MPF-based digital signature using Fiat-Shamir heuristic

Extended Abstract

Aleksejus Mihalkovich[1], Eligijus Sakalauskas[1] and Kestutis Luksys[1]

Kaunas University of Technology, Lithuania, aleksejus.michalkovic@ktu.lt

Keywords: matrix power function · digital signature · Fiat-Shamir heuristic · non-commuting cryptography

Introduction

ML-DSA is a Schnorr-like signature scheme and applies the Fiat-Shamir heuristic to an interactive protocol between the prover and the verifier. Similarly to the standardized ML-DSA, which uses matrices to construct an MLWE problem, our research in asymmetric cryptography is also based on matrix computations. Moreover, we think that particular interest is to continue the investigation and research of non-commutative algebraic structures to create quantum-safe cryptographic schemes. One of the possible approaches is to use the so-called matrix power function (MPF), which is a conjectured one-way function [7]. This way we can keep our proposals fairly close to the classical early algorithms.
MPF can have numerous realizations depending on platform and power matrices definition. In our recent work, we consider the family of modular maximal-cyclic groups usually denoted by $\mathbb{M}_{2^t}$, which is defined by two non-commuting generators a and b and the following relations:

$$\mathbb{M}_{2^t} = \langle a, b | a^{2^{t-1}} = e, b^2 = e, bab^{-1} = a^{2^{t-2}+1} \rangle, \tag{1}$$

where e is the identity of the group. These groups have a valuable property that they cannot be represented either by direct or a free product of several groups [2]. This is useful since the discrete logarithm mapping cannot be applied to simplify the cryptanalysis of problems defined in such groups. Therefore, we think that the realization of digital signatures based on such groups has some scientific interest.
Here we use the results previously published in [3] as a basis to construct a valid signature using the Fiat-Shamir heuristic. Additionally, we consider the secure parameter values of our signature based on the output of the selected hash function.

1 Mathematical background

Let $\mathbb{S}$ be a multiplicative (semi)group, where each element has a multiplicative order of at most $\operatorname{ord}\mathbb{S}$. Also, let $\mathbb{Z}_{\operatorname{ord}\mathbb{S}}$ be the ring of integers, where operations are performed modulo $\operatorname{ord}\mathbb{S}$. We use the notations $\mathbb{S}^{m\times m}$ and $\mathbb{Z}_{\operatorname{ord}\mathbb{S}}^{m\times m}$ to denote sets of matrices with entries in $\mathbb{S}$ and $\mathbb{Z}_{\operatorname{ord}\mathbb{S}}$ respectively.

Definition 1 *Let $\mathbf{W} \in \mathbb{S}^{m\times m}$ and $\mathbf{X} \in \mathbb{Z}_{\operatorname{ord}\mathbb{S}}^{m\times m}$ be two square $m \times m$ matrices. The left-sided matrix power function (LMPF) is a mapping $\mathbb{Z}_{\operatorname{ord}\mathbb{S}}^{m\times m} \times \mathbb{S}^{m\times m} \mapsto \mathbb{S}^{m\times m}$ denoted as $\mathbf{E}_L = {}^{\mathbf{X}}\mathbf{W}$, where $\mathbf{E}_L \in \mathbb{S}^{m\times m}$ is the left matrix exponent with entries calculated as follows:*

$$(e_L)_{ij} = \prod_{k=1}^{m} w_{kj}^{x_{ik}}. \tag{2}$$

Definition 2 *Let $\mathbf{W} \in \mathbb{S}^{m\times m}$ and $\mathbf{Y} \in \mathbb{Z}_{\operatorname{ord}\mathbb{S}}^{m\times m}$ be two square $m\times m$ matrices. The right-sided matrix power function (RMPF) is a mapping $\mathbb{S}^{m\times m}\times\mathbb{Z}_{\operatorname{ord}\mathbb{S}}^{m\times m}\mapsto\mathbb{S}^{m\times m}$ denoted as $\mathbf{E}_R=\mathbf{W}^{\mathbf{Y}}$, where $\mathbf{E}_R\in\mathbb{S}^{m\times m}$ is the right matrix exponent with entries calculated as follows:*

$$(e_R)_{ij}=\prod_{k=1}^{m} w_{ik}^{y_{kj}}. \tag{3}$$

We refer to $\mathbb{S}$ as a *platform (semi)group* and to $\mathbb{Z}_{\operatorname{ord}\mathbb{S}}$ as a *power ring*. Also, we refer to $\mathbf{W}$ as a *base matrix* and to $\mathbf{X},\mathbf{Y}$ as the *power matrices*.
Notably, in our case $\mathbb{S}=\mathbb{M}_{2^t}$ is non-commuting, and hence the order of operations matters. Therefore, in this paper, we use the notions of LMPF and RMPF mappings. However, since it is clear from the context which mapping (left- or right-sided) is being applied we may omit the first letter of the abbreviations, and refer to them simply by MPFs.
To ensure the validity of our previous MPF-based schemes where we used $\mathbb{M}_{2^t}$ as a platform group we have defined the following templates [4]:

- The base matrix $\mathbf{W}\in\mathbb{M}_{2^t}^{m\times m}$ has the following structure [4]:

$$\mathbf{W}=\begin{pmatrix} ba^{2\omega_{11}+1} & a^{\omega_{12}} & \dots & b^{\alpha_{1c}}a^{\omega_{1c}} & \dots & ba^{2\omega_{1m}+1}\\ a^{2\omega_{21}} & a^{\omega_{22}} & \dots & b^{\alpha_{2c}}a^{\omega_{2c}} & \dots & a^{2\omega_{2m}}\\ \dots & \dots & \dots & \dots & \dots & \dots\\ a^{2\omega_{i1}} & a^{\omega_{i2}} & \dots & b^{\alpha_{ic}}a^{\omega_{ic}} & \dots & a^{2\omega_{im}}\\ \dots & \dots & \dots & \dots & \dots & \dots\\ a^{2\omega_{(m-1)1}} & \dots & \dots & \dots & \dots & a^{2\omega_{(m-1)m}}\\ ba^{2\omega_{m1}+1} & a^{\omega_{m2}} & \dots & b^{\alpha_{mc}}a^{\omega_{mc}} & \dots & ba^{2\omega_{mm}+1} \end{pmatrix}, \tag{4}$$

  where the values of ω_{ij} can be chosen randomly from the ring $\mathbb{Z}_{2^t}$ and the value of c between 2 and $m-1$ is chosen at random and fixed afterwards.

- The generator $\mathbf{L}\in\mathbb{Z}_{2^t}^{m\times m}$ of the set of left power matrices has the following structure [4]:

$$l_{i1}+l_{im}\equiv 0 \bmod 2 \quad \forall i=1,2,\dots,m. \tag{5}$$

  Other entries of the matrix $\mathbf{L}$ can be chosen freely from $\mathbb{Z}_{2^t}$.

- The generator $\mathbf{R}\in\mathbb{Z}_{2^t}^{m\times m}$ of the set of right power matrices has the following structure [4]:

$$r_{cj}\equiv 0 \bmod 2 \quad \forall j=1,2,\dots,m. \tag{6}$$

  Other entries of the matrix $\mathbf{R}$ can be chosen freely from $\mathbb{Z}_{2^t}$.

Notably, any of the power matrices satisfying these templates are singular modulo 2, and hence power matrices cannot be inverted modulo any power of two. Furthermore, these templates are preserved when calculating polynomials of the form $f(x)=\alpha_1 x+\alpha_2 x^2+\dots+\alpha^k x^k$. However, if the templates are neglected, then the key identity does not hold, and hence the cryptographic primitive falls apart.

2 Sigma identification protocol

We now present the SIP previously proposed in [3]. The prover generates his data: a private key $\mathbf{PrK}=(\mathbf{X},\mathbf{Y})$, where $\mathbf{X}=\sum_{i=1}^{m-1}x_i\mathbf{L}^i$ and $\mathbf{Y}=\sum_{i=1}^{m-1}y_i\mathbf{R}^i$. His public key is $\mathbf{A}=\left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}$.
Assume that the prover desires to prove his identity to the verifier without revealing it. He initiates the following three-step communication [3]:

1. The prover picks at random two coefficient vectors $\vec{u}$ and $\vec{v}$ and computes matrices $\mathbf{U}=\sum_{i=1}^{m-1}u_i\mathbf{L}^i$, $\mathbf{V}=\sum_{i=1}^{m-1}v_i\mathbf{R}^i$.
2. Using these matrices he calculates a commitment $\vec{\mathbf{C}}=\{\mathbf{C}_0,\mathbf{C}_1,\mathbf{C}_2\}$, where:

$$\mathbf{C}_0=\left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{V}},\quad \mathbf{C}_1=\left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{Y}},\quad \mathbf{C}_2=\left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{V}}. \tag{7}$$

3. The verifier generates a challenge of the form $\vec{\mathbf{H}} = \{\mathbf{H}_1, \mathbf{H}_2\}$, where $\mathbf{H}_1 \in \mathrm{Span}(\mathbf{L})$, and $\mathbf{H}_2 \in \mathrm{Span}(\mathbf{R})$ come from linear spans of the first m powers of $\mathbf{L}$ and $\mathbf{R}$ denoted by $\mathrm{Span}(\mathbf{L})$ and $\mathrm{Span}(\mathbf{R})$ respectively. Note that the zeroth power is excluded since the identity matrix does not follow the presented templates. He sends the challenge $\vec{\mathbf{H}}$ to the prover.
4. The prover responses by computing a vector $\vec{\mathbf{S}} = \{\mathbf{U} + \mathbf{H}_1\mathbf{X}, \mathbf{V} + \mathbf{Y}\mathbf{H}_2\}$. The response $\vec{\mathbf{S}}$ is sent to the verifier.

The verifier accepts if the following key identity is valid:

$$\left({}^{\mathbf{S}_1}\mathbf{W}\right)^{\mathbf{S}_2} = \mathbf{C}_0 \odot \mathbf{C}_1^{\mathbf{H}_2} \odot {}^{\mathbf{H}_1}\mathbf{C}_2 \odot {}^{\mathbf{H}_1}\mathbf{A}^{\mathbf{H}_2}. \tag{8}$$

Interestingly enough, the order of actions on the right-hand side of identity (8) does not matter since all the base matrices (i.e., $\mathbf{C}_i$'s and $\mathbf{A}$) consist of commuting entries.

3 Fiat-Shamir heuristic

We use the secure hash algorithm 3 (SHA-3), which comes from a subset of the Keccak family of cryptographic primitives, to implement the Fiat-Shamir heuristic. For the commitment $\vec{\mathbf{C}}$ and the message μ we compute SHA-3$(\vec{\mathbf{C}}, \mu)$. We use the hash output to obtain the coefficients of polynomials used to calculate the challenge $\vec{\mathbf{H}}$. Therefore, we need the SHA-3 to produce a hash of length at least $2m \cdot (t-1)$ bits. We cut the obtained string into $2m$ parts of $t-1$ bits, i.e. SHA-3$(\vec{\mathbf{C}}, \mu) = \alpha_1 \| \alpha_2 \| \ldots \| \alpha_m \| \beta_1 \| \beta_2 \| \ldots \| \beta_m$, where $\|$ is the concatenation operator.
The Fiat-Shamir signature scheme can now run as presented below:

1. The signer performs the first and second steps of the SIP. In other words, he acts as a prover and obtains a pair of matrices $(\mathbf{U}, \mathbf{V})$ and a commitment vector $\vec{\mathbf{C}}$;
2. The signing algorithm *SignAlg* calculates a challenge $\vec{\mathbf{H}}$ as presented above and sends it to the signer. Therefore, *SignAlg* acts as a verifier in the presented SIP but uses the SHA-3 to calculate two vectors of coefficients rather than generating them at random;
3. The signer calculates a response $\vec{\mathbf{S}}$ for the obtained challenge as in the SIP;
4. Upon obtaining the response *SignAlg* outputs a signature $\mathrm{Sig}(\mu) = (\vec{\mathbf{C}}, \vec{\mathbf{S}})$.

To check the validity of $\mathrm{Sig}(\mu)$ the verification algorithm *VerAlg* obtains a hash SHA-3$(\vec{\mathbf{C}}, \mu)$, calculates $\vec{\mathbf{H}}$ as above, and accepts the signature if the identity (8) is valid. Otherwise, *VerAlg* rejects the signature.

4 Security analysis

The security of our scheme is based on the following problem:

Definition 3 *Let $\mathbf{W} \in \mathbb{M}_{2^t}^{m \times m}$ be a publicly known matrix with the structure (4). Also, let $\mathbf{W} \in \mathbb{M}_{2^t}^{m \times m}$ be publicly known. A decisional non-commuting MPF problem is to decide if there is a pair of matrices $(\mathbf{X}, \mathbf{Y})$ satisfying constraints (5) and (6) respectively, such that $\mathbf{A} = \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}$.*

Previously we have considered the complexity of this problem in our paper [4]. There we have shown that this problem is NP-complete. However, in the context of the KEP, the challenge space is limited to the linear spans $\mathrm{Span}(\mathbf{L})$ and $\mathrm{Span}(\mathbf{R})$ for left and right power matrices respectively. Therefore the cardinality of the challenge space is $2^{2m(t-1)}$.
In the paper [5] we have shown that the entries of the MPF value matrix $\mathbf{A}$ are uniformly distributed in a cycle $\langle a \rangle$ generated py powers of a. Also, in that paper, we considered the security game aimed at compromising the Diffie-Hellman type KEP presented in [4]. Based on the results of that research we claim that the shared key matrix $\mathbf{K}$ is indistinguishable from a randomly generated matrix $\mathbf{K}'$ whose entries are uniformly and independently sampled from $\langle a \rangle$. Therefore, we make a conjecture that the presented scheme might be quantum-resistant. However, additional research is needed to either approve or disprove our claim.

The SIP presented here is built using the same tools as in [4]. Therefore, the challenge space remains the same. The main difference is that here we use three extra matrices as a commitment $\vec{\mathbf{C}}$. However, all of these matrices have the same structure as the public key matrix $\mathbf{A}$. Therefore, the explored statistical properties also hold for these matrices. Based on these facts we claim that $\left({}^{\mathbf{S}_1}\mathbf{W}\right)^{\mathbf{S}_2}$ is indistinguishable from a randomly generated matrix whose entries are uniformly and independently sampled from $\langle a \rangle$. Also, we have shown in [3] that the MPF-based SIP presented above has the special honest verifier zero-knowledge (HVZK) and knowledge soundness properties. Also, the presented scheme has unpredictable commitments, which can be formalized by the following proposition:

Proposition 1 *Assume that the prover's keys PrK and PuK as well as the conversation $(\vec{\mathbf{C}}, \vec{\mathbf{H}}, \vec{\mathbf{S}})$ are fixed. Then for the randomly chosen matrices $\widehat{\mathbf{U}} \in \mathrm{Span}(\mathbf{L})$ and $\widehat{\mathbf{V}} \in \mathrm{Span}(\mathbf{R})$ the probability that the prover and the verifier produce the conversation $(\vec{\mathbf{C}}, \vec{\mathbf{H}}, \vec{\mathbf{S}})$ is $2^{-2m(t-1)}$.*

The proof of this fact relies on the notion of linear span and its basis. Relying on these three properties and an exponentially growing challenge space, we claim that the proposed digital signature is secure [1].

5 Security parameters

Since SHA-3 produces outputs of predetermined length, namely $224, 256, 384$ or 512 bit strings, we base the choice of public parameters on the length of SHA-3 output.
Once the platform group size is chosen, the format of the square matrices is calculated momentarily. This is because we must have exactly $2m$ coefficients to define two polynomials. We present a table with public parameter values based on the length of the SHA-3 hash.

