New hybrid signature schemes with increasing level of resistance

A V Komarova¹³, A A Menshchikov¹ and A G Korobeynikov¹²

¹ Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverksky Prospekt, Saint-Petersburg, 197101, Russia
² Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation of the Russian Academy of Sciences (IZMIRAN), 5, lit. B Universitetskaya embankment, Saint-Petersburg, 199034, Russia
³ E-mail: piter-ton@mail.ru

Abstract. Post-quantum cryptography is becoming an increasingly popular topic for research around the world. The global cryptographic community is on the verge of standardizing new post-quantum algorithms. The world's largest organizations conduct their own research in this direction. In this article, two hybrid schemes are proposed. They are constructed on generalized methods of increasing resistance of authentication schemes. Hybrid schemes consist of a combination of two independent signature schemes, one of which is the well-known classical asymmetric electronic signature scheme and another one is post-quantum scheme. Thus, this paper suggests the combining Crystals-Dilithium scheme with Rabin scheme and Elgamal scheme respectively. The paper also provides estimates of public key and signature lengths. Conclusions are drawn about the expediency of using generalized methods of combining with such kind of schemes.

1. Introduction

Every year, the quantum computer and everything related to it are mentioned more and more often in scientific publications. Despite the fact that such fully working device has not yet been created, there were a lot of prerequisites for this. Currently, there is a need to standardize new cryptographic systems, which are resistant to quantum calculations.

In 2016 after the workshop on post-quantum cryptography The National Institute of Standards and Technology (the NIST) announced the Post-Quantum Cryptography project (PQC project) [1] and maid the report on PQC: NISTIR 8105 [2]. At the same time the NIST announced the process of developing cryptographic systems that can interoperate with existing communications protocols and are secure against both classical and quantum computers. There are three core cryptographic functionalities: public key encryption, digital signatures, and key exchange, therefore, the creation of these post-quantum standards is one of the primary goals of the project.

Of all the post-quantum approaches (the lattice theory, multidimensional quadratic systems, electronic signatures on hash functions, the theory of algebraic coding, isogeny of elliptic curves, the theory of braids), the lattice theory is the most interesting and promising approach for constructing not
only signature schemes but key exchange and public key encryption also according to the author's opinion.

This statement is confirmed by the fact that out of the seven 3rd round finalists five relate to lattice theory. All the schemes that passed the third round were subjected to a thorough analysis accompanied by the entire world cryptographic community.

By now, the 3rd round of the competition is coming to an end. Of the original 82 candidates, 15 remain at the moment: 7 finalists and 8 alternates. Among the signatures: 3 finalists (Crystals-Dilithium [3], Falcon [4], Rainbow [5]) and 3 alternates (GeMSS [6], Picnic [7], SPHINCS+ [8]). The most promising algorithms we expect to be ready for standardization at the end of the 3rd round (sometime close to the end of 2021) [9]. To ensure maximum cryptographic stability in the following years after standardization, the authors of this article suggest using hybrid schemes. This article suggests combined signature schemes based on several difficult problems simultaneously.

2. Motivation and the main ideas

There are several methods for improving the security of signature schemes. In papers [10, 11] we suggested some of such methods. Exactly the methods of combining post-quantum electronic signature scheme with existing proven signature schemes were shown. In papers [12, 13] we presented some schemes resistant to quantum computer calculations and based simultaneously on the complexity of several difficult-to-solve cryptographic problems. They were Short Integer Solution problem (SISP), Integer Factorization problem and the Discreet Log Problem in finite field (DLP) or elliptic curves Discreet Log Problem (ECDLP). In this article we propose electronic signature schemes created by combining the post-quantum electronic signature scheme Falcon [4], which passed the third round of PQC project [1], with existing and well-known asymmetric schemes such as the Rabin scheme [14], the Schnorr scheme [15], the Elgamal scheme [16], the Russian Standard GOST 34.10-2012 [17].

In this paper authors want to focus on the possibility of creating other combined electronic signature schemes based simultaneously on the difficulty of solving complex computable problems in one scheme. Using the methods from paper [10] it's possible to create new schemes that are resistant to a quantum computer calculations. As a post-quantum scheme on lattices, it was decided to use another scheme that also passed the third round of the PQC project [1] - Crystals-Dilithium [3].

Since both lattice based schemes Falcon [4] and Crystals-Dilithium [3] have matrices and vectors as public and private keys, it is quite feasible to create combined hybrid schemes using the methods from [10] with Crystals-Dilithium.

3. Crystals-Dilithium

The design of Crystals-Dilithium is based on the "Fiat-Shamir with Aborts" technique [18] of Lyubashevsky which uses rejection sampling to make lattice-based Fiat-Shamir schemes compact and secure. It is based on the hardness of Module-SIS and Module-LWE problems. Let's consider the steps of key generating and signing procedures and signature verifying procedure. In this article, we will use simplified variants of these procedures, since the use of specific rejection sampling algorithms will not change the basic essence of using the combined method, but in many ways it will complicate the understanding for the reader. All algebraic operations in this scheme are assumed to be over the polynomial ring \( R_q = \mathbb{Z}_q[x]/(x^n + 1) \). The authors suggest using \( n=256 \).

