UDC 004.056.55

IMPROVED MATHEMATICAL MODEL OF THE POST-QUANTUM ELETRONIC SIGNATURE MECHANISM

Yurij Gorbenko[1], Kateryna Isirova[2]

[1] JSC "Institute of Information Technologies", 12 Bakulin St., Kharkiv, 61166, Ukraine
GorbenkoU@iit.kharkov.ua

[2] V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
KaterinaIsirova@gmail.com

Reviewer: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, 64849, Mexico.
kalash@itesm.mx

Received on November 2018.

Abstract. *In the paper new electronic signature mechanisms which will be urgent in the post-quantum period development necessity is grounded. The main one time key mechanisms are briefly described. Problems related with Lamport OTS mechanism and Winternits OTS mechanism related to private and public keys sizes are revealed. Main evaluation criteria are defined. In the paper improved mechanism called POST which can be used in post-quantum period is proposed. POST mechanism is tends to avoid the disadvantages as previous ones. Also processes of signature generation and validation for POST mechanism are presented.*

Keywords: *post-quantum cryptography; post-quantum electronic signatures; improved mechanism POST; one time key mechanisms.*

1 Introduction

Development and standardization post-quantum asymmetric cryptographic transformation is one of the most important problems of our time. The leading states, including NIS, realizing the need to find new asymmetric cryptographic primitives electronic signature (ES) and asymmetric encryption to be relevant and can be used in post quantum period, announced a competition to develop standards of post quantum asymmetric cryptographic primitives [1-3]. Bids were accepted NIST until the 30th November 2017. They relate primarily asymmetric algorithms ES. The European Union (EU) is also active in the development and research of post-quantum asymmetric cryptographic standards, including standards post-quantum ES.

Conducted in technologically developed countries showed that one of the promising areas post-quantum ES creation, can be direction based on the use of hash functions and Merkle tree [6]. The basis of this trend assigned keys and single-use one time ES. Historically the current time and offered substantially explored these mechanisms for generating and using single-key ES based on hash functions (*symmetric cryptographic functions and traction*):

- Lamport mechanism of one time keys LOTS [7];
- Winternits mechanisms with one time keys WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8,10];
- modification mechanism of one time keys Biba, HORS, HORS +, HORS ++ and HORST [10].

2 Problem and opportunities

Significant development of ES mechanism based on OTS is Winternits OTS [4,8]. The fact is that although the Lamport OTS and Lamporta – Diffie OTS may provide the potential properties of cryptographic resistance (and indeed encryption), but the size and ES and OTS keys are quite large. Reducing the size of the ES mechanism achieved in ES with OTS as proposed in [4,13], called Winternits mechanism (W OTS) [8]. The idea Winternits mechanism is signed so that, unlike the Lamport OTS already several bits of hash - values using a sequence OTS single secret key. Another feature is the use Winternits mechanism aimed one-way function that we believe can be called

clutch function. The peculiarity of the clutch functions is possibility of public key obtained directly from the ES. In our view this is a crucial feature of the Winternits mechanism.

As in the Lamport OTS and Lamport – Diffie OTS mechanisms, the Winternits mechanism (WOTS) uses a one-way hash - function and cryptographic hash - function. Parameter Winternits ES $w \geq 2$ selected as the number of bits that must be signed (encrypted) simultaneously using a single key. ES is also an option WOTS using additional control method based on integrity checksum hash - value that is encrypted. Applying additional method of monitoring the integrity aims to reinforce stability Winternits OTS ES.

Also, the analysis showed that the main papers related to one time keys are used insufficiently "true" cryptographic evaluation criteria cryptographic stability and complexity. In our opinion, when evaluating and comparing different mechanisms of ES OTS, should at least use [5]:

- Lc, Lv and Lp - length, respectively classified Ks and public key ES in April and open;
- the number of secret Nk one time key ES WOTS that can be used with equal probability;
- entropy source key H (Nk) of the modification ES WOTS single key;
- secure a TB as expectation time disclosure of cryptographic system known in the application of analytical power and attacks by both classical and quantum computers and, in this case for example the definition of secret key provided and consequently ES single public key ES OTS;
- distance unity sources l_0 OTS one time ES secret keys;
- complexity of a successful crypto analysis Ic ES with OTS in the application of force;
- complexity of a successful crypto analysis Ia ES OTS in applying analytical methods.

Basic definitions and the application of the proposed criteria and indicators for assessing the ES from OTS to be applied in required in the analysis and comparison.