Table 1: Public parameters for standardized SHA-3 output lengths

SHA-3-224	SHA-3-256	SHA-3-384	SHA-3-512
$\mathbb{M}_{32}, m = 28$	$\mathbb{M}_{32}, m = 32$	$\mathbb{M}_{16}, m = 64$	$\mathbb{M}_{32}, m = 64$
$\mathbb{M}_{256}, m = 16$	$\mathbb{M}_{512}, m = 16$	$\mathbb{M}_{32}, m = 48$	$\mathbb{M}_{512}, m = 32$
$\mathbb{M}_{512}, m = 14$	$\mathbb{M}_{2^{17}}, m = 8$	$\mathbb{M}_{128}, m = 32$	$\mathbb{M}_{2^{17}}, m = 16$
$\mathbb{M}_{2^{15}}, m = 8$	$\mathbb{M}_{2^{33}}, m = 4$	$\mathbb{M}_{512}, m = 24$	$\mathbb{M}_{2^{33}}, m = 8$

We can see from the presented table that we have to settle for a balance between two parameters t and m. We think that $\mathbb{M}_{512}$ is a reasonable candidate for the platform group for practical implementation since this group can be used for all of the standardized hash lengths, and the size of matrices is sufficient. Furthermore, creating coefficients from a hexadecimal string produced by most software is easy. However, note that the security of our scheme comes from the complexity of the decisional non-commuting MPF problem and the security game defined in [4].

Conclusions

In this paper, we have shown how to construct the digital signature based on the MPF mapping defined over a non-commuting algebraic group using the Fiat-Shamir heuristic. Relying on our previous results, we have proven Proposition 1, thus establishing unpredictable commitments property. Furthermore, in Section 5, we used the standardized SHA-3 function to generate the vector of coefficients to calculate the power matrices. Based on our observations, summarized in Table 1, we suggest $\mathbb{M}_{512}$ as a platform group for our scheme.

References

[1] Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography.*

[2] Helen Grundman and Tara Smith. Automatic realizability of galois groups of order 16. *Proceedings of the American Mathematical Society*, 124(9):2631–2640, 1996.

[3] Aleksejus Mihalkovich, Kestutis Luksys, and Eligijus Sakalauskas. Sigma identification protocol construction based on mpf defined over non-commuting platform group. *Mathematics*, 10(15):2649, 2022.

[4] Aleksejus Mihalkovich, Eligijus Sakalauskas, and Kestutis Luksys. Key exchange protocol defined over a non-commuting group based on an np-complete decisional problem. *Symmetry*, 12(9):1389, 2020.

[5] Aleksejus Mihalkovich, Jokubas Zitkevicius, and Eligijus Sakalauskas. The security analysis of the key exchange protocol based on the matrix power function defined over a family of non-commuting groups. *AIMS Mathematics.*, 9(10):26961–26982, 2024.

[6] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. Number Federal Information Processing Standard (FIPS) 204. August 2024.

[7] Eligijus Sakalauskas, Narimantas Listopadskis, and Povilas Tvarijonas. Key agreement protocol (kap) based on matrix power function. *Advanced Studies in Software and Knowledge Engineering*, 2(4):92–96, 2008.

Public key cryptosystem design based on MRHS problem (Extended Abstract)

Milan Vojvoda Pavol Zajac *

Slovak University of Technology in Bratislava, Slovakia

Multiple Right-Hand Sides (MRHS) equations are formal inclusions in the form $\mathbf{xM} \in S$, where $\mathbf{M}$ is some known matrix, and S is a set of potential right-hand sides. In general, it is difficult to solve a system of MRHS equations. In [2], we show that the existence of a solution of a random MRHS system (MRHS problem) is an NP-complete problem. On the other hand, we study some specific classes of MRHS systems, which can be solved in polynomial time. Given existence of easy and (probably) difficult instances, it is conceivable that MRHS problem can be a basis for a (quantum resistant) public key cryptosystem.

In [4] we have presented a concept of a digital signature scheme based on MRHS equation systems. The main principle of the system was to describe a symmetric cipher with a masked set of MRHS equations. The secret key was based on the symmetric key of the underlying cipher. The signature generation was produced by simulating encryption, while signature could be verified by checking the consistency of the MRHS system. Unfortunately, practical versions of the system based on known ciphers (such as AES and LowMC) could be solved with MRHS solver [1] due to a structured version of the joint matrix of the MRHS system.

Our new idea of the MRHS problem based public key cryptosystem is based on observations from [3]. If the joint matrix of the MRHS system is sparse, the system can potentially be solved by a class of bit-flipping algorithms (and as further research shows, it can be even faster with genetic algorithms). On the other hand, MRHS systems with dense joint matrix seem difficult to solve with any known method, while easy to verify (they are in the NP class). Thus, we might try to construct a public key system based on trap-door one-way function, where the trap-door basically masks underlying sparse MRHS system (easy to solve), and presents public dense MRHS system (hard to solve).

The main idea of the public key cryptosystem

Let $\mathbf{M}$ be random sparse $n \times km$ matrix over $\mathbb{F}_2$. The matrix can be written as a concatenation of m blocks $\mathbf{M}_i$ with n rows and k columns each. Furthermore, we require that $rank(\mathbf{M}) = n$, and $rank(\mathbf{M}_i) = k$, for each $i = 1, 2, \ldots, m$. Let $\mathbf{R}$ be a random dense invertible $n \times n$ matrix over $\mathbb{F}_2$. Matrices $(\mathbf{R}, \mathbf{M})$ form a secret key of the cryptosystem. In practical terms, they can be deterministically derived (e.g. using a PRNG or XOF) from a shorter secret key k of required length given by desired security level. Dense matrix $\mathbf{P} = \mathbf{RM}$ is the public key.

It should be difficult to factor public matrix $\mathbf{P}$ into the original secret components $\mathbf{R}$, $\mathbf{M}$, or to find other decomposition $\mathbf{P} = \mathbf{R'M'}$, where $\mathbf{M'}$ is sparse. This problem is related to binary matrix factorization [5], but we have not been able to find an exact reference for this specific type of problem.

The encryption process is simple: Let $\mathbf{m} \in \mathbb{F}_2^n$ be a cleartext. In this abstract we suppose it is a random bit string. Let $\mathbf{v} = \mathbf{mP}$. Split vector $\mathbf{v}$ into m blocks of length k denoted by $\mathbf{v}_i$. Select m random strings $\mathbf{c}_i$ of length k, such that $\mathbf{c}_i \in_R \mathbb{F}_2^k \setminus \{\mathbf{v}_i\}$. The encryption of message $\mathbf{m}$ is $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m)$.

*This work was in part supported by the NATO SPS project G5985, and in part by grant VEGA 1/0105/23.

The encrypted message along with matrix $\mathbf{P}$ gives rise to a MRHS system in the form $\mathbf{mP}_i \in \mathbb{F}_2^k \setminus \{\mathbf{c}_i\}$ (which can be simply written as $\mathbf{mP}_i \neq \mathbf{c}_i$). In general, it is difficult to compute the solution of this MRHS system.

The recipient can however compute a solution of the hidden MRHS system $\mathbf{yM}_i \neq \mathbf{c}_i$, using algorithm that exploit the sparsity of the joint matrix $\mathbf{M}$. After this, the recipient finds the decrypted message using $\mathbf{m} = \mathbf{yR}^{-1}$.

Parameter selection

The parameters of the cryptosystem must be carefully selected to create a secure system. Parameter k defines an equivalence between the public and hidden MRHS system, and a related k-XOR-SAT problem. For given k, we need a different ratio between the number of MRHS equations m and number of unknowns n. The ration should be selected in such a way that random system of given size should have exactly one solution (or respectively, expected on average). Note that due to the construction, we are guaranteed that the solution of the system exists, but we want to ensure there are no other (false) solutions. However, if we increase m two much, it might be possible to find the sparse decomposition of the public matrix.

Larger k increases the ciphertext size, thus optimal selection seems to be $k = 2$. The public system can be mapped to 2-XOR-SAT problem, which is polynomially equivalent to 3-SAT, and thus NP-hard. On the other hand, sparse (secret) verion of the problem is nearer to a 2-SAT problem, which is polynomially solvable. The density of the secret matrix (average number of ones in each column) cannot be too low, otherwise the matrix factorization is trivial (due to repeated colums). On the other hand, the complexity of solving the corresponding secret systems quickly grows with the density. Thus we should use lowest possible density that ensures that sparse matrix factorization is difficult.

For $k = 2$, every MRHS equation is satisfied (vector $\mathbf{yM}_i \in S$) with probability $3/4$. Probability that each of the MRHS equations in the system is satisfied is $(3/4)^m$. The condition that we expect 1 solution on average requires that $2^n \cdot (3/4)^m = 1$. Given n, we get that $m = -n/\log_2(3/4) \approx 2.4n$.

Note that n should be larger than security level λ. Using approach from [1], we can solve the public system by using linear algebra to produce $3^{n/2}$ candidate solutions in the first $n/2$ blocks, which are verified using the rest of the system. Thus, the logarithm of complexity is at most $n/2 \cdot \log_2(3) \approx 0.79n$. Thus, given security level λ, we need $n > 1.26\lambda$, $m > 3\lambda$. E.g. for security level $\lambda = 128$, we can use cleartexts of size $n = 162$ bits, and ciphertext of size $km = 768$ bits. The public key size is then $n \times km = 124416$ bits (15.2 kB). It might be possible to compress the system size further, if we can securely employ (quasi-)cyclic matrices instead of general matrices.

References

[1] Raddum, H., and Zajac, P. MRHS solver based on linear algebra and exhaustive search. *Journal of Mathematical Cryptology 12*, 3 (2018), 143–157.

[2] Zajac, P. MRHS equation systems that can be solved in polynomial time. *Tatra Mt. Math. Publ 67*, 1 (2016), 205–219.

[3] Zajac, P. On solving sparse MRHS equations with bit-flipping. *Publ. Math. Debrecen 100* (2022), 683–700.

[4] Zajac, P., and Spacek, P. A new type of signature scheme derived from a MRHS representation of a symmetric cipher. *Infocommunications Journal 11*, 4 (2019), 23–30.

[5] Zhang, Z., Li, T., Ding, C., and Zhang, X. Binary matrix factorization with applications. In *Seventh IEEE International Conference on Data Mining (ICDM 2007)* (2007), pp. 391–400.

SIGNITC: Supersingular Isogeny Graph Non-Interactive Timed Commitments

Knud Ahrens
University of Passau, Germany
knud.ahrens@uni-passau.de

1 Introduction

The concept of time-lock puzzles (TLP) [19] has been around for more than twenty years and timed commitments [5] developed shortly after. We will use the rather new definition of Non-Interactive Timed Commitment schemes (NITC) by Katz, Loss, and Xu [17] from the year 2020. These protocols satisfy binding and efficient verification just like usual commitment schemes, but a commitment can be opened by anyone after some delay t_{fd}, so hiding only lasts for this time t_{fd}. A possible application is a sealed bid auction, where all bids can be revealed after time t_{fd} even if some of the bidders refuse to open their commitment. Other applications include e-voting, fair coin tossing or contract signing [5].

Our approach uses random walks in the isogeny graph of supersingular elliptic curves to construct a NITC, hence the name Supersingular Isogeny Graph Non-Interactive Timed Commitments or SIGNITC[1] for short. The main idea is that computing isogenies of large or non-smooth degree is slow, but if we know the endomorphism ring of the starting curve, we can find a smooth shortcut. So we use a secret isogeny to a curve with known endomorphism ring for fast commitment and verification, but the forced decommitment has to compute the delay isogeny and thus it needs time at least t_{fd}.

The advantage of isogeny-based cryptography is that it is presumably quantum secure and relatively slow compared to other fields of post-quantum cryptography. Since we need a delay, this is a good thing. The field has undergone thorough scrutiny due to the candidates SIKE [16] and SQISign [12] in NIST competitions for post-quantum protocols and is still very active. The protocol has no theoretical black box algorithms like zero knowledge proofs, succinct non-interactive arguments of knowledge or one-way functions. To our knowledge this is the first quantum secure NITC scheme with explicit algorithms.

Related Work There are several NITC schemes [2, 10, 17, 21] using non-interactive zero knowledge (NIZK) proofs and/or repeated squaring in a group of unknown order, but none of them is quantum secure.

NITC schemes are related to verifiable delay functions (VDF) [6] in the sense that both have fast verification and a function that needs a long time to evaluate. We can construct NITC schemes from VDFs, but the contrary is difficult or impossible, depending on the protocol.

[1] pronounced like "signets"

VDFs have direct applications to blockchains and there already are several approaches. There are even some isogeny-based candidates for VDFs, but they all still have some flaws. The pairing-based approach [11] is not quantum secure. Chavez-Saab et al. [8] use SNARGS and their verification time increases for larger delays. Finally, there is one base on Kani's criterion for abelian surfaces [13], but the authors state that it is not clear how to implement it. A different approach based on endomorphism rings [1] has the problem that the generation of a challenge also gives (a significant advantage in finding) the response. So it is closer to a NITC scheme and gave the initial idea for this article. De Feo et al. [7] introduced isogeny-based delay encryption, but they use the same delay as the pairing-based VDF.

2 Preliminaries

Non-Interactive Timed Commitments The first formal definition of *Non-Interactive Timed Commitments* (NITC) was given by Katz et al. [17]. It consists of five algorithms `PGen`, `Com`, `ComVrfy`, `DecVrfy` and `FDecom` with the following properties: The parameter generation `PGen` produces a common reference string **crs**. The commitment algorithm `Com` takes a message m and has a commitment $\mathbf{C}$ and proofs π_{com}, π_{dec} as output. The proof π_{com} is used by the commitment verification algorithm `ComVrfy` to verify that $\mathbf{C}$ can be opened by `FDecom`. The decommitment verification algorithm `DecVrfy` uses π_{dec} to check if m corresponds to $\mathbf{C}$ and `FDecom` can forcefully open $\mathbf{C}$ to reveal m.

To be relevant for applications a NITC also needs to satisfy three further properties. It has to be *practical*, i.e. verification has to be faster than forced opening, and satisfy *hiding*, i.e. the commitment does not leak information about the message, and *binding*, i.e. a commitment can not be opened to two different messages.

Isogeny-based Cryptography An *isogeny* is a homomorphism between elliptic curves and isomorphic elliptic curves have the same j-invariant. Isogeny-based cryptography mainly uses isogenies between *supersingular* elliptic curves. These curves are defined over fields $\mathbb{F}_{p^2}$ of characteristic $p > 0$ and have endomorphism rings that are isomorphic to maximal orders $\mathcal{O}$ in the quaternion algebra $\mathcal{B}_{p,\infty}$ [20]. The *Deuring correspondence* relates an isogeny $\varphi\colon E \to E'$ of degree d between supersingular curves to a left $\mathcal{O}$- and right $\mathcal{O}'$-ideal I_φ of reduced norm d where $\mathcal{O} \cong \operatorname{End} E$ and $\mathcal{O}' \cong \operatorname{End} E'$ [22]. We assume that computing the codomain of an isogeny of degree $d = \prod q_i^{e_i}$ needs at least $\sum e_i\sqrt{q_i}$ field operations (for distinct primes q_i). For our purposes isogenies $\varphi\colon E \to E'$ can be given as a single point $K \in E$ generating its kernel and we write $E' \cong E/\langle K\rangle$.

Finding the endomorphism ring or equivalently the corresponding maximal order of a supersingular elliptic curve is considered a hard problem. Finding an isogeny between two given supersingular curves is also considered hard, but finding a left $\mathcal{O}$- and right $\mathcal{O}'$-ideal for given $\mathcal{O}$ and $\mathcal{O}'$ is not [23]. If we know the endomorphism ring of a supersingular curve E, we can use this to find shortcuts for an isogeny $\varphi\colon E \to E'$. To do this we translate the isogeny into an ideal, use KLPT [18] or similar algorithms to find an equivalent ideal of desired norm and use `IdealToIsogeny` algorithms to find an isogeny $\psi\colon E \to E'$ of smooth degree or a higher dimensional isogeny that allows to efficiently compute φ.

