Universitätsstraße 33, Mon–Sun 7:00–24:00
- Osteria “Panta Rhei”
  Universitätsstraße 25, Tel.: +43 699 11404279, Mon 18:00 – 22:00, Tue–Fri 11:30 – 14:00 and 18:00 – 22:00, Sat 18:00 – 22:00
- Restaurant “Uni Pizzeria”
  Universitätsstraße 33, Tel.: +43 463 25088, Mon–Sat 11:00–23:00, Sun 11:00–22:00
- Restaurant “Chinesischer Garten”
  Villacher Straße 221, Tel.: +43 463 220139, Mon–Sun 11:30–14:30 and 17:30–23:30
- Restaurant “Maria Loretto”
  Lorettoweg 54, Tel.: +43 463 24465 (reservation recommended), Mon–Sun 11:00–24:00
- Restaurant “Villa Lido - Pizzeria Trattoria”
  Friedlstrand 1, Tel.: +43 463 210712 (reservation recommended), Mon–Sun 9:00–23:30
- Drugstore “Bipa”
  Universitätsstraße 37, Mon–Fri 8:00–19:00, Sat 8:00–18:00
- Supermarket “Spar”
  Villacher Straße 171, Mon–Fri 7:40–20:00, Sat 7:40–18:00
- Supermarket “Hofer”
  Villacher Straße 181, Mon–Fri 7:40–20:00, Sat 7:40–18:00
- Bank “Raiffeisenlandesbank Kärnten”
  Nautilusweg 11, Mon–Thu 8:00–12:30 and 13:30–15:30, Fri 8:00–15:30
- Bank “Kärntner Sparkasse”
  Nautilusweg 12, Mon–Fri 8:00–12:30 and 14:00–16:00
- Post office
  Lakeside B01 West, ground floor, Mon–Fri 8:00–12:00
- Newspapers, magazines, cigarettes (“Trafik”)
  Universitätsstraße 23, Mon–Fri 7:30–12:30 and 15:00–18:00, Sat 7:30–12:30
- Pharmacy “Uni-Apotheke”
  Universitätsstraße 23, Tel.: +43 463 210349, Mon–Fri 8.00–18:30, Sat 8:00–12.00

Taxi. These are the main companies that run a taxi service in Klagenfurt.

Taxi-Funkzentrale: +43 463 31111 (`http://www.taxi-klagenfurt.at`)
Taxi Erich: +43 463 46276

Taxi 2711: +43 463 2711 (`www.taxi2711.at`)
Taxi 23222: +43 463 23222 (`www.taxi-23222.at`)
Taxi 22277: +43 463 22277 (`www.taxi-22277.com`)
Taxi Funkkette: +43 463 281111
Taxi Klagenfurt: +43 463 499799 (`www.taxi-klagenfurt.com`)
Taxi Weratschnig KEG: +43 664 2410444 (`www.taxi-weratschnig.at`)
Lindwurmtaxi: +43 676 4419077 (`www.klagenfurter-taxi.com`)

Typical taxi fares (approximately)

Airport to university: €20
Airport to city center: €14
City center to university: €13

Train station to university: €15
Train station to city center: €9

Tourist Information. The tourist information office of Klagenfurt can be found in the town hall (*Rathaus*) in Neuer Platz.

Tel.: +43 463 5372223
E-mail: tourismus@klagenfurt.at
`http://www.info.klagenfurt.at/`
Mon–Fri 8:00–18:00, Sat 10:00–17:00, Sun 10:00–15:00

Swimming. The University of Klagenfurt is located near the beautiful lake Wörthersee. There are two public swimming areas in the proximity of the campus: Strandbad Klagenfurt and Strandbad Maria Loretto.

Opening hours: Mon–Sun from 8:00 to at least 19:00 (depending on the weather)
Daily ticket: €4.30 (from 15:00 €3.10, from 19:00 €2.00)
2-hour ticket: €3.10

Emergency numbers (Notruf).

- European emergency number: 112
- Fire brigade (*Feuerwehr*): 122
- Police (*Polizei*): 133
- Ambulance (*Rettung*): 144

https://www.math.aau.at/cecc2015/