The analysis of the basic mechanisms of one time keys - Lamport OTS, OTS Winternits (WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8,9]) and modification mechanism of one time keys (Biba, HORS, HORS +, HORS ++ and HORST) do not meet the requirements of space and time complexity, which greatly complicates the implementation post-quantum ES based on hash functions. The fact is that when trying to reduce the size of the keys and the ES is a dESarture from the true perfect ES [13-15]. However, in our view, there is the possibility of building a ES post-quantum based OTS keys as perfekt OTS (POTS) [13], the properties are almost not inferior Lamport mechanism. Therefore, we consider the nature, the study of properties, advantages and disadvantages, as well as conditions and opportunities for improved use of POTS mechanism in various applications post-quantum period.

3 Improved mathematical model of the post-quantum electronic signature mechanism

Terms. In Winternits OTS (WOTS) ES mechanism exists over the Lamport mechanism, the ability to produce shorter ES, but the number of private and public keys with increasing parameter w increases significantly. Also generally WOTS mechanism that is adequate for the characteristics of the Lamport mechanism significantly increased temporal and spatial complexity. The specified limits the use of Winternits mechanisms (WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8,9]) for the case when the requirement should be similar to that performed Lamport mechanism. There is no possibility to use the private key for both signature and some much larger number of hash - value (WFTS) [9]. Using this idea, consider an improved POTS mechanism with one time keys, which are the main advantages of reducing the lengths of one-time keys (*private and public key*) and the length of the ES. There are also options for its use and WFTS.

As in LOTS and LDOTS, in an enhanced POTS mechanism or will use the one-way hash – function

$$f: \{0, 1\}^{l} \rightarrow \{0, 1\}^{l} \quad (1)$$

and required cryptographic hash - function

$$g: \{0, 1\}^{*} \rightarrow \{0, 1\}^{l}.$$

In ES first message *M* made hash message *M* using coherent (typically cryptographic) hash - functions with parameters *Pr* and computed hash – value

$$h_M = H(M, Pr)) \tag{2}$$

Further value h_M essentially means replacing the encrypted blocks w bits of hash - value h_M one time secret key encryption process this continues for all blocks of bits hash - value h_M.

So, l_h bit hash – value h_M replaced (encrypted) once the keys essentially steady course codes as a sequence of bits h_M replaced one time secret random order. Sequence l_k secret sequence is the message M. This ES ES with a selected x_i or y_i sequences is as open and accessible to users (*verifyer*) of the domain and the offender (*crypto analytics*). Later this ES in the appropriate format transmitted and stored along with the message and is its single ES. In the case of POTS ES mechanism consists of k random sequences, and $k \le l_h$.

Key generation mechanism for POTS. We assume that the parameter $w \ge 1$ determines the number of bits of hash - value that should be signed simultaneously, ie replaced by a secret key. Moreover, if $w = 1$ have particular case - OTS Lamport mechanism of keys. If $w \ge 2$ have a common Winternits mechanism submission, although further validation and encryption function is modified.

In the POTS mechanism ES (encryption) is performed (not necessarily) by applying to all w_b block conversion type

$$z = Z(w_b) \tag{3}$$

Therefore, w bits of the block are displayed in bits w * new unit. Moreover L_{bi} length b_i Block can be either more or less length L_{bi*} bloc b_i^* Derived from transformation (3).

Immediately note that the main difference POTS mechanism is that it applies each transformation b_i block according to [13] in this form. If

$$0 \le b_i \le (2^w / 2) - 1 \tag{4}$$

then each b_i encrypted block (replaced) sequentially secret key from the set X, or encrypted (*replaced*) sequentially secret key from the set Y.

Also, similar to the generalization Winternits define parameters t_1, t_2, t as [7,8]

$$t_1 = \left\lceil l / \log_2 w^* \right\rceil, t_2 = \left\lceil \log_2 t_1((w^* - 1)) / \log_2 w^* \right\rceil + 1, \quad t = t_1 + t_2. \tag{5}$$

We assume that the hash - value message supplied in blocks b_i (b_i^*) type

$$\text{d = bt1-1 || .bi. . || b0,} \tag{6}$$

can determine the checksum in the form [7]

or as

$$c^* = \sum_{i=1}^{t_1} (w^* - 1 - b_i^*), \tag{7}$$

$$c^* = \sum_{i=1}^{t_1 1} (2^{w^*} - b_i^*). \tag{8}$$

In the POTS model is not excluded that the parameters t_1, t_2, t can be defined otherwise. In mechanisms POTS data hash - value d (6) and checksum C (7) and (8) can encrypt different handicap, such as a checksum with more or less depending on the requirements of the handicap.