3 The Protocol

We start by fixing the supersingular elliptic curve $E_0 \colon y^2 = x^3 + x$ with known endomorphism ring $\operatorname{End} E_0$ and corresponding maximal order $\mathcal{O}_0$. Then we choose a prime $p \equiv 3 \bmod 4$ such that $d_s = 2^\kappa \gtrsim \sqrt{p}$ divides $p+1$ where κ is the security parameter. For a given delay $t_{\mathrm{fd}} \in \mathrm{poly}(\log p)$ we find e and $d_T = \prod q_i^{e_i}$ such that d_T is coprime to d_s, divides $p^e - (-1)^e$ and satisfies $\sum e_i \sqrt{q_i} \geq t_{\mathrm{fd}}$. Next we define a map $F : a + b\mathrm{i} \mapsto a + |b| \bmod N$ that maps j-invariants of supersingular elliptic curves (written as elements of $\mathbb{F}_p[\mathrm{i}] \cong \mathbb{F}_{p^2}$) into the group $M = \mathbb{Z}/N\mathbb{Z}$ for $N \leq \lfloor p^{1/4}/12 \rfloor$. Together with some precomputations this forms the common reference string **crs** that is generated by the parameter generation algorithm `PGen`.

For the commitment algorithm `Com` we randomly choose two secret isogenies $\varphi_s \colon E_0 \to E_s$ and $\varphi'_T \colon E_0 \to E'_T$ of fixed degrees d_s and d_T, respectively. Let the point $K'_T \in E_0$ be the generator of $\ker \varphi'_T$. Then the kernel of the pushforward $\varphi_T = [\varphi_s]_\star \varphi'_T \colon E_s \to E_T$ is generated by $K_T = \varphi_s(K'_T)$. The message $m \in M$ is hidden by computing $u = m - F(j(E_T)) \in M$ where $j(E_T)$ is the j-invariant of E_T. The output of `Com` is $(\mathbf{C}, \pi_{\mathrm{com}}, \pi_{\mathrm{dec}})$ where $\mathbf{C} = (E_s, K_T, u)$, π_{com} is empty and π_{dec} allows `DecVrfy` to use the same shortcuts as `Com`.

Given a commitment (E_s, K_T, u) the commitment verification `ComVrfy` just checks that E_s is a supersingular elliptic curve, K_T is a point on E_s, $u \in M$ and optionally $K_T \in \mathbb{F}_{p^{2e}}^2$. The decommitment verification `DecVrfy` uses π_{dec} to compute $F(j(E_T))$ the same way `Com` does. For given commitment $\mathbf{C}$ and message m it checks if $u + F(j(E_T)) = m$. To forcefully open a commitment (E_s, K_T, u) the algorithm `FDecom` computes $E_T \cong E_s/\langle K_T \rangle$ as codomain of the delay isogeny φ_T with kernel $\langle K_T \rangle$ and returns $m = u + F(j(E_T))$.

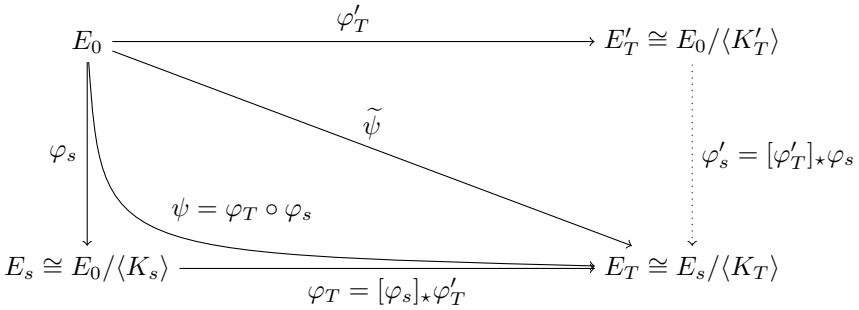

Figure 1: Walk in the isogeny graph with (efficiently computable) smooth degrees $\deg(\varphi_s), \deg(\widetilde{\psi})$ and large and/or non-smooth degree $\deg \varphi_T$.

Computing φ_s is fast because its degree d_s is smooth and divides $p+1$. The degree d_T, however, was chosen in a way that computing the delay isogeny φ_T is slow. To find a shortcut for `Com` and `DecVrfy` we use the knowledge of $\mathcal{O}_0$, φ_s and φ'_T. We translate the isogenies φ_s and φ'_T into ideals I_s and I'_T and compute the ideal $I_\psi = I_s \cap I'_T$ corresponding to the isogeny $\psi = \varphi_T \circ \varphi_s \colon E_0 \to E_T$. Then we use KLPT [18] and `IdealToIsogeny` algorithms to find an isogeny $\widetilde{\psi} \colon E_0 \to \widetilde{E}_T$ of smooth degree as in SQIsign [9] or a higher dimensional isogeny that allows to compute ψ efficiently as in SQIsign2D-West [3]. The 1-dimensional variant

is depicted in Figure 1. Note that these shortcuts might change E_T to $\widetilde{E}_T$ where $\widetilde{E}_T$ is isomorphic to E_T or its Galois conjugate, i.e. $j(\widetilde{E}_T) = a \pm b\mathrm{i}$ for $j(E_T) = a + b\mathrm{i}$. This allows us to efficiently compute $F(j(E_T)) = F(j(\widetilde{E}_T))$ and $u = m - F(j(E_T))$.

4 Security

Binding The commitment $\mathbf{C} = (E_s, K_T, u)$ fixes a curve $E_T \cong E_s/\langle K_T \rangle$ up to isomorphism so we have a unique j-invariant $j_T = j(E_T)$ associated to this commitment. Since M is a group and $u, F(j_T) \in M$ this gives a unique $m \in M$. So valid commitments can not be opened to different messages and SIGNITC satisfies binding.

Hiding An adversary sends two message m_0, m_1 and receives the commitment (E_s, K_T, u_b) corresponding to m_b for a random $b \in \{0, 1\}$. It knows that $F(j(E_T))$ is equal to $F_0 = \ominus u_b \oplus m_0$ or $F_1 = \ominus u_b \oplus m_1$, but none of them is more likely than the other. To verify one of them, it would have to find $F(j(E_T))$ and hence a curve isomorphic to E_T or its Galois conjugate. To find a shortcut for $\varphi_T \colon E_s \to E_T$ we need to know $\mathcal{O}_s \cong \operatorname{End} E_s$ or an isogeny connecting E_s to a curve with known endomorphism ring. Both φ_s and $\mathcal{O}_s \cong \operatorname{End} E_s$ are secret and finding an isogeny from E_0 to E_s or finding $\mathcal{O}_s \cong \operatorname{End} E_s$ are considered hard problems. We assume that the fastest attack (with a quantum computer) is to find an isogeny from E_0 to E_s in $\widetilde{O}(d_s^{1/4})$ operations [14, 15]. Since $d_s^{1/4} \gtrsim p^{1/8}$ and $t_{\mathrm{fd}} \in \operatorname{poly}(\log p)$, the fastest way to find $F(j(E_T))$ is to compute φ_T of degree $d_T = \prod q_i^{e_i}$, i.e. using `FDecom`, which is assumed to take at least $\sum e_i \sqrt{q_i} \geq t_{\mathrm{fd}}$ operations. So for time less than t_{fd} an adversary can choose the correct b only be negligibly better than guessing and SIGNITC satisfies hiding.

Practicality We want the verification (and optimally also the commitment) to be significantly faster than the forced decommitment. The commitment verification `ComVrfy` only needs $O(1)$ operations. The algorithms `Com` and `DecVrfy` are very similar. Computing isogenies of smooth degree, translating isogenies starting at E_0 into ideals and using KLPT and `IdealToIsogeny` has been implemented efficiently for SQIsign or SQIsign2D-West. So `Com` and `DecVrfy` need $\operatorname{poly}(\log p)$ operations. Forced decommitment `FDecom` is also polynomial in $\log p$, but it takes at least t_{fd} operations and we can make t_{fd} almost as large as $p^{1/8}$ without breaking hiding. So we can choose t_{fd} large enough to ensure that `Com`, `ComVrfy` and `DecVrfy` are much faster than `FDecom` and SIGINTC is practical.

Acknowledgments

The author would like to thank Antonio Sanso for pointing out the concept of NITC schemes, Valerie Gilchrist and Lorenz Panny and anonymous reviewers for their comments on previous versions of this article, Max Duparc for interesting discussions on pushforwards and higher dimensional isogenies, and Jens Zumbrägel for his support during the work on this article.

References

[1] Knud Ahrens and Jens Zumbrägel. DEFEND: Towards verifiable delay functions from endomorphism rings. Cryptology ePrint Archive, Paper 2023/1537, 2023. URL `https://eprint.iacr.org/2023/1537`.

[2] Miguel Ambrona, Marc Beunardeau, and Raphaël R. Toledo. Timed commitments revisited. Cryptology ePrint Archive, Paper 2023/977, 2023. URL `https://eprint.iacr.org/2023/977`.

[3] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. Sqisign2d–west. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology – ASIACRYPT 2024*, pages 339–370, Singapore, 2025. Springer Nature Singapore. ISBN 978-981-96-0891-1. doi: 10.1007/978-981-96-0891-1_11.

[4] Alex Biryukov, Ben Fisch, Gottfried Herold, Dmitry Khovratovich, Gaëtan Leurent, María Naya-Plasencia, and Benjamin Wesolowski. Cryptanalysis of algebraic verifiable delay functions. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 457–490, Cham, 2024. Springer Nature Switzerland. ISBN 978-3-031-68382-4. doi: 10.1007/978-3-031-68382-4_14.

[5] Dan Boneh and Moni Naor. Timed commitments. In Mihir Bellare, editor, *Advances in Cryptology – CRYPTO 2000*, pages 236–254, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg. doi: 10.1007/3-540-44598-6_15.

[6] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 757–788, Cham, 2018. Springer International Publishing. doi: 10.1007/978-3-319-96884-1_25.

[7] Jeffrey Burdges and Luca De Feo. Delay encryption. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 302–326, Cham, 2021. Springer International Publishing. ISBN 978-3-030-77870-5. doi: 10.1007/978-3-030-77870-5_11.

[8] Jorge Chavez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi. Verifiable isogeny walks: Towards an isogeny-based postquantum VDF. In Riham AlTawy and Andreas Hülsing, editors, *Selected Areas in Cryptography*, pages 441–460, Cham, 2022. Springer International Publishing. doi: 10.1007/978-3-030-99277-4_21.

[9] Jorge Chavez-Saab, Maria Corte-Real Santos, Luca De Feo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign algorithm specifications and supporting documentation. Project Homepage, 2023. URL `https://sqisign.org/spec/sqisign-20230601.pdf`.

[10] Peter Chvojka and Tibor Jager. Simple, fast, efficient, and tightly-secure non-malleable non-interactive timed commitments. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *Public-Key Cryptography – PKC 2023*, pages 500–529, Cham, 2023. Springer Nature Switzerland. doi: 10.1007/978-3-031-31368-4_18.

[11] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 248–277, Cham, 2019. Springer International Publishing. doi: 10.1007/978-3-030-34578-5_10.

[12] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing. doi: 10.1007/978-3-030-64837-4_3.

[13] Thomas Decru, Luciano Maino, and Antonio Sanso. Towards a quantum-resistant weak verifiable delay function. In Abdelrahaman Aly and Mehdi Tibouchi, editors, *Progress in Cryptology – LATINCRYPT 2023*, pages 149–168, Cham, 2023. Springer Nature Switzerland. doi: 10.1007/978-3-031-44469-2_8.

[14] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing. doi: 10.1007/978-3-319-78372-7_11.

[15] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. Association for Computing Machinery. doi: 10.1145/237814.237866.

[16] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular isogeny key encapsulation. Project Homepage, 2020. URL `https://sike.org/files/SIDH-spec.pdf`.

[17] Jonathan Katz, Julian Loss, and Jiayu Xu. On the security of time-lock puzzles and timed commitments. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography*, pages 390–413, Cham, 2020. Springer International Publishing. doi: 10.1007/978-3-030-64381-2_14.

[18] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS J. Comput. Math.*, 17:418–432, 2014. doi: 10.1112/S1461157014000151.

[19] Ronald L. Rivest, Adi Shamir, and David A. Wagner. Time-lock puzzles and timed-release crypto. Technical report, USA, 1996.

[20] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer New York, 1986. doi: 10.1007/978-1-4757-1920-8.

[21] Sri Aravinda Krishnan Thyagarajan, Guilhem Castagnos, Fabian Laguillaumie, and Giulio Malavolta. Efficient CCA timed commitments in class groups. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, CCS '21, page 2663–2684, New York, NY, USA, 2021. Association for Computing Machinery. doi: 10.1145/3460120.3484773.

[22] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer Cham, 2021. doi: 10.1007/978-3-030-56694-4.

[23] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2022. doi: 10.1109/FOCS52979.2021.00109.

Fast tripling on Hessian Kummer lines

Thomas Decru & Sabrina Kunzweiler

Extended abstract

Throughout the past decades, elliptic curves have become a cornerstone of cryptography in the form of ECC, but also as a viable alternative in the post-quantum era by means of isogenies connecting them. To speed up computations, various models such as the Montgomery and Edwards forms have been studied. A twisted Hessian curve $\mathcal{H}_{a,d}/k$ is a projective elliptic curve defined by the polynomial

$$aX^3 + Y^3 + Z^3 = 3dXYZ,$$

where $a(d^3 - a) \neq 0$ and $(0 : -1 : 1)$ is the neutral element. Furthermore,

$$\mathcal{H}_{a,d}[3] = \langle (1 : -\alpha : 0), (0 : -\omega : 1) \rangle,$$

where ω is a cubic root of unity and $\alpha^3 = a$. Explicit formulae to compute all 3-isogenies with domain $\mathcal{H}_{a,d}$ are well-known, but we provide an alternative point of view. For the sake of simplicity, assume an *untwisted* Hessian curve for now; i.e. $a = 1$.
It is well known that the coordinates $(X : Y : Z)$ correspond to level-3 theta functions [2]. In particular, the action by the 3-torsion points on the coordinates is normalized as

$$(X : Y : Z) + P_1 = (Y : Z : X), \quad (X : Y : Z) + P_2 = (\omega^2 X : \omega Y : Z),$$

where $P_1 = (1 : -1 : 0)$ and $P_2 = (0 : -\omega : 1)$. A similar observation in the context of level-2 theta functions, has led to a simple description of 2-isogenies by Robert [3, Section 7]. In his description, the 2-isogeny is decomposed into three operations: coordinate-wise squaring, a Hadamard transformation, and coordinate-wise scaling. We show that an analogous decomposition can be achieved for 3-isogenies in Hessian form.
Define the following operations:

- $\odot^3$: Coordinate-wise cubing; i.e. $\odot^3(X : Y : Z) = (X^3 : Y^3 : Z^3)$.
- M: Discrete Fourier transform; i.e.

$$M(X : Y : Z) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

- $C_{(\lambda,\mu)}$: Scaling; i.e. $C_{\lambda,\mu}(X:Y:Z) = (\lambda X:\mu Y:\mu Z)$.

One can then show that the map

$$\phi_1 : (X:Y:Z) \mapsto C_{(1,d')} \circ M \circ \odot^3(X:Y:Z),$$

where $(d')^3 = d^3(d^3-1)$, defines an isogeny with kernel $\langle(0:-\omega:1)\rangle$. It is unsurprising that computing a (radical) 3-isogeny requires computing a cubic root (in this case d'), but when given the information of a 9-torsion point laying above $(0:-\omega:1)$, one can furthermore show that no root need be computed. The discrete Fourier transform map M can be shown to exhibit additional interesting behaviour; e.g.

$$M(\langle(0:-\omega:1)\rangle) = \langle(-1:1:0)\rangle, \quad M(\langle(-1:1:0)\rangle) = \langle(0:-\omega:1)\rangle,$$

where equality needs to be interpreted on an isomorphic curve with a distinct parameter d. In particular, it can be seen as a nontrivial symplectic base-change on the 3-torsion of $\mathcal{H}_{a,d}$.
The strength of this interpretation is most eminent on the Hessian Kummer line. Indeed, given that negation on $\mathcal{H}_{a,d}$ is given by swapping the Y- and Z-coordinates, one can define the Hessian Kummer line $\mathcal{HK}_{a,d}$ as the codomain of the projection map

$$\pi : \mathcal{H}_{a,d} \to \mathcal{HK}_{a,d}, (X:Y:Z) \mapsto (X:U) = (X:Y+Z).$$

With slight abuse of notation, from this one can then show that for example the isogeny ϕ_1 can be interpreted on the Hessian Kummer line as

$$\phi_1 : (X:U) \mapsto (aX^3+U^3 : d(2aX^3-U^3)+3aX^2U).$$

The interpretation of our three operations from before on $\mathcal{HK}_{a,d}$ are as follows:

- $\odot^3 : (X:U) \mapsto (aX^2(U+dX) : U(dU^2-aX^2))$;
- $M : (X:U) \mapsto (X+U : 2X-U)$;
- $C_{\lambda,\mu} : (X:U) \mapsto (\lambda X : \mu U)$.