The key generation procedure consists of the following steps:

- Matrix \( A \in \mathbb{Z}_q^{m \times n} \) is generated.
- Vector \( s \in \mathbb{Z}_q^m \) is sampled.
- Parameter of public key is computed as \( t = Round(A s) \). Each coefficient of these vectors is an element of \( R_q \) with small coefficients.

The public key is \((A, t)\).
The secret key is \( s \).

The signing procedure to message \( M \) is as follows:

- Random vector \( y \in \mathbb{Z}^m_q \) is generated.
- Parameter \( w = \text{Round}(Ay) \) is calculated.
- Using the hash function SHAKE-256 \( c = H(M || w) \) is computed.
- The part of the signature is calculated as \( z = cs + y \).
- To avoid the dependency of \( z \) on the secret key Rejection Sampling of \( z \) is uses.

The signature for the message \( M \) is a pair \( (z, c) \).

Signature verification procedure to message \( M \):

- Parameter \( w' = Az - ct \) is calculated.
- The condition satisfiability is verified \( \|z\| < \beta \), where the parameter \( \beta \) is selected depending on the required level of security.
- Value is calculated \( c' = H(M || w') \).
- If \( c' = c \) then the signature is recognized as genuine.

4. New hybrid signature schemes

4.1 Combining the Crystals-Dilithium scheme and Rabin’s scheme

According to the Method 1 of the article [10] let’s create a new hybrid scheme. The block schemes of the developed algorithm are presented in figures 1 and 2.

The main idea is to represent the Crystals-Dilithium part of the signature \( z \) in the form numerical value \( a \). Then the number \( a \) should be used in Rabin scheme [14] as a primitive root modulo \( n \), where \( n = pq \). Further it is necessary to calculate the value of the combined signature \( s', s' = a^{\frac{1}{2}} \mod n \).

Rabin signature scheme [14] is based on the complexity of calculating square roots by a composite module which is the product of two large prime numbers. In the thesis [19] of Dernova E. an approach was proposed to modify the parameters of the Rabin scheme in order to achieve a gain in speed. This approach is used to generate the module \( n \) in our scheme. Also, in the modified scheme the \((\text{Compress}(s))\) and \((\text{Decompress}(s))\) algorithms are used. The \((\text{Compress}(s))\) algorithm takes a polynomial \( s \) as input and outputs its compressed numerical representation \( s \), the algorithm \((\text{Decompress}(s))\) does the opposite.

Thus, it is possible to achieve embedding the post-quantum scheme in the classical asymmetric scheme without the need to increase the final signature length. However, it should be noted that for the correct operation of this method it is necessary that the number \( s' \) is a quadratic residue, that is, it is necessary to check the feasibility of comparisons \( a^{\frac{p-1}{2}} \equiv 1 \mod p \) and \( a^{\frac{q-1}{2}} \equiv 1 \mod q \), in case of non-fulfillment of any of them, return to the generation of a new \( a \).

The proposed method allows to preserve the original signature length (See table 1), however, according to the theorem of quadratic residues, only a quarter of elements in the group will satisfy the conditions imposed, that is, scheme performance is reduced on the average of four times.

4.2 Combining the Crystals-Dilithium scheme and Elgamal’s scheme

According to the Method 3 of the article [10] let’s create another new hybrid scheme. The block schemes of the developed algorithm are presented in figures 3 and 4.

This method involves the addition of a random vector \( e \) to postquantum part of the signature \( z \): \( k = z + e \). Then it’s necessary to find the numerical representation of \( k \), \( k = \text{Compress}(k) \). The obtained value
of \( k \) can be used in Elgamal scheme [16] as an order \( k \) of the antiderivative root \( a \).

**Figure 1.** Signature generation algorithm using method 1.

**Figure 2.** Signature verification algorithm using method 1.

**Table 1.** Estimation of public key and private key lengths and signature length of developed scheme using method 1 at different security levels.

| Security level | Scheme | Public key length, byte | Signature length, byte |
|----------------|--------|-------------------------|------------------------|
| 1              | Crystals-Dilithium I | 1312                     | 2420                   |
|                | Rabin scheme       | 384                      | 768                    |
|                | Combination of C-D I and Rabin scheme | 1696                     | 768                    |
|                | Crystals-Dilithium III | 1952                     | 3293                   |
| 3              | Rabin scheme       | 576                      | 1152                   |
|                | Combination of C-D III and Rabin scheme | 2528                     | 1152                   |
|                | Crystals-Dilithium V | 2592                     | 4595                   |
| 5              | Rabin scheme       | 768                      | 1536                   |
|                | Combination of C