However, a preliminary analysis showed that the type conversion functions blocks (3) and (4) can significantly affect the cryptographic resistance to existing and potential attacks. Therefore, one of the important objectives of this study is to determine the conversion functions, which will allow to provide shorter secret and public keys, and reduce the length of the ES, providing acceptable cryptographic resistance to existing and potential attacks from classical and quantum computers.

After you convert (6) or (7) checksum C^* in blocks of bits w^* concatenation of hash - value (6) d and then runs simultaneous identical encryption POTS and verification. Note that checksums are

calculated arbitrarily depending on the need. Also mentioned ES d and checksums *C* (7) and (8), etc., can be encrypted worthy of OTS.

Specification of parameters for POTS. To make ES refine your first signature - *t1*, *t2* and *t*. If the length of L_s random or pseudorandom sequence multiples w^*. Then *t1* determines the number of blocks of bits hash - value that will be signed (encrypted) a secret key. In this case

$$t = t1 = n / w^* \tag{9}$$

If n is not a multiple w^*, The last block is less than w^* bits, so the number of bits required to sign necessary to increase the way that *t1* was intact. In (8) *t2* determines the number of blocks by which filed checksum. Generally

$$t^* = t1 + t2 \tag{10}$$

Without loss of both theoretical and practical presentation and research WOTS can (*but not necessarily*) considered that the length of the block *w = 1,2,3,3., 4.6...* . Under this condition for each unique encryption w_i vacancies in general

$$N_w = 2^w,\ w = 2,3,4,5,6... \ . \tag{11}$$

random sequences each secret key.

In case (4) for each encryption w_i unit must

$$N_w = 2 \tag{12}$$

random sequences each secret key. Therefore, depending on the value of *w*, *U* gain to reduce the length of the secret key in general to respect POST is WOST

$$U = 2^{w-1} \tag{13}$$

ES secret key POTS $X_d\ (w^*)$, $Y_d(w^*)$ is a sequence of *t* secret keys sets

$$\begin{aligned} X_d(w^*) &= (x_{t-1},\ldots,\ x_i,\ \ldots,\ x_0) \\ Y_d(W^*) &= (y_{t-1},\ldots,\ yi,\ \ldots,\ y_0) \end{aligned} \tag{14}$$

the length of each of the sequences secret $l(w^*)$.

Each set (14) secret keys $X_d\ (w^*)$, $Y_d(w^*)$ is part of the secret (*private*) key.

Public key verification mechanism for ES POTS calculated way hash secret keys (14) using one or directed cryptographic hash - functions *f(g)*. Due *t* get 2 sets of keys to open each:

$$\begin{aligned} H_d(X) &= H(x_{t-1}),\ldots,\ \mathrm{H}(x_i),\ \ldots,\ \mathrm{H}(x_0) \\ H_d(Y) &= H(y_{t-1}),\ldots,\ \mathrm{H}(y_i),\ \ldots,\ \mathrm{H}(y_0) \end{aligned} \tag{15}$$

length of hash - value l_h Each secret key sequence.

Developing a mechanism for POTS ES.

Let the message M have hash - value

$$g(M) = h = (h_l,...,h_i,...,h_0), \tag{16}$$

which should be signed using cryptographic hash - function *g*.

In general, if l_h not fold w^*. Then l_h added to the required number of zeros, so that the length l_h had multiple w^*. Line l_h bits divided into *t* blocks $b_{t-1},...,b_i,...,b_0$ length of w bits each. But we will consider, as a rule, without losing generality case (9).

Further to ES and ES validation rules will apply when the length of the block will change. In fact, as a result of this transformation *w* bits b_i unit displayed in bits $w * b_i^*$ the new unit, and the length L_{hi*} new unit b_i^* can be either more or less length L_{hi} bloc b_i derived from transformation (7).

Thus the POTS mechanism implemented following the previous transformation:

- line l_h bit hash - value is divided into blocks t $b_{t-1},...,b_i,...,b_0$ w bits length of each block;
- w bit b_i blocks appear in the new bit w^* b_i^* blocks, and active case when $b_i^* = b_i$;
- w^* new bit blocks (3) b_i^* encrypted using a secret key ($X_d(b_i^*)$, $Y_d(b_i^*)$) according to (12) - (14) with a length of each of the sequences secret $l(w^*)$.