Remarkably, the (potentially expensive) multiplications by cubic roots of unity from M have completely vanished on the Kummer. One can then show that in this interpretation, it holds that the isogeny projected on the Kummer can be computed as

$$\phi_1 : (X:U) \mapsto C_{(1,d)} \circ M \circ \odot^3(X:U).$$

One can verify that the dual isogeny $\hat{\phi}_1$ also has kernel generated by $(0:-\omega:1)$, such that the multiplication-by-3 map can be expressed as applying this last formula twice since $[3] = \hat{\phi}_1 \circ \phi_1$. From this it follows that on any twisted Hessian Kummer line $\mathcal{HK}_{a,d}$, multiplication-by-3 can be evaluated in $4\mathbf{M}+4\mathbf{S}+8\mathbf{M}_{a,d}$, where $\mathbf{M}, \mathbf{S}, \mathbf{M}_{a,d}$ denote a multiplication, a squaring and a multiplication by a curve constant respectively. Given an appropriate curve (e.g. an untwisted

Hessian curve with $a = 1$ and d small such that $\mathbf{M}_d$ is closer to an addition than a multiplication), this collapses to a mere $4\mathbf{M} + 4\mathbf{S}$. The previous state-of-the-art for tripling on elliptic curves with similar appropriately-chosen curve parameters a and d was $4\mathbf{M} + 8\mathbf{S}$ in [1] (or $4\mathbf{M} + 6\mathbf{S}$ if multiplication by ω is cheap but we do not require such field restrictions). Compared to tripling on Kummer lines, the previous state-of-the-art was $5\mathbf{M} + 5\mathbf{S}$ on the Montgomery Kummer line.

References

[1] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted hessian curves. In Kristin E. Lauter and Francisco Rodríguez-Henríquez, editors, *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, volume 9230 of *Lecture Notes in Computer Science*, pages 269–294. Springer, 2015.

[2] David B Mumford. On the equations defining abelian varieties. *I. Inventiones Mathematicae*, 1(4):287–354, 1966.

[3] Damien Robert. Some notes on algorithms for abelian varieties. Cryptology ePrint Archive, Paper 2024/406, 2024.

Differential MITM attacks on SLIM and LBCIoT

Peter Grochal* Martin Stanek†

Department of Computer Science
Faculty of Mathematics, Physics and Informatics
Comenius University

1 Introduction

Lightweight cryptography addresses the problem of using cryptography in constrained environments, such as sensors, IoT devices with limited computational power, memory, battery, etc. Since conventional cryptographic algorithms are impractical in these scenarios, dedicated constructions are proposed. SLIM [1] and LBCIoT [5] are lightweight 32-bit block ciphers. The 32-bit block is divided into left and right 16-bit halves. Both ciphers use an 80-bit key to derive 32 round keys, each 16 bits long. SLIM is a Feistel cipher, and even though the round function of LBCIoT resembles a Feistel cipher, its structure is different.

We propose and analyze two improvements to a differential meet-in-the-middle (MITM) cryptanalysis [3], and apply it at SLIM and LBCIoT. Our attack at LBCIoT is the best known attack to date. Furthermore, we show problems in the analysis of differential attacks that are of independent interest. Namely, the problem of using low-probability differentials, and a problem with commonly used assumptions of filter uniformity.

2 Attacking SLIM and LBCIoT

2.1 Overview of the differential MITM attack

Let $E, D : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^n$ be the encryption and decryption functions of a block cipher with the key length l and the block size n. In the rest of the paper we assume E can be split into three consecutive transformations $E = E_{\text{out}} \circ E_{\text{m}} \circ E_{\text{in}}$. For iterated block ciphers, e.g., SLIM and LBCIoT, various splits are possible using subsequent rounds. In such case, we denote the respective numbers of rounds by r_{in}, r_{m}, and r_{out}.

A difference of two n bit vectors is a bitwise xor of these vectors. A differential $\Delta = (\alpha \to \beta)$ over E_m is a pair of input and output differences. Its probability is usually given by this formula, where k is a key for the entire cipher, with E_m using only the relevant bits:

$$\Pr[E_{\text{m}}(k,x) \oplus E_{\text{m}}(k, x \oplus \alpha) = \beta; \text{ for random } k \in \{0,1\}^l \text{ and } x \in \{0,1\}^n]. \tag{1}$$

We show in Section 3.1 that for practical application of both differential attack and differential MITM attack it is important to distinguish whether (1) is calculated for a random or fixed k.

*pegro@protonmail.com
†martin.stanek@fmph.uniba.sk

Given a differential $\Delta = (\alpha \to \beta)$, we denote by k_{in} the set of indices of key bits whose values are sufficient to compute a plaintext block $\widetilde{P}$ from any block P, such that $E_{\text{in}}(P) \oplus E_{\text{in}}(\widetilde{P}) = \alpha$. Similarly, k_{out} is the set of indices whose values are sufficient to compute $\widetilde{C}$ from any block C, such that $E_{\text{out}}^{-1}(C) \oplus E_{\text{out}}^{-1}(\widetilde{C}) = \beta$. See Figure 1 for visual representation of these concepts.

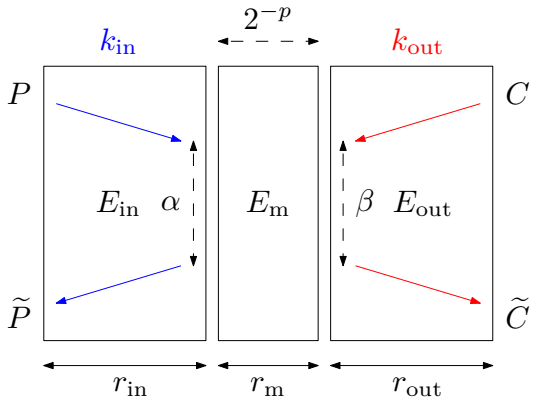

Figure 1: Splitting a cipher for differential MITM attack

The differential MITM attack is a chosen plaintext attack, recently proposed and used to attack multiple block ciphers [2, 3, 6]. The main idea of the attack is to find any pair of plaintexts P, $\widetilde{P}$, with corresponding ciphertexts C, $\widetilde{C}$, such that the differential Δ occurs for E_{m}. The successful search will reveal candidate key bits for k_{in} and k_{out}. We find such a pair P, $\widetilde{P}$ using MITM approach.

1. For a fixed random P, we guess the value i for k_{in}, and compute $\widetilde{P}$ such that the difference of P and $\widetilde{P}$ after the transformation E_{in} results in α.

2. We ask for the ciphertext C corresponding to P and ciphertext $\widehat{C}$ corresponding to $\widetilde{P}$ (using chosen plaintext oracle). We store the pair $(\widehat{C}, i)$ in a hash table, using $\widehat{C}$ as key.

3. Independently, we guess the value j for k_{out}, and compute $\widetilde{C}$ from C such that their difference after E_{out}^{-1} is β. Then, for each pair $(\widetilde{C}, i)$ found in the hash table, we get a candidate combination (i, j) for k_{in}, and k_{out}. We store this candidate in a multiset.

Since the probability of the differential Δ is 2^{-p}, we repeat the procedure $\kappa \cdot 2^p$ times with different P, so that we can expect the differential to occur κ times for the correct (i, j) values from the actual key. Generally, κ is a small constant. In our experiments $\kappa = 7$ was sufficient. There is a possibility to optimize the search if k_{in} and k_{out} overlap.

2.2 Identical bits

In the candidates (i, j), we noticed bits with the following property, the value of the bit was *identical* across all candidates with the highest multiplicity. Based on this observation, we propose the following: The attack outputs one partial candidate – the indices of identical bits, and their values. In our experiments (on SLIM and LBCIoT) almost all bits were identical.

In the rare instance when the number of candidates with the highest multiplicity is much smaller than the number of candidates satisfying the identical bits $2^{|k_{\text{in}}|+|k_{\text{out}}|-m}$ (m is the number of identical bits), then the attack should output the exact set of candidates.

If multiple differentials are known, we can repeat the attack for each differential, hopefully covering the majority of round key bits for the first r_{in} rounds and the last r_{out} rounds. The remaining few bits can be brute-forced.

2.3 Deterministic bits

The notion of *deterministic bits* allows us to detect situations when a particular differential certainly did not occur, thus making the attack faster. Deterministic bits for a differential $\Delta = (\alpha \to \beta)$ and E_{out} are a subset of bits in a ciphertext block whose difference is constant, provided that the difference before E_{out} is β.

We use the deterministic bits as a filter, to detect incorrect P or guesses of k_{in}. In our experiments, we could often skip the third step, as there was no valid pair $(\widehat{C}, i)$ stored in the hash table. The hash table was nonempty less than once every 2^{10}-th random plaintext P.

2.4 Attacks

We denote by $\text{DM}(r_{\text{in}}, r_{\text{m}}, r_{\text{out}})$ the differential MITM attack on $(r_{\text{in}} + r_{\text{m}} + r_{\text{out}})$-round cipher split into r_{in}-round E_{in}, r_{m}-round E_{m}, and r_{out}-round E_{out}. We have applied our attacks at SLIM and LBCIoT. The attack on LBCIoT is the best known attack to this date.

						bits recovered	
cipher	rounds	attack	$\mathcal{T}$	$\mathcal{S}$	$\mathcal{D}$	$\lvert k_{\text{in}}\rvert$	$\lvert k_{\text{out}}\rvert$
SLIM	14*	differential [4]	2^{32}	2^{12}	2^{32}	-	12
	16	$\text{DM}(3, 11, 2)$	$\kappa \cdot 2^{71}$	$\kappa \cdot 2^{65}$	2^{32}	45	26
	18*	$\text{DM}(3, 13, 2)$	$\kappa \cdot 2^{73}$	$\kappa \cdot 2^{67}$	2^{32}	42	26
	19	linear [7]	$2^{64.4}$	2^{38}	2^{32}	-	36
LBCIoT	19	differential [4]	2^{32}	2^{3}	2^{31}	does not work†	
	25	$\text{DM}(4, 17, 4)$	$\kappa \cdot 2^{71}$	$\kappa \cdot 2^{71}$	2^{32}	37	38
	26*	$\text{DM}(4, 18, 4)$	$\kappa \cdot 2^{67}$	$\kappa \cdot 2^{65}$	2^{32}	37	30

(*) The attack fails for a substantial portion of keys, see Section 3.1.

(†) The published version of the attack fails. But it can be tweaked to be correct.

Table 1: Selected attacks on reduced versions of SLIM of LBCIoT

3 Problems in analyzing cryptographic attacks

3.1 Low-probability differentials

SLIM and LBCIoT were analyzed in [4] using differential cryptanalysis. We use the differentials found by the authors of [4]. We have experimentally verified the probabilities of these differentials (according to the equation (1)).

The probability of differential, as defined in (1), does not guarantee the desired property for each fixed key we aim to reconstruct in the classical differential and differential MITM

attacks. This is an issue, especially for differentials with probabilities close to 2^{-n}, where a selection of plaintexts is not independent, since almost the entire plaintext space is exhausted.

We illustrate this problem on SLIM and LBCIoT, where the authors of [4] employ differentials with probability close to 2^{-n} (2^{-32}). We performed a simple experiment where a random key is tested on the entire plaintext space to find out, whether the desired differential occurs at least once. The results presented in Table 2 show that for a substantial portion of 10 000 keys we tested, the output difference was never observed. For such keys, the classical differential cryptanalysis and the differential MITM cryptanalysis can never succeed.

	r	α	β	2^p	% of keys
SLIM	11	`4827 0080`	`0020 08b4`	2^{-26}	0%
	12	`0b82 000a`	`0a00 801b`	2^{-28}	30.06%
	13	`a208 a000`	`a000 b208`	2^{-31}	40.61%
LBCIoT	16	`0006 0400`	`0020 1000`	2^{-26}	0%
	17	`0006 0400`	`0100 2040`	2^{-28}	0.01%
	18	`6000 0040`	`0000 0800`	2^{-30}	5.95%

Table 2: Percentage of tested keys for which the differential never occurs in SLIM and LBCIoT

3.2 Problems with l-bit filters

In our experiments, we have noticed that the standard and commonly used assumptions of filter uniformity do not hold for small attacks, even by several orders of magnitude (depending on the cipher and the filter size). This affects the overall complexity estimates for these attacks as well. It remains an open problem whether the estimates hold for more rounds.

More specifically, the time and space complexities of this attack depend on the expected number of candidates found, and this number is, according to [2, 3, 6]: $\kappa \cdot 2^p \cdot 2^{|k_{\text{in}}|+|k_{\text{out}}|-n}$ for some constant κ. The papers get to these estimates by taking the maximal possible number of candidates $2^{|k_{\text{in}}|+|k_{\text{out}}|}$, and reducing them by the application of an n-bit filter by the factor 2^n. Specifically, "after matching through the relation $\widehat{C} = \widetilde{C}$", i.e. matching on n bits. Table 3 shows the theoretical, expected number of candidates and the actual number of candidates found by the differential MITM attack for comparison.

cipher	rounds	attack	total	expected
SLIM	8	DM(1, 6, 1)	119	$\kappa \cdot 2^{-1}$
	8	DM(2, 4, 2)	9 102 387	458 752
	10	DM(1, 8, 1)	166	56
LBCIoT	12	DM(2, 8, 2)	22	$\kappa \cdot 2^{-16}$
	14	DM(2, 10, 2)	40	$\kappa \cdot 2^{-9}$
	18	DM(2, 14, 2)	72	$\kappa \cdot 2^{0}$

Table 3: Number of candidates (experiments with $\kappa = 7$)

References

[1] Bassam Aboushosha et al. *SLIM: A Lightweight Block Cipher for Internet of Health Things*. In: *IEEE Access* 8 (2020), pp. 203747–203757. DOI: 10.1109/ACCESS.2020.3036589.

[2] Zahra Ahmadian et al. *Improved Differential Meet-in-the-Middle Cryptanalysis*. In: *Advances in Cryptology – EUROCRYPT 2024*. Springer, 2024, pp. 280–309. ISBN: 978-3-031-58716-0. DOI: 10.1007/978-3-031-58716-0_10.

[3] Christina Boura et al. *Differential Meet-In-The-Middle Cryptanalysis*. In: *Advances in Cryptology – CRYPTO 2023*. Springer, 2023, pp. 240–272. ISBN: 978-3-031-38548-3. DOI: 10.1007/978-3-031-38548-3_9.

[4] Yen Yee Chan et al. *On the resistance of new lightweight block ciphers against differential cryptanalysis*. In: *Heliyon* 9.4 (2023). ISSN: 2405-8440. DOI: 10.1016/j.heliyon.2023.e15257.

[5] Rabie A. Ramadan et al. *LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices*. In: *Computers, Materials & Continua* 67.3 (2021), pp. 3563–3579. ISSN: 1546-2226. DOI: 10.32604/cmc.2021.015519.

[6] Ling Song, Qianqian Yang, and Huimin Liu. *Revisiting the Differential Meet-In-The-Middle Cryptanalysis*. Cryptology ePrint Archive, Paper 2023/1302. 2023. URL: https://eprint.iacr.org/2023/1302.

[7] Nobuyuki Sugio. *Bit-Based Evaluation of Lightweight Block Ciphers SLIM, LBC-IoT, and SLA by Mixed Integer Linear Programming*. In: *IET Information Security* 2024.1 (2024), p. 1741613. DOI: 10.1049/2024/1741613.

A new approach to evolution of bijective S-boxes with AI based swap predictions (Extended abstract)

Terezia Gurbalova Pavol Zajac *

Slovak University of Technology in Bratislava, Slovakia

Evolution of S-boxes

In this article, the term n-bit S-box will denote any bijective vectorial Boolean function, $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Let $\mathcal{S}_n$ denote a set of all n-bit S-boxes.

In cryptographic applications, we require that S-boxes have some specific qualities, such as low differential uniformity and high non-linearity [1]. In general, let $\nu : \mathcal{S}_n \to \mathbb{R}$ denote some function that measures the relative quality of an S-box. We say that S-box S_1 has higher quality than S-box S_2 if $\nu(S_1) > \nu(S_2)$. We say that S-box $S_1 \in \mathcal{S}_n$ is optimal (in $\mathcal{S}_n$) if for any S-box $S_2 \in \mathcal{S}_n$, $\nu(S_2) \leq \nu(S_1)$.

An S-box evolution is a sequence of S-boxes $S_1, S_2, \ldots, S_m$ given by some function $f : \mathcal{S}_n \to \mathcal{S}_n$, such that $S_{i+1} = f(S_i)$ with the property that $\nu(S_i) < \nu(S_j)$ for all $1 \leq i < j \leq m$. An optimal function f is defined in such a way, that S_m is optimal for each starting S_1.

Intuitively, some optimal function f must exists for every n and ν, but it is not known how to construct it efficiently. Instead, we want to study the opposite approach: define some efficient function f, and observe the properties of S-boxes obtained by evolution (using function f) of randomly selected starting S-boxes.

Let $\tau_{i,j}$ denote a swap operation performed on an S-box vector of values. That is, let $\tau_{i,j}(S_1) = S_2$. Then $S_1(i) = S_2(j)$, $S_1(j) = S_2(i)$, and $S_1(x) = S_2(x)$ for each $x \notin \{i, j\}$. We say that swap operation $\tau_{i,j}$ improves S-box S_1, if and only if $\nu(S_1) < \nu(\tau_{i,j}(S_1))$.

Given starting S-box S_1, we can generate any other S-box S_2 with a sequence of swap operations of length at most 2^n (the length of the vector of values of S_1), even the optimal ones. Unfortunately, such a sequence of swaps is not necessarily evolution sequence (according to our definition), as some swaps along the way might reduce the score given by ν (to later produce an even better score).

Our object of study in this contribution is an evolution sequence given by a series of swaps. Our aim is to find a predictor for a suitable swap operation that improves of the S-box. Given S-box S, predictor π should output two integers i, j that define swap operation $\tau_{i,j}$. Predictor π is successful, if the score of the new S-box improves, that is $\nu(\tau_{\pi(S)}(S)) > \nu(S)$. Predictor π should have better success rate than using randomly generated swaps, and should not require evaluation of ν for other S-boxes (except for the comparison of the new S-box with the previous score).

Predictor with the best success rate leads to an optimal evolution algorithm for improving S-boxes with swaps from a random starting point (as any other algorithm would require to assess more S-boxes along the way).

Predicting evolution steps with AI

Our goal is to create black-box oracle for π that for given S-box S returns some swap τ, such that $\tau(S)$ has better quality than S with higher probability p than a random guess (probability p_r). Quality of the oracle is measured by the increase in probability, $p - p_r$.

*This work was in part supported by the Slovak Research and Development Agency under the Contract no. APVV-23-0292, and in part by grant VEGA 1/0105/23.

The input S-box will be represented by its vector of values, which is sequence of all 2^n (non-repeating) values from $\mathbb{F}_2^n$. The output of the oracle is a tuple of values $i, j \in \mathbb{F}_2^n$. These are the inputs of the S-box, corresponding to positions of values that need to be swapped.

Our approach general approach to this problem is as follows:

- Prepare a (large) dataset of positive examples $(S, i, j) \in \mathcal{S} \times \mathbb{F}_2^n \times \mathbb{F}_2^n$. S-boxes in the dataset are chosen randomly. An exhaustive (or random) search of pairs (i, j) is performed for each S-box. The dataset contains only those pairs that improved quality of the S-box. We use simple function ν that only uses the differential properties of the S-box.

  Let d_i denote maximum value in DDT of S-box S_i, and let c_i denote the number of times d_i is present in the DDT of S_i. Then $\nu(S_i) > \nu(S_j)$ if $d_i < d_j$, or if $d_i = d_j$, and $c_i < c_j$. We have not explored different scoring functions, such as proposed in [2]. The utility of a more complex scoring function in our use case is questionable, as the main idea is to train on a dataset of examples of S-box improving swaps. Our (untested) hypothesis is that the method should be agnostic to the exact details of the scoring function.

- Train a neural network (with some specific architecture) to work in a Seq2Seq mode using the provided dataset (some part of it). The input sentence for translation is S-box S, the output sequence is the pair (i, j).

- Use the trained neural network as a predictor π, and evaluate its quality (using a validation dataset of S-boxes).

Experimental results

In our experiments we focus on two categories of S-boxes: small S-boxes with $n = 4$, and large S-boxes with $n = 8$. We have prepared two corresponding datasets of $N = 20000$ S-boxes each. In order to obtain S-boxes with higher quality, we have iterated a greedy algorithm starting from a random S-box, and stored unique S-boxes and corresponding swaps that improve differential properties (differential uniformity, as well as number of DDT elements with maximal value was taken into account).

In the experiments, both S-boxes and swaps are represented as one-hot encoded vectors (essentially, an S-box is stored as a permutation matrix, and similarly the swap positions). We trained two different neural network architectures on the data from the dataset, with the goal of predicting a suitable swap that improves the differential profile of the input S-box

Sequence-to-Sequence LSTM Model

The first approach is based on a reccurent neural network architecture known as Long short-term memory (LSTM). We use LSTM architecture suitable for Sequence-to-Sequence task: the input sequence is the one-hot encoded vector of values of the S-box, and the output sequence is the (potentially) suitable swap (sequence of length two). Technically, the architecture transforms the input S-box into an internal representation through LSTM layers, and then a final *Dense* layer generates output that contains two vectors of length 256 (in general 2^n, for n-bit S-boxes) that each correspond to one value of the swap. Each vector contains scores assigned for all possible 2^n values (corresponding to the likelihood that the value at this position should be swapped). To select the swap, we use the pair with the highest score each.

CNN-Based Model

The second approach uses a more simple convolution neural network architecture. The input first passes through a *Conv2D* layer, followed by a *MaxPooling2D* layer, which reduces dimensionality by selecting the most relevant features. This process is repeated three times, with the *Conv2D* layers progressively increasing in filter size: 32, 64, and finally 128 filters. The output is flattened into a one-dimensional vector using the *Flatten* layer. Output from that layer is then passed trough *Dense* layer with activation function *ReLU*. Followed by another *Desne* layer with output size of two times 256 (2^n in general), and a softmax activation function generates the final swap prediction, similar to LSTM case.

Results

We have performed a series of experiments with various LSTM and CNN settings with both 4-bit and 8-bit S-boxes on our dataset. In Table 1 we summarize the main results of the experiments. In the first row, we give a probability (and standard deviation) that random swap improves S-boxes from a validation set (random subset of the dataset). In the next two rows we present the results of the swaps obtained with the best setting in each case (LSTM vs. CNN).

Method	4×4	8×8
random	34.65 ± 0.87 %	19.96 ± 0.55 %
LSTM	36.60 %	23.96 %
convolution	35.40 %	21.29 %

Table 1: Results of the experiments with 2 architectures, compared to random selection.

If we use normal distribution to model the success rate of the random selection, the probabilities for $n = 4$ are two low in both LSTM and CNN case to be considered sufficiently better than random. Similarly, in case $n = 8$, convolution network does not produce a significant result. On the other hand, our LSTM results are more the 7σ better than the random case, which indicates that the model was able to learn some information from the input dataset, and produces better predictions than random guesses.

Using our neural predictor, we might improve the (heuristic) search for better quality S-boxes (such as in [3]). While on average, we need to explore 5 random swaps to get an improvement (in every iteration of the search), neural predictor reduces this to only 4 swaps. Moreover, the neural predictor produces a distribution of scores for each potential swap, thus it might be even more efficient in practice. Note that these results were obtained with only limited resources, and with larger datasets and more resources these results have a potential to improve further.

An open question is whether similar results can be also obtained for non-linearity measures, and for a combination of multiple S-box quality criteria. Furthermore, in our experimental dataset, the input S-boxes have different qualities. It would be interesting to see how the quality of the input S-box influences the prediction quality. This type of experiment would however require a large dataset of high-quality S-boxes (that can be improved further). From the cryptographic research point of view, it is an interesting theoretical question, why the black-box prediction works, and whether we can reproduce these black-box results with proper (mathematical) algorithms.

References

[1] Carlet, C., Crama, Y., and Hammer, P. L. Vectorial boolean functions for cryptography., 2010.

[2] Picek, S., Cupic, M., and Rotim, L. A new cost function for evolution of s-boxes. *Evolutionary Computation 24*, 4 (12 2016), 695–718.

[3] Zajac, P. Improving differential properties of s-boxes with local changes of DDT. In *Boolean Functions and Applications* (2023).

The power of three in pseudorandomness

Katalin Gyarmati and Károly Müllner

Extended abstract

In 1997, Mauduit and Sárközy introduced the following quantitative measures in order to study the pseudorandomness of finite binary sequences.

Definition 1. *For a binary sequence*

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N,$$

define the well-distribution measure of E_N *as*

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|,$$

where the maximum is taken over all a, b, t *such that* $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ *and* $1 \le a \le a+tb \le N$, *while the correlation measure of order* ℓ *of* E_N *is defined as*

$$C_\ell(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, \dots, d_\ell)$ *and* M *such that* $0 \le d_1 < \dots < d_\ell < M + d_\ell \le N$.

These measures characterize the necessary random properties of binary sequences in various applications (such as cryptography, Monte Carlo methods, and many others). It's also crucial to have strong pseudorandom constructions for which these measures are provably small. According to papers by Cassaigne, Mauduit, Sárközy [2] and later Alon Kohajakawa Maduit,

Moreira, and Rödl [1], the pseudorandomness of a sequence E_n is considered to be very strong if

$$W(E_N) \ll N^{1/2}(\log N)^c,$$
$$C_\ell(E_N) \ll N^{1/2}(\log N)^{c_\ell}$$

hold at least for small ℓ's. In the literature, there are numerous constructions with strong pseudorandomness properties (e.g., see [3], [5], [4], [6], [7], [8], [9], [10], [12], [13], [14], [15]). However, the most natural and strongest construction to date is the following:

Construction 2 (Hoffstein, Liemann)**.** *Let p be a prime and $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree k. Define $E_p = (e_1, \dots, e_p)$ by:*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1, \\ +1 & \text{for } p \mid f(n). \end{cases}$$

This construction was introduced by Hoffstein and Leimann, but nothing has been proven about the pseudorandom properties of the sequences. One year later, Goubin, Mauduit and Sárközy proved the following:

Theorem A [Goubin, Mauduit, Sárközy] *Let p be a prime and $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree k, which is not of the form $cg(x)^2$, where $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$. Define $E_p = (e_1, \dots, e_p)$ by Construction 2. Then*

$$W(E_p) \ll kp^{1/2} \log p.$$

Assume that one of the following three conditions for ℓ, which is the order of the correlation, holds true:
(i) $\ell = 2$;
(ii) $\ell < p$ and 2 is a primitive root modulo p;
(iii) $(4k)^\ell < p$.
Then

$$C_\ell(E_p) \ll k\ell p^{1/2} \log p.$$

Although, Construction 2 has strong pseudorandom properties, it is conceivable that an algorithm might be found in the future which determines the value of the polynomial f from knowing p^{ε} consecutive elements of the sequence E_p (if the degree of the polynomial is under a certain bound). In this case, the entire sequence (e.g., used as the secret key) might be determined from a few elements of the sequence. This can be facilitated by an idea that only slightly modifies the above sequence using not one but three different polynomials. For this, we introduce the following construction:

Construction 3. *Let p be a prime and $f(x), g(x), h(x) \in \mathbb{F}_p[x]$ be a polynomials of degree $\leq k$. Define $E_{f,g,h} = (e_1, \dots, e_p)$ by:*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{if } \left(\frac{h(n)}{p}\right) \in \{0,1\} \text{ and } p \nmid f(n)g(n) \\ \left(\frac{g(n)}{p}\right), & \text{if } \left(\frac{h(n)}{p}\right) = -1 \text{ and } p \nmid f(n)g(n) \\ 1, & \text{if } p \mid f(n)g(n). \end{cases}$$

Note that if $f = g$, then this construction coincides with Construction 2.

In this construction, if $p \nmid f(n)g(n)h(n)$, then the following formula can be proved:

$$e_n = \frac{1}{2}\left(1 + \left(\frac{h(n)}{p}\right)\right)\left(\frac{f(n)}{p}\right) + \frac{1}{2}\left(1 - \left(\frac{h(n)}{p}\right)\right)\left(\frac{g(n)}{p}\right). \qquad (1)$$

From this formula we will prove the following using multiplicative character techniques (e.g., Weil theorem):

Theorem 4. *Let p be a prime and $f(x), g(x), h(x) \in \mathbb{F}_p[x]$ be three polynomials of degree k, that have no multiple roots; and*

$$f(x) \nmid \prod_{t=1}^{p} g(x+t)h(x+t) \quad \text{and} \quad g(x) \nmid \prod_{t=1}^{p} h(x+t). \qquad (2)$$

Define $E_{f,g,h} = (e_1, \dots, e_p)$ by Construction 3. Then

$$W(E_{f,g,h}) \ll kp^{1/2} \log p.$$

Assume that one of the following three conditions for ℓ, which is the order of the correlation, holds:

(i) $\ell = 2$*;*
(ii) $\ell < p$ *and 2 is a primitive root modulo* p*;*
(iii) $(4k)^\ell < p$*.*
Then

$$C_\ell(E_{f,g,h}) \ll 2^\ell \ell k p^{1/2} \log p.$$

For symmetric reasons, the theorem holds even if (2) is replaced by $g(x) \nmid \prod_{t=1}^{p} f(x+t)h(x+t)$, $f(x) \nmid \prod_{t=1}^{p} h(x+t)$.

Thus, even though Construction 3 is slightly more complicated, we still have strong bounds for the pseudorandom measures.

At first glance, checking condition (2) may be unpleasant, but it does not require much computation for small primes p using polynomial divison. There are several ways to avoid this polynomial division, one of which is to use only irreducible polynomials. Another possibility is that f, g and h are all products of second degree irreducible polynomials. We will prove the following

Theorem 5. *Let* p *be prime, and* F*,* G*,* H *be sets containing only quadratic non-residues modulo* p *for which*

$$F \not\subseteq G \cup H \quad \text{and} \quad G \not\subseteq H.$$

The polynomials f*,* g*, and* h *are defined as follows.*

$$f(x) = \prod_{n \in F}(x^2 - n), \;\; g(x) = \prod_{n \in G}(x^2 - n), \;\; h(x) = \prod_{n \in H}(x^2 - n).$$

Define $E_{f,g,h} = (e_1, \ldots, e_p)$ *by Construction 3. Then,*

$$W(E_{f,g,h}) \ll k p^{1/2} \log p$$
$$C_\ell(E_{f,g,h}) \ll 2^\ell \ell k p^{1/2} \log p.$$

It is also clear that condition (2) cannot be completely dropped from Theorem 4. This is because, if, for example $f(x)g(x)h(x)$ is a square of a polynomial, then the elements of the sequence $E_{f,g,h}$ are all 1, with a few exceptions, according to (1). The strength of Construction 3 will also be supported by numerical calculations, and we will compare pseudorandom measures of some sequences in Constructions 1 and 2.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. Lond. Math. Soc. 95(3) (2007), 778-812.