Thus, unlike Winternits mechanism, the POTS mechanism w bits b_i. Blocks are displayed in bits w^* b_i^* blocks that may have a shorter and more towards w.

The result is as follows ES

$$\{M; Z^* = (\{x_{t^*-1} \mid y_{t^*-1}\}), \{x_{t^*-2} \mid y_{t^*-2}\}, ..., \{x_i \mid y_i\}, ..., \{x_0 \mid y_0\}) =$$

$$\left\{M, Z^* = (z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0^*)\right\} \quad (17)$$

In (17) the symbol " | " means that when encryption ES appears in one of the sequences used secret - x_i or y_i, defined i - by unit of length w^* bits. Further parameter t^* means the number of blocks that can be both more and less than t, and equal to t.

Check ES mechanism for POTS. Check ES carried out in that order.

1. Using cryptographic hash - hash function g made Message M^* for which the test is ES The result is a hash – value

$$h_{Mi^*} = g(M^*, \Pr). \quad (18)$$

If the length of h_{Mi^*} not a multiple of w, then the string of bits h_{Mi^*} in accordance with the agreement a number of zeros is added, so that the length h_{Mi^*} was a multiple of w. Line h_{Mi^*} bits is divided into blocks t^* $b_{t^*-1},...,b_i,...,b\ 0$ length w^* bits each.

2. In accordance with the values b_i blocks h_{Mi^*} verification of the public key ES (15) selected hash - value $H(x_i)$ or $H(y_i)$, because we find that

$$Z^* = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\}, ..., \{H(x_i) \mid H(y_i)\}, ..., \{H(x_n) \mid H(y_n)\}) =$$

$$(z_{t-1}^*, z_{t-2}^*, ..., z_i^*, ..., z_0^*). \quad (19)$$

3. Finally, the user has received a signed message hash all sequences ES (17), gets them hash – value

$$(H(z_{t^*}), H(z_{t^*-1}), ..., H(z_i), ..., H(z_0)) \quad (20)$$

and compares the values with the values (17), i.e. $(z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)$. If all t^* when comparing values coincide, the ES is a real, otherwise the ES considered distorted.

4 Conclusions

The idea of the Winternits mechanism is signed so that, unlike the Lamport OTS already several bits of hash - values using a sequence OTS single secret key. Another feature is the use Winternits mechanism aimed one way function that we believe can be called clutch function. The peculiarity of the functions clutch is possibility of public key obtained directly from the ES. In our view this is a crucial feature of the mechanism Winternits.

The analysis of the basic mechanisms of one time keys - Lamporta OTS, OTS Winternits (WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$) And modification mechanism of one time keys (Biba, HORS, HORS +, HORS ++ and HORST) do not meet the requirements of space and time complexity, which greatly complicates the implementation post-quantum ES based on hash functions. However, in our view, there is the possibility of building a ES post-quantum based OTS keys as perfekt OTS (POTS) [13].

Preliminary analysis showed that the type conversion functions blocks (5) can significantly affect and cryptographic resistance to existing and potential attacks. Therefore, one of the important objectives of this study is to determine the conversion functions, which will allow to provide shorter secret and public keys, and reduce the length of the ES, providing acceptable cryptographic resistance to existing and potential attacks from classical and quantum computers.

Thus, the offer of the use of POTS mechanisms one time keys and also as a result of one-time ES, can make conclusions about the possibility of their use in ES post-quantum mechanisms based on hash - functions.