[2] J. Cassaigne, C. Mauduit, and A. Sárközy *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. 103 (2) (2001), 97-118.

[3] Z.-X. Chen, *Elliptic curve analogue of Legendre sequences*, Monatsh. Math. 154 (2008), 1-10.

[4] Z. Chen, S. Li, and G. Xiao, *Construction of pseudorandom binary sequences from elliptic curves by using the discrete logarithms*, in: Sequences and their applications - SETA 2006, LNCS 4086, Springer, 2006; pp. 285-294.

[5] Z. Chen, A. Ostafe, and A. Winterhof, *Structure of pseudorandom numbers derived from Fermat quotients*, Lecture Notes in Comput. Sci., 6087, Springer, Berlin, 2010, Arithmetic of finite fields, 73-85.

[6] K. Gyarmati, A. Pethő, and A. Sárközy, *On linear recursion and pseudorandomness* (English) Zbl 1081.11055 Acta Arith. 118(4) (2005), 359-374.

[7] H. Liu, *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. 125 (2006), 11-19.

[8] H. Liu, *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, Acta Arith. 130 (2007), 167-180.

[9] S. Louboutin, J. Rivat and A. Sárközy, *On a problem of D. H. Lehmer*, Proc. Amer. Math. Soc. 135 (2007), 969-975.

[10] C. Mauduit, J. Rivat and A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. 141 (2004), 197-208.

[11] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences, I. Measures of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (4) (1997), 365-377.

[12] L. Mérai, *A construction of pseudorandom binary sequences using both additive and multiplicative characters*, Acta Arith. 139 (2009), 241-252.

[13] L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), 35-49.

[14] L. Mérai, *Construction of large families of pseudorandom binary sequences*, Ramanujan J. 18 (2009), 341-349.

[15] J. Rivat and A. Sárközy, *Modular constructions of pseudorandom binary sequences with composite moduli*, Period. Math. Hungar. 51 (2005), 75-107.

On the measures of pseudorandomness of binary lattices

Károly Müllner

Extended Abstract

Pseudorandom binary lattices play a central role in various applications where multidimensional randomness is needed. In this paper, we propose and analyze a simple construction method based on two short binary sequences. The study of pseudorandomness in higher dimensions is a natural extension of classical one-dimensional sequence analysis. We will also examine a couple of cases in 3 dimensions.

In 1997, Mauduit and Sárközy [8] introduced a new constructive approach in order to study the pseudorandomness of binary sequences

$$E_N = \{e_1, \dots, e_N\} \in \{-1, 1\}^N. \tag{0.1}$$

In particular, in [12], Mauduit and Sárközy first introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|, \tag{0.2}$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N$, and the *correlation measure* of order k of E_N is defined as

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \dots, d_k)$ and M such that $0 \le d_1 < d_2 < \cdots < d_k \le N - M$. They also introduced the *combined* (well-distribution-correlation) *pseudorandom measure* of order k:

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} \cdots e_{a+jb+d_k} \right|, \tag{0.3}$$

where the maximum is taken over all a, b, t, and $D = (d_1, d_2, \ldots, d_k)$ such that all the subscripts $a + jb + d_i$ belong to $\{1, 2, \ldots, N\}$. The sequence E_N is considered to be a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ are small in terms of N.

In order to study the multidimensional analog of pseudorandomness, Hubert, Mauduit, and Sárközy [7] introduced the following definitions and notations:

Denote by I_N^n the set of n-dimensional vectors whose coordinates are integers between 0 and $N-1$:

$$I_N^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_1, \ldots, x_n \in \{0, 1, \ldots, N-1\}\}.$$

This set is called an n-dimensional N-lattice or, briefly, an N-lattice.

In [7], the definition of binary sequences is extended to more dimensions by considering functions of type

$$\eta(\mathbf{x}) : I_N^n \to \{-1, +1\}.$$

If $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, x_2, \ldots, x_n))$ then we will slightly simplify the notation by writing $\eta(\mathbf{x}) = \eta(x_1, x_2, \ldots, x_n)$.

Such a function can be visualized as the lattice points of the N-lattice replaced by the two symbols $+$ and $-$; thus, they are called binary N-lattices. Binary 2- or 3 dimensional pseudorandom lattices also have many applications, e.g., in the encryption of digital images or maps.

The definition of I_N^n is extended to more general lattices in the following way: Let $\mathbf{u_1}, \mathbf{u_2}, \ldots \mathbf{u_n}$ be n linearly independent vectors, where the i-th coordinate of $\mathbf{u_i}$ is non-zero, and the other coordinates of $\mathbf{u_i}$ are 0, so $\mathbf{u_i}$ is of the form $(0, 0, \ldots, 0, z_i, 0, \ldots, 0)$. Let $t_1, t_2, \ldots, t_n$ be integers with $0 \leq t_1, t_2, \ldots, t_n < N$. Then we will call the set

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + x_2\mathbf{u_2} + \cdots + x_n\mathbf{u_n} : 0 \leq x_i|\mathbf{u_i}| \leq t_i (< N) \text{ for } i = 1, 2, \ldots, n\}$$

an n-dimensional box N-lattice or, briefly, a box N-lattice.

In [7], Hubert, Mauduit and Sárközy introduced the following pseudorandom measure of binary lattices:

Definition 1. *Let*

$$\eta : I_N^n \to \{-1, +1\}.$$

The pseudorandom measure of order ℓ of η is defined by

$$Q_\ell(\eta) = \max_{B, d_1, \ldots, d_\ell} \left| \sum_{x \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell \in I_N^n$ *and all box* N*-lattices* B *such that* $B + \mathbf{d_1}, \ldots, B + \mathbf{d}_\ell \subseteq I_N^n$.

Then, η is said to have strong pseudorandom properties, or, briefly, it is considered a good pseudorandom lattice if the measure $Q_\ell(\eta)$ is small (much smaller than the trivial upper bound N^n) for fixed n and ℓ and large N. This terminology is justified by the fact that, as was proved in [7], for a truly random binary lattice defined on I_N^n and for fixed ℓ, the measure $Q_\ell(\eta)$ is small (less than $N^{n/2}$ multiplied by a logarithmic factor).

So far, numerous pseudorandom lattices have been generated with optimal pseudorandom measures, see e.g., [2], [3], [5], [7], [9], [10], [11], and [6].

For almost all constructions of pseudorandom binary lattices with strong pseudorandom properties the generation of the elements of the lattice is quite slow. However, in certain applications, we need to generate the elements of the lattice quickly. In these cases, we recommend the following algorithm: Let $E = (e_1, e_2, \ldots, e_N)$ and $F = (f_1, f_2, \ldots, f_N) \in \{-1, +1\}^N$ be two pseudorandom binary sequences with strong pseudorandom properties; then, we define the binary lattice $\eta = \eta_{E\times F} : I_N^2 \to \{-1, 1\}$ by

$$\eta(x, y) = e_{x+1} f_{y+1}$$

The main results concern the estimation of pseudorandomness measures of binary lattices derived from two sequences. We approximate the lattice pseudorandomness measures using combined measures of the base sequences. The results distinguishes between even and odd cases: In the odd case, the combined measure factorizes, while in the even case, a nontrivial lower bound is obtained. These differences highlight the fundamental asymmetry between the two cases.

Then, the elements of the lattice can be generated rapidly since each element can be obtained by a simple multiplication, where the multiplicands are all 1 or -1. The question is, how large are the pseudorandom measures of the lattice? I can determine the exact values of Q_2 and Q_{2k+1} of the lattice, but unfortunately, the value of Q_{2k} is always large if $k \geq 2$:

Theorem 1. *Let* $E \in \{-1, +1\}^N$ *and* $F \in \{-1, +1\}^N$ *be pseudorandom binary sequences. Then,*

$$Q_{2\ell+1}(\eta_{E\times F}) = \\ \max\{Q_1(E), Q_3(E), \ldots, Q_{2\ell+1}(E)\} \max\{Q_1(F), Q_3(F), \ldots, Q_{2\ell+1}(F)\}$$

Theorem 2. *Let* $E \in \{-1, +1\}^N$ *and* $F \in \{-1, +1\}^N$ *be pseudorandom*

binary sequences. Then,

$$Q_2(\eta_{E\times F}) = \max\{NQ_2(E), NQ_2(F)\}$$

Theorem 3. *Let $E \in \{-1,+1\}^N$ and $F \in \{-1,+1\}^N$ be pseudorandom binary sequences and $\ell \geq 2$. Then,*

$$Q_{2\ell}(\eta_{E\times F}) \geq (N-\ell+1)^2$$

This generation method is viable when we want to use the lattices in applications where it is sufficient that the measures Q_1, Q_2, and Q_3 are small (e.g., Monte Carlo methods). If we still need Q_4 to be small (e.g., in encryptions), we need to look for another method.

Note also that Gyarmati [1] generated a sequence of length N^2 from the lattice $\eta : I_N^2 \to \{-1,+1\}$, by writing the rows of the lattice consecutively from the bottom up to the top. She proved that if, for the lattice $\eta : I_n^2 \to \{-1,+1\}$, Q_k is small, then the resulting sequence of length N^2 has a small C_k measure. By incorporating this method into our previous construction, we can generate a lattice from two sequences E and $F \in \{-1,+1\}^N$, and then a sequence of length N^2, by writing the rows of the lattice consecutively in sequence from the bottom up to the top. Then, the resulting sequence of length N^2 has small pseudorandom measures W, C_2, and C_3 if the measures $Q_2(E), Q_2(F), Q_3(E)$, and $Q_3(F)$ of the original sequences of length N are small. With this technique, we obtained a much longer sequence (length N^2) from two short sequences (length N), such that the low-order pseudorandomness measures W, C_2, and C_3 are close to optimal.

References

[1] K. Gyarmati, *On the correlation of subsequences* Unif. Distrib. Theory 7 (2012), 181-197.

[2] K. Gyarmati, C. Mauduit, A. Sárközy *On finite pseudorandom binary lattices* Discrete Appl. Math. 216(3) (2017), 589-597.

[3] K. Gyarmati, A. Sárközy, C.L. Stewart *On Legendre symbol lattices*Unif. Distrib. Theory 4(1) (2009), 81-95.

[4] K. Gyarmati, *Measures of pseudorandomness* Radon Ser. Comput. Appl. Math. 11 (2013), 43-64.

[5] K. Gyarmati, C. Mauduit, A. Sárközy *Pseudorandom binary sequences and lattices* Acta Arith. 135 (2008), 181-197.

[6] R. Hofer, L. Mérai, A. Winterhof, *Measures of pseudorandomness: Arithmetic autocorrelation and correlation measure*, In: C. Elsholtz, P. Grabner (Eds.), Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday.: Springer, 303-312, Springer, Cham, 2017

[7] P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51-62.

[8] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequence I: Measure of pseudorandomness, the Legendre symbole*, Acta Arith. 82(1997), 365-377

[9] L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), no. 1, 35-49.

[10] L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. 139(2) (2011), 407-420.

[11] L. Mérai, J. Rivat, A. Sárközy, *The measures of pseudorandomness and the NIST tests*, Lecture Notes in Comput. Sci., 10737, Springer, Cham, 2018, 197-216.

[12] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377-384.

Provably secure authenticated anonymous batch messaging for VANETs

Andrea Huszti Tamás Girászi Norbert Oláh

May 19, 2025

1 Introduction

A Vehicle Ad Hoc Network (VANET) is a system that enables communication among vehicles (V2V) and between vehicles and infrastructure (V2I) within a range of approximately 100 to 300 meters. Its primary goals are to enhance road safety and optimize traffic. Ensuring more secure communication among VANET entities is vital. These networks are vulnerable to numerous attacks, such as spoofing, tampering, and replay, all of which compromise the system's reliability. ([9]). For example, if a malicious vehicle transmits false traffic information, it could cause congestion or even life-threatening scenarios.

An essential requirement is the validation of incident reports while simultaneously protecting the driver's private data and preserving the anonymity of the message sender ([7]). A widely adopted approach to achieving sender anonymity involves the use of pseudonyms ([1], [8]). Typically, vehicles obtain short-lived anonymous certificates, referred to as pseudonyms, from a trusted authority (TA), which are then used to sign and encrypt outgoing messages. However, interaction with trusted authorities (TA) causes computational overhead, especially for high-speed vehicles that require frequent certificate renewals. Furthermore, the use of the same pseudonym can compromise user privacy, GPS data can expose the vehicle trajectory. To guarantee unlinkability, it is necessary for vehicles to frequently update their pseudonyms.

We propose an identity- and pseudonym-based **Authenticated Anonymous Batch Message Broadcast (AABMB)** protocol for VANETs. In the proposed model, when an incident (such as an accident or traffic jam) occurs, vehicles broadcast messages anonymously to other vehicles and the surrounding infrastructure. Receivers are able to verify the authenticity of these messages, ensuring that they are sent by eligible vehicles, i.e., registered and nonmalicious participants. In our scheme TA stores the Master Secret Key (MSK) to prevent its leakage in the event of OBU compromises. On-board units (OBUs) are capable of generating an unlimited number of pseudonyms independently, removing the need for pseudonym-exchange mechanisms. Formal security analysis is provided based on computationally infeasible problems.

Schemes	MSK stored by TA	Pseudonyms by OBU	Provably Secure
Pournaghi et al. [12]	no	no	no
Bayat et al. (2020) [4]	no	no	yes
Bayat et al. (2015) [3]	no	yes	no
Zhang et al. [18]	no	yes	no
Debiao He et al. [10]	no	yes	yes
Tzeng et al. [15]	no	yes	yes
Wang et al. [17]	yes	no	no
Bansal et al. [2]	yes	no	yes
Huszti et al. [11]	yes	yes	no
This work	yes	yes	yes

Table 1: Comparison to other schemes.

2 Preliminaries

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where q is a prime power. Given a finite cyclic group of elliptic curve points G with order n.

Definition 1. *Given $P, aP, bP \in G$ for some $a, b \in \mathbb{Z}_q^*$, compute abP. Computational DiffieHellman(CDH) is considered to be computationally infeasible.*

Shamir introduced the idea of identity-based encryption in [14]. These schemes usually are based on bilinear maps.

Definition 2. *Suppose that G_1 is an additive and G_2 is a multiplicative group of order q, where q is a large prime. A function $\hat{e} : G_1 \times G_1 \to G_2$ is considered to be an admissible bilinear map such that:*

- Bilinear*: For all $P, Q \in G_1$ and all $a, b \in \mathbb{Z}$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.*
- Non-degenerate*: The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2. Since G_1, G_2 are groups of prime order, if P is a generator of G_1 then $\hat{e}(P, P)$ is a generator of G_2.*
- Computable*: There is an efficient algorithm to compute $\hat{e}$.*

For all $P, Q, R \in G_1$, $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$ and $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$. In case of Weil and Tate pairings, G_1 is an elliptic-curve group, and G_2 is the multiplicative group of a finite field. The Decisional Bilinear Diffie-Hellman (DBDH) assumption is introduced in [6] by Boneh and Franklin.

Definition 3. *Given $P, A = aP, B = bP, C = cP \in G_1$ for some $a, b, c \in \mathbb{Z}_q^*$, moreover let be $z \in \mathbb{Z}_q^*$. The Decisional Bilinear Diffie-Hellman problem consists of constructing an algorithm to efficiently distinguish $(P, A, B, C, \hat{e}(P,P)^{abc})$ from $(P, A, B, C, \hat{e}(P,P)^{z})$.*

3 The proposed AABMB scheme

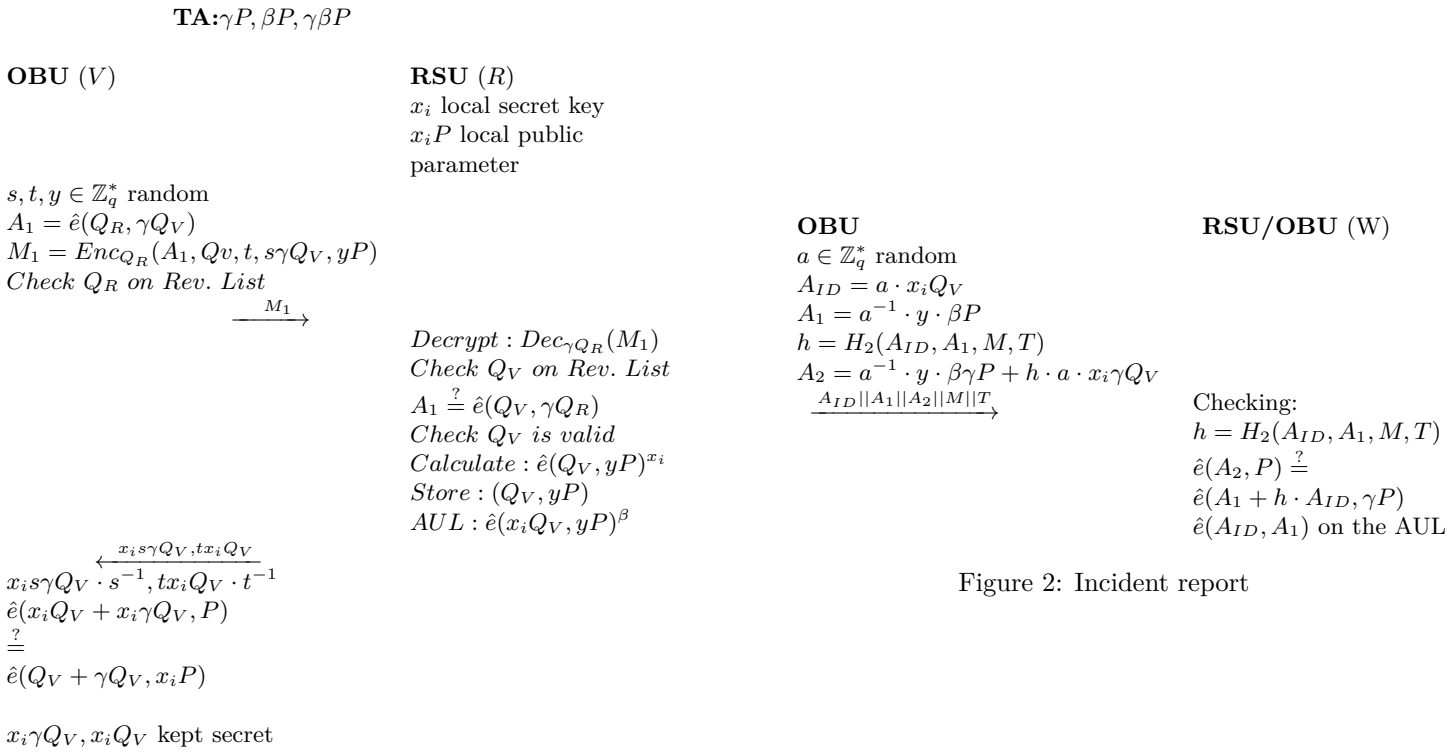

Figure 1: Communication setup

Figure 2: Incident report

3.1 Participants and lists

We differentiate three participants: the **Trusted Authority (TA)**, the **On-board Units (OBUs)**, and the **Roadside Units (RSUs)**. **Trusted Authority (TA)** is responsible for defining the system parameters, generating cryptographic keys, and managing public keys. Additionally, it loads data to OBUs online during system initialization or updates. **On-board Units (OBUs)** are devices integrated into vehicles and are equipped with a *Trusted Execution Environment (TEE)*. They report local traffic information when necessary. **Roadside Units (RSUs)** are fixed infrastructure components also equipped with a TEE. They facilitate communication with the OBUs, other RSUs, and the TA. Each RSU is responsible for authenticating OBUs that enter its communication range.

In the proposed protocol, two lists are maintained: the **Revocation List** and the **Anonymized User List**. **Revocation List** contains the identifiers of malicious users who have been excluded from the system, as well as users whose secret keys have been compromised. This list is maintained and updated by the TA whenever an anonymous user is revoked or a new key pair is issued. The revocation list is stored locally by both OBUs and RSUs. Note that, this list is not checked during the incident reporting process, thereby enhancing efficiency. **Anonymized User List** is managed by the RSUs and the TA. It allowes the system to revoke a user's anonymity if malicious behavior is detected.

3.2 Phases

The protocol consists of three phases: *Initialization*, *Communication Setup* and *Incident Report*. In the **Initialization phase**, TA generates the identity-based key pairs for the participants and initialize the system parameters, i.e. public parameters, the groups G_1, G_2, the bilinear map $e : G_1 \times G_1 \to G_2$, a generator element P of G_1, the hash functions $H_1 : \{0,1\}^* \to G_1$ and $H_2 : \{0,1\}^* \to Z_q^*$. TA randomly chooses $\gamma \in Z_q^*$, which is the master secret key, and $\beta \in Z_q^*$, a secret system parameter, and calculates public $\gamma P, \beta P, \gamma\beta P$.

The **Trusted Authority (TA)** calculates an identity-based key pair for each participant. Each vehicle receives an identity value defined as $Q_V = H_1(ID_V||T)$, where ID_V is the license plate and T is the timestamp of the corresponding key generation. RSUs also get $Q_R = H_1(ID_R||T)$ as an ID, where ID_R is its GPS coordinate. The corresponding secret keys γQ_V and γQ_R are also computed by the TA. These values serve as long-term parameters and identity-based keys used during the protocol. Furthermore, the two lists, the **Revocation List** and the **Anonymized User List**, are initialized.

The goal of the **Communication Setup** phase is to deliver authorized secret and public keys to eligible vehicles. This authorized key pair allows vehicles to communicate in a way that is both anonymous and authenticated. When a vehicle enters the domain of an RSU, the communication setup protocol is initiated between the **OBU** and the RSU.

Let the RSU be denoted by R and the vehicle by V. During Communication Setup, mutual authentication is performed between R and V, and each party checks if the corresponding identifier (Q_V or Q_R) appears in the current **Revocation List**. The missing identifier, which is based on a valid number plate IDV, means that vehicle V is eligible for message.

The RSU randomly generates a local secret key $x_i \in \mathbb{Z}_q^*$ and computes the corresponding local public key x_iP. Value x_i authorizes the OBU to report an incident in the RSUs domain after successful registration. Whenever the identity of an OBU registered within the RSUs domain is added to the **Revocation List**, the RSU generates a new x_i, and all OBUs within its domain are required to establish a new authorized secret key pair $(x_iQ_V, x_i\gamma Q_V)$. OBU chooses $s, t, y \in \mathbb{Z}_q^*$ randomly. The value s is needed to randomize γQ_V to prevent data leakage of $x_i\gamma Q_V$ and also the secret key of the OBU for the RSU.

It is also protected against active attacks, such as masquerading and replay attacks. The value t is a challenge in determining whether the RSU can correctly decrypt the encrypted message. The curve point yP represents the OBUs AUL parameter. The message M_1 is constructed using Boneh and Franklin encryption over the concatenation of Q_V, A_1, t, $s\gamma Q_V$, and yP.

Mutual authentication is based on challenge-and-response using the long-lived secret keys of the parties. The RSU verifies the validity of $A_1 = \hat{e}(\gamma Q_V, Q_R)$ by comparing it with $\hat{e}(Q_V, \gamma Q_R)$. OBU verifies $\hat{e}(x_i\gamma Q_V + x_iQ_V, P) = \hat{e}(\gamma Q_V + Q_V, x_iP)$. If these are equal, RSU decrypted the ciphertext M_1 correctly.

The TA and the RSU collaboratively compute the value $\hat{e}(Q_V, yP)^{x_i\beta}$ and insert it into the **AUL**. The TA aggregates data from multiple vehicles, permutes the resulting values, and uploads them to the AUL in a single batch. This batching and permutation process prevents the possibility of correlating the uploaded data with the OBU that registered at a specific time. Additionally, the entries on the AUL are periodically re-permuted and exponentiated with a fresh random value generated by the TA, further enhancing unlinkability and long-term privacy. Figure 1 shows in detail the steps of the phase.

In the **Incident Report** phase, a vehicle anonymously transmits messages to other OBUs and the RSU whenever an incident occurs. For each message, the sender vehicle generates a fresh pseudonym ($A_{ID} = ax_iQ_V$, $ax_i\gamma Q_V$), where $a \in \mathbb{Z}_q^*$ is chosen at random. This pseudonym serves as proof of the sender's eligibility, i.e. demonstrating that the RSU has issued an authorized key pair to the sender. The value A_2 is computed based on the incident report, a timestamp, the sender's authorized secret key, and the AUL parameter. Value A_1 is included for verification purposes. Since the format of incident reports are standardized, identical reports sent by different OBUs at the same time can be aggregated into a batch. This enables efficient verification, requiring only two bilinear map computations per batch.

Figure 2 illustrates in detail the structure of the incident report. These messages are broadcast by OBUs to all other OBUs and the RSU within the same domain. Receivers equipped with public values $(P, \gamma P)$ can verify the validity of the message received. If a malicious message is detected, it is reported, and the anonymity of the sender is revoked. The reporting entity submits A_{ID} and A_1 of the suspected malicious user to both the RSU and the TA. The TA then computes $\hat{e}(A_1, A_{ID})^{\beta^{-1}}$ with β, and applying an exhaustive search RSU finds (Q_V, yP) related to $\hat{e}(Q_V, x_iyP)$. TA inserts Q_V into the Revocation List and the fresh list is shared.

4 Security analysis

4.1 Security requirements

We focus on the requirements of the **Incident Report**, particularly the anonymity of the sender, as well as the authenticity and integrity of the transmitted message. Additionally, we address the mechanisms for anonymity revocation and the non-repudiation of malicious messages. We refer to [11], where the secrecy of these properties and the authentication of the communicating entities in the **Communication Setup** phase are formally proven using `ProVerif`. It is verified that adversaries are unable to impersonate legitimate OBUs or RSUs, and that the generated authorized secret keys remain confidential. Furthermore, it is ensured that authorized secret keys are issued exclusively to eligible participants.

Whenever an OBU reports an incident, the privacy of the vehicle owner must be protected. It is crucial that the protocol guarantees the anonymity of the reporting entities. Therefore, incident report must not leak any information that could reveal the senders identity. To achieve user anonymity, the protocol must ensure that incident reports are *unlinkable*, *i.e.*, an adversary should not be able to associate multiple messages with the same sender. Although anonymous messaging enables privacy, it also creates opportunities for authorized vehicles to behave maliciously. In cases where an OBU broadcasts an invalid or false message, the TA must be able to revoke the anonymity of the sender. Furthermore, the *non-repudiation* of incident reports must also be ensured.

In the case of VANETs, both OBUs and RSUs might become senders and receivers.

We apply the *malicious but cautious* security model, which introduced in [13]. In the context of VANETs, OBUs are typically assumed to be malicious, *i.e.*, they may deviate arbitrarily from the protocol specification. However, we consider RSUs to behave more cautiously. We adopt the model as *malicious-but-cautious* under the assumption that an RSU does not initiate any attack that would result in verifiable evidence of its misbehavior. We also assume that secret keys and system parameters remain protected from adversaries, as they are securely stored within the RSUs Trusted Execution Environment (TEE). However, the RSUs database may be compromised and leaked to the adversary.

We introduce the *existentially unforgeable under an adaptive chosen-sender attack* that is considered in the security evaluation. Loosely speaking, the adversary is able to access the polynomial number of broadcast messages, where the senders are chosen adaptively and then output new valid messages. We have decided to choose the chosen-sender attack

instead of the chosen-message attack for the following reasons. In the VANET environment, there are only a few predefined messages, hence the attacker would be limited too much if he could only intercept messages from one sender. Furthermore, the secret keys of different senders were generated with the same master key, i.e. valid messages from different senders were generated with the same secret key parameter (similar to the chosen-message attack).

Definition 4. *(adaptive chosen-sender attack)*
We define the adaptive chosen-sender attack *as follows. The adversary $\mathcal{A}$ selects senders for a given receiver R and proceeds honest and valid executions of the Incident Report phase of the protocol polynomial times in security parameter. We assume that $\mathcal{A}$ is allowed to select senders and run the oracle after receiving the transcripts as well.*

Definition 5. *Message broadcasting is* existentially unforgeable under an adaptive chosen-sender attack*, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ the probability, that $\mathcal{A}$ produces a new valid message* **M** *based on the transcripts received during the attack is negligible.*

Definition 6. *If an adversary is deterministic and restricts its action to choosing a sender and a receiver oracle and then faithfully conveying each flow from one oracle to the other, with the sender oracle beginning first, it is called* benign.

Definition 7. *A protocol is a* secure anonymous authenticated message broadcast *if*

1. *In the presence of the benign adversary, the sender and the receiver oracle always accept and*

for every adversary $\mathcal{A}$ and uncorrupted receiver and sender oracles

2. *message broadcasting is existentially unforgeable under an adaptive chosen-sender attack and*

3. *for the tested oracles chosen by $\mathcal{A}$ the $Adv^{\mathcal{A}}(\kappa)$ is negligible.*

Theorem 1. *The proposed authenticated anonymous message broadcast protocol is secure in the malicious-but-cautious model if solving the Computational Diffie-Hellman is computationally infeasible. The bilinear map is considered in the generic bilinear group [5] model and the hash functions are supposed as random oracles.*

The proposed AABMB scheme meets the requirements. Theorem 1 states that our scheme is secure according to Definition 7, hence it guarantees message authenticity and integrity for incident reports and sender anonymity. Additionally, the anonymity of malicious senders can be revoked. Together, TA and RSU can calculate the ID of the vehicle following the Malicious Use Management process. Unlinkability of incident reports is also provided. For each report message, the sender chooses a new random value, denoted as a. The receiver then verifies whether the vehicle is on the list AUL by calculating $e(A, B)$. The elements within the list AUL are frequently randomized and permuted. Hence messages from the same sender cannot be linked. Let us consider several relevant attacks for review. In a man-in-the-middle (MIM) attack, an attacker positions themselves between a sender and a receiver. However, this attack is not relevant in our case because we send incident reports as broadcast messages. Protection against impersonation and modification attacks is achieved since message authenticity and integrity of incident reports are proven in Theorem 1. In a replay attack, an attacker intercepts and retransmits incident report messages. Since the messages are timestamped, any retransmission with an invalid timestamp will be rejected.

5 Conclusion and efficiency

This paper presents an Authenticated Anonymous Batch Message Broadcast (AABMB) designed for VANETs and based on identity-based cryptography. Our protocol uses bilinear pairings and does not require devices to store the master secret key. OBUs only need to download the Revocation and the Anonymized User Lists, and it is essential, if necessary, that the sender's anonymity can be revoked. We improve the efficiency comparing to [11] and also provide a detailed security analysis for the Incident Report phase. We introduce a new adversarial model and a definition for a secure anonymous authenticated message broadcast scheme and show that our scheme is secure if the Computational Diffie-Hellman problem is computationally infeasible.

To assess efficiency, we compare the performance of AABMB with existing schemes referencing the execution times for various cryptographic operations [2], [10], [17], and [19].

Scheme	**Inc. submission time**	**Inc. verification time**
Zhang et al. [18]	1.7161 ms	16.0581 ms
Bayat et al. [3]	7.8311 ms	18.7551 ms
Wang et al. [16]	1.7161 ms	18.748 ms
Our scheme	1.7161 ms	14.3491 ms

Table 2: Time efficiency of incident submission and verification

References

[1] IEEE standard for wireless access in vehicular environments–security services for applications and management messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pages 1–240, 2016.

[2] Udit Bansal, Jayaprakash Kar, Ikram Ali, and Kshirasagar Naik. Id-ceppa: Identity-based computationally efficient privacy-preserving authentication scheme for vehicle-to-vehicle communications. *Journal of Systems Architecture*, 123:102387, 2022.