References

[1] Koblitz N. Menezes A. J. A riddle wrapped in an enigma. URL:https://eprint.iacr.org/2015/1018.pdf
[2] Report on Post-Quatum Cryptography / Chen L. and all. NISTIR 8105 (DRAFT). URL:http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
[3] Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop. 1st Quantum-Safe-Crypto Workshop: E-proceedings. Sophia Antipolis, Sep. 26-27. 2013. P.25–28. URL: https://docbox.etsi.org/workshop/2013/201309_crypto/e-proceedings_crypto_2013.pdf
[4] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
[5] Post-quantum cryptography and mechanisms for its implementation / Gorbenko I.D. and all. Radiotechnics. 2016. Vol. 186. P. 32–52.
[6] Merkle R. A certified digital signature. Advances in Cryptology - CRYPTO '89 / Gilles Brassard, editor. Springer, 1990. Vol. 3.35 of LNCS. P. 218–238.
[7] Lamport L. Constructing digital signatures from a one way function. SRI International Computer Science Laboratory: Technical. Report SRI-CSL-98, 1979. URL:https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf
[8] Hülsing A. W-OTS + - shorter signatures for hash-based signature schemes. Progress. in Cryptology - AFRICACRYPT 2013 / A. Youssef, A. Nitaj, and A.-E. Hassanien, editors. Springer, 2012. Vol. 7918 of LNCS. P. 173–188.
[9] SPHINCS: practical stateless hash-based Signatures. A certified digital signature / D. J. Bernstein and all. Advances in Cryptology - CRYPTO '89 / Gilles Brassard, editor. Springer, 1990. Vol. 3.35 of LNCS. P. 218–238.
[10] SPHINCS: practical stateless hash-based Signatures / D. J. Bernstein and all. URL: djb@cr.yp.to. daira@leastauthority.com, zooko@leastauthority.com.
[11] Gorbenko, I., Ponomar, V. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application. EasternEuropean Journal of Enterprise Technologies. 2017. Vol. 2, Issue 9(86). P. 21–32. URL: http://journals.uran.ua/eejet/article/view/96321/93.881.12
[12] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
[13] Horbenko Yu.I., Melnyk T.V., Horbenko I.D. Analysis of potential post-quantum electronic signatures based on the hash - functions. Radiotechnics. 2017. Vol. 189. P. 115–131.
[14] Gorbenko Yu. Methods of construction of and Analysis, standardization and application KRSM: Monograph / Ed. Gorbenko I. D. Kharkov: Fort, 2015. 958 p.
[15] Horbenko Yu.I., Hanzya R.S. Stability analysis top cryptosystem against quantum cryptanalysis algorithm based on Grover. Data protection: Scientific journal. 2014. P. 22–28.

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологический університет Монтеррея, пр. Еухеніо Гарса Сада 2501, Монтеррей, 64849, Мексика.
E-mail: kalash@itesm.mx

Надійшло: Листопад 2018.

Автори:
Юрій Горбенко, к.т.н., перший заступник головного конструктора ПАТ «Інститут інформаційних технологій», вул. Бакуліна, 12, Харків, 61166, Україна.
E-mail: GorbenkoU@iit.kharkov.ua
Катерина Ісірова, аспірантка, Харківський національний університет ім. В. Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна.
E-mail: KaterinaIsirova@gmail.com

Удосконалений механізм одноразових ключів для постквантового періоду на основі геш–функцій.

Анотація. Обгрунтовано необхідність розробки нових механізмів електронного підпису, які будуть актуальними і можуть застосовуватися в постквантовий період. Виявлено проблеми, пов'язані з механізмами одноразової підписи Lamport і Winternits щодо розмірів особистих і відкритих ключів. Визначено основні критерії оцінки. У роботі пропонується вдосконалений механізм POST, який може бути використаний в пост квантовому періоді. Механізм POST позбавлений недоліків, описаних в попередніх механізмах. Також описані процеси генерації і перевірки підпису для механізму POST.

Ключові слова: постквантова криптографія; постквантові електронні підписи; вдосконалений механізм POST; механізми одноразових ключів.

Рецензент: Вячеслав Калашников, д.т.н., проф., Технологический университет Монтеррея, пр. Еухенио Гарса Сада 2501, Монтеррей, 64849, Мексика.
E-mail: kalash@itesm.mx

Поступила: Ноябрь 2018.

Авторы:
Юрий Горбенко, к.т.н., первый заместитель главного конструктора АО "Институт информационных технологий", ул. Бакулина, 12, Харьков, 61166, Украина.
E-mail: GorbenkoU@iit.kharkov.ua

Екатерина Исирова, аспирантка, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина.
E-mail: KaterinaIsirova@gmail.com

Усовершенствованный механизм одноразовых ключей для постквантового периода на основе хеш-функций.

Аннотация. Обоснована необходимость разработки новых механизмов электронной подписи, которые будут актуальными и могут применяться в постквантовый период. Выявлены проблемы, связанные с механизмами одноразовой подписи Lamport и Winternits относительно размеров личных и открытых ключей. Определены основные критерии оценки. В работе предлагается усовершенствованный механизм POST, который может быть использован в постквантовом периоде. Механизм POST лишен недостатков, описанных в предыдущих механизмах. Также описаны процессы генерации и проверки подписи для механизма POST.

Ключевые слова: постквантовая криптография; постквантовые электронные подписи; усовершенствованный механизм POST; механизмы одноразовых ключей.