[3] M. Bayat, M. Barmshoory, M. Rahimi, et al. A secure authentication scheme for vanets with batch verification. *Wireless Netw.*, 21:1733–1743, 2015.

[4] Majid Bayat, Morteza Pournaghi, Majid Rahimi, and Mostafa Barmshoory. Nera: A new and efficient rsu based authentication scheme for vanets. *Wireless networks*, 26:3083–3098, 2020.

[5] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, pages 440–456. Springer, 2005.

[6] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, pages 213–229, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[7] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 20(1):770–790, 2017.

[8] TS ETSI. 102 941 v2. 2.1 (2022-11); intelligent transport systems (its); security; trust and privacy management. *European Telecommunications Standards Institute: Sophia Antipolis, France*, 2021.

[9] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7–20, 2017.

[10] Debiao He, Sherali Zeadally, Baowen Xu, and Xinyi Huang. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Trans. Info. For. Sec.*, 10(12):26812691, dec 2015.

[11] Andrea Huszti, Szabolcs Kovács, and Norbert Oláh. Hybrid anonymous message broadcast for vanets. In *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 103–108. IEEE, 2021.

[12] Seyed Morteza Pournaghi, Behnam Zahednejad, Majid Bayat, and Yaghoub Farjami. Necppa: A novel and efficient conditional privacy-preserving authentication scheme for vanet. *Computer Networks*, 134:78–92, 2018.

[13] Mark D Ryan. Enhanced certificate transparency and end-to-end encrypted mail. *Cryptology ePrint Archive*, 2013.

[14] Adi Shamir. Identity-based cryptosystems and signature schemes. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, pages 47–53, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[15] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan. Enhancing security and privacy for identity-based batch verification scheme in vanets. *IEEE Transactions on Vehicular Technology*, 66(4):3235–3248, 2017.

[16] Shibin Wang and Nianmin Yao. Liap: A local identity-based anonymous message authentication protocol in vanets. *Computer Communications*, 112:154 – 164, 2017.

[17] Xianglong Wang, Qiuting Chen, Zhenwan Peng, and Yimin Wang. An efficient and secure identity-based conditional privacy-preserving authentication scheme in vanets. *International Journal of Network Security*, 24(4):661–670, 2022.

[18] Jianhong Zhang, Min Xu, and Liying Liu. On the security of a secure batch verification with group testing for vanet. *Int. J. Netw. Secur.*, 16:355–362, 2014.

[19] Xiaotong Zhou, Min Luo, Pandi Vijayakumar, Cong Peng, and Debiao He. Efficient certificateless conditional privacy-preserving authentication for vanets. *IEEE Transactions on Vehicular Technology*, 71(7):7863–7875, 2022.

How to Sign Quantum Messages

1 Background

Given the consistent advancements in quantum computing, it is expected that future communications will feature quantum computers transmitting over quantum channels. A fundamental question naturally arises: how can quantum data be securely transmitted within the emerging quantum internet? One option is for users to share secret keys through secure channels. Yet, this option quickly becomes unwieldy as the number of users grows or when secure channels are not readily available. Another option is to rely on quantum key distribution [7], but this too is inefficient for large-scale applications as it requires several rounds of interaction with each user. In contrast, classical information can be encrypted and authenticated non-interactively via public channels. Can a similar feat be achieved quantumly?

Towards this goal, several works have shown how to encrypt quantum information from standard assumptions [2, 3]. Yet, somewhat surprisingly, signing quantum information has been shown to be impossible [6, 3]. On the other hand, classical digital signature schemes have been crucial cryptographic primitives - realizing a range of applications including email certification, online transactions, and software distribution.

As a result of the impossibility, researchers have focused on an alternative approach to quantum authentication called *signcryption*. In this setting, the sender uses the recipient's public encryption key to encrypt a message before signing it. Only the recipient can verify that the signature is authentic by using their secret decryption key which means that signcryption does not allow for public verifiability – only a single receipient can verify. Such schemes clearly rely on assumptions for public-key encryption such as trapdoor functions. Until this point, it was widely believed that signcryption is the only way to evade the impossibility result. In fact, Algaic, Gagliardoni, and Majenz [3] carried out an in-depth analysis on the possibility of signing quantum information and concluded that *"signcryption provides the only way to achieve integrity and authenticity without a pre-shared secret"*. In this work, we address and revisit the questions: *Are there alternative methods to authenticate quantum information without a pre-shared secret?*

Interestingly, this question has important implications in quantum public key encryption (QPKE). Traditionally, classical public-key encryption (PKE) can not be built from one-way functions [17] and requires stronger assumptions such as trapdoor functions. However, the works [15, 11] show that PKE can be achieved from post-quantum secure classical one-way functions (pq-OWF) if the public-keys are quantum! Yet, these constructions face a serious problem: authenticating a quantum state is difficult. This issue is not addressed in these

works; as a result, these constructions need to assume secure quantum channels for key distribution which is quite a strong physical setup assumption given the goal of encryption is to establish secure communication over insecure channels. On the other hand, there are well-established methods to distribute classical keys, for instance through the use of classical digital signatures. Such procedures are referred to as *public-key infrastructure*.

Ideally, we aim to establish encryption based on public-key infrastructure and one-way functions. More simply, we want to authenticate the quantum keys in QPKE schemes using classical certification keys. Prior to this work, the only way to do this would be through the use of signcryption. But, then we are back to relying on assumptions of classical PKE. In particular, the following is another critical question addressed in this work: *Is QPKE with publicly-verifiable quantum public-keys possible from pq-OWFs?*

Another relevant application of quantum signatures pertains to public-key quantum money. Public-key quantum money has only been constructed assuming indistinguishability obfuscation [1, 25, 23] or from new complex mathematical techniques and assumptions [13, 21, 20] which we are only beginning to understand and, some of which, have been shown to be susceptible to cryptanalytic attacks [8]. Sadly, all existing constructions for indistinguishability obfuscation are built on assumptions that are post-quantum insecure [4, 19, 18] or on new assumptions [14, 24] that have been shown to be susceptible to cryptoanalytic attacks [16]. As a result, public-key quantum money remains an elusive goal, which raises the following important question addressed in this work: *Is public-key quantum money possible from standard computational assumptions?*

2 Our Contribution

The impossibility of signing quantum information was first discussed by [6] and, later, established more rigorously in [3]. Informally, the core argument is that any verification algorithm, denoted as V, which can deduce the quantum message (or some information thereof) from a signature, can be effectively inverted $V^\dagger$ to sign a different message.

The central innovation of this work lies in recognizing that, in specific scenarios, this inversion attack consumes a prohibitive amount of resources. This study explores two variations of this concept, with the resource factor taking the form of either time or quantum space, as we clarify in the ensuing discussion.

2.1 Time-Dependent Signatures

We introduce the concept of time-dependent (TD) signatures, where the signature of a quantum message depends on the time of signing and the verification process depends on the time of the signature reception. We construct this primitive assuming the existence of post-quantum secure one-way functions (pq-OWFs) and time-lock puzzles (TLPs) [22, 9].

A TLP is a cryptographic primitive that enables hiding a message for a time t from any QPT adversary but allows for decryption in a similar time $t' \approx t$. Encryption should be much more efficient than decryption – specifically, the encryption circuit should have depth $\log(t')$ and size t'. [9, 10] showed that TLP can be constructed, assuming the existence of pq-OWFs, from a random oracle. Essentially, the TLPs ensure that the verification procedure demands prohibitive time to inverse.

We provide a brief description of our construction for TD signatures. We denote the algorithms for a one-time symmetric authenticated encryption scheme on quantum messages as $(\mathsf{1QGen}, \mathsf{1QEnc}, \mathsf{1QDec})$, which exists unconditionally [6]. To sign a quantum message ϕ, we sample a key $\mathsf{k} \leftarrow \mathsf{1QGen}(1^\lambda)$ and authenticate the message as $\tau \leftarrow \mathsf{1QEnc}(\mathsf{k}, \phi)$. Following this, we generate a TLP Z requiring 1 hour to solve and whose solution is the message $(\mathsf{k}, T, \mathsf{sig})$, where T corresponds to the time at the moment of signing and sig is a signature of (k, T) under a classical signature scheme. Consequently, the signature of ϕ is (τ, Z).

Assume that a receiver gets the signature at time T'. To verify, the receiver solves the puzzle Z to learn $(\mathsf{k}, T, \mathsf{sig})$. If the signature sig is valid and the time of reception is close to T, i.e. T' is within half an hour from T, then the verifier outputs $\mathsf{1QDec}(\mathsf{k}, \tau)$ to retrieve ϕ. However, it is crucial to understand that the verifier can no longer use the pair (k, T) to sign a new message because by the time the puzzle is unlocked, it has already become obsolete! Specifically, the time is at least $T + 1$, leading future verifiers to reject a message signed using sig. Notice how the use of TLP gives us the ability to add intricacy to the verification process, and this is precisely what is needed to circumvent the impossibility result.

Dynamic Verification Keys: By utilizing verification keys that evolve over time, we eliminate the need for TLPs in our construction. This leads to TD signatures from pq-OWFs with dynamic verification keys. This approach also enforces a verification process that is time-consuming to invert. However, in this case, this enforcement is achieved more directly by delaying the announcement of the verification key. Specifically, we authenticate and encrypt a quantum messages in a symmetric-key fashion, as before, but announce the symmetric key later. By the time the key is revealed, allowing users to validate old signatures, it is too late to exploit the key for forging new signatures. As a result, the verification key must be continually updated to allow for new signature generation. An attractive aspect of this signature approach is that it can be based solely on pq-OWFs, yielding surprisingly powerful applications from fundamental assumptions.

Applications: We demonstrate how to utilize TD signatures to build more secure QPKE schemes where the quantum public-keys are signed with TD signatures. In particular, our QPKE scheme features authenticated quantum public-keys that resist adversarial tampering. This approach allows basing QPKE on pq-OWFs and public-key infrastructure.

Furthermore, we employ TD signatures to construct a time-dependent public-key quantum money scheme based on a standard computational assump-

tion, namely pq-OWFs, where the quantum money consists of quantum signatures. The verification key in this setting is dynamic, preventing a completely offline money scheme. We are able to mitigate this issue and obtain a completely offline public-key quantum money scheme by utilizing TLPs.

2.2 Signatures in the BQSM

Our second strategy for signing quantum information involves a verification process that necessitates an impractical amount of quantum memory to invert. To achieve this, we need to assume the adversary's quantum memory (qmemory) size is limited leading us to the *bounded quantum storage model* (BQSM) [12]. We show that quantum messages can be signed with *information-theoretic security* in this model i.e. without any computational assumptions.

Our construction requires users to have ℓ^2 qubits of quantum memory, where ℓ is the size of the quantum message to be signed, and is information-theoretically secure against adversaries with $\mathtt{s}$ quantum memory where $\mathtt{s}$ can be set to any fixed value that is polynomial with respect to the security parameter. Note that $\mathtt{s}$ is not related to ℓ and only has an effect on the length of the quantum transmissions involved. The construction is technically involved and builds on previous work in the BQSM [5].

3 Conclusion

Signing quantum messages has long been considered impossible even under computational assumptions. In this work, we challenge this notion and provide three innovative approaches to sign quantum messages that are the first to ensure authenticity with public verifiability.

More generally, this work demonstrates the power of utilizing time in cryptography, showing how incorporating time-dependence can aid in the construction of fundamental cryptographic primitives such as QPKE, quantum signatures, and public-key quantum money. This is particularly encouraging given the simplicity and security of implementing time-dependence in practice. Therefore, an interesting avenue for future work is to consider what other cryptographic primitives can benefit from this approach.

Finally, we believe that the BQSM has not received adequate attention. Given the practical challenges of storing and operating on quantum states, this model is very well motivated. However, research on cryptographic primitives within this framework remains limited. We hope that this work will encourage further research in this area.

References

[1] Scott Aaronson and Paul Christiano. "Quantum money from hidden subspaces". In: *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*. 2012, pp. 41–60.

[2] Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael St. Jules. "Computational security of quantum encryption". In: *Information Theoretic Security: 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers 9*. Springer. 2016, pp. 47–71.

[3] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. "Can you sign a quantum state?" In: *Quantum* 5 (2021), p. 603.

[4] Prabhanjan Ananth, Aayush Jain, Huijia Lin, Christian Matt, and Amit Sahai. "Indistinguishability obfuscation without multilinear maps: new paradigms via low degree weak pseudorandomness and security amplification". In: *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III*. Springer. 2019, pp. 284–332.

[5] Mohammed Barhoush and Louis Salvail. "Powerful Primitives in the Bounded Quantum Storage Model". In: *arXiv preprint arXiv:2302.05724* (2023).

[6] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. "Authentication of quantum messages". In: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* IEEE. 2002, pp. 449–458.

[7] Charles H Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *arXiv preprint arXiv:2003.06557* (2020).

[8] Andriyan Bilyk, Javad Doliskani, and Zhiyong Gong. "Cryptanalysis of three quantum money schemes". In: *Quantum Information Processing* 22.4 (2023), p. 177.

[9] Nir Bitansky, Shafi Goldwasser, Abhishek Jain, Omer Paneth, Vinod Vaikuntanathan, and Brent Waters. "Time-lock puzzles from randomized encodings". In: *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*. 2016, pp. 345–356.

[10] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. "On the compressed-oracle technique, and post-quantum security of proofs of sequential work". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2021, pp. 598–629.

[11] Andrea Coladangelo. "Quantum trapdoor functions from classical one-way functions". In: *arXiv preprint arXiv:2302.12821* (2023).

[12] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. "Cryptography in the Bounded-Quantum-Storage Model". In: *SIAM Journal on Computing* 37.6 (2008), pp. 1865–1890. ISSN: 0097-5397. DOI: 10.1137/060651343. arXiv: quant-ph/0508222.

[13] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. "Quantum money from knots". In: *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. 2012, pp. 276–289.

[14] Romain Gay and Rafael Pass. "Indistinguishability obfuscation from circular security". In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 2021, pp. 736–749.

[15] Alex B Grilo, Or Sattath, and Quoc-Huy Vu. "Encryption with Quantum Public Keys". In: *arXiv preprint arXiv:2303.05368* (2023).

[16] Sam Hopkins, Aayush Jain, and Huijia Lin. "Counterexamples to new circular security assumptions underlying iO". In: *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II 41*. Springer. 2021, pp. 673–700.

[17] Russell Impagliazzo and Steven Rudich. "Limits on the provable consequences of one-way permutations". In: *Proceedings of the twenty-first annual ACM symposium on Theory of computing*. 1989, pp. 44–61.

[18] Aayush Jain, Huijia Lin, and Amit Sahai. "Indistinguishability obfuscation from LPN over F_p, DLIN, and PRGs in NC_0". In: *Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part I*. Springer. 2022, pp. 670–699.

[19] Aayush Jain, Huijia Lin, and Amit Sahai. "Indistinguishability obfuscation from well-founded assumptions". In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 2021, pp. 60–73.

[20] Daniel M Kane, Shahed Sharif, and Alice Silverberg. "Quantum money from quaternion algebras". In: *arXiv preprint arXiv:2109.12643* (2021).

[21] Andrey Boris Khesin, Jonathan Z Lu, and Peter W Shor. "Publicly verifiable quantum money from random lattices". In: *arXiv preprint arXiv:2207.13135* (2022).

[22] Ronald L Rivest, Adi Shamir, and David A Wagner. "Time-lock puzzles and timed-release crypto". In: (1996).

[23] Omri Shmueli. "Public-Key Quantum Money With a Classical Bank". In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. 2022, pp. 790–803.

[24] Hoeteck Wee and Daniel Wichs. "Candidate obfuscation via oblivious LWE sampling". In: *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part III*. Springer. 2021, pp. 127–156.

[25] Mark Zhandry. "Quantum lightning never strikes the same state twice. or: quantum money from cryptographic assumptions". In: *Journal of Cryptology* 34 (2021), pp. 1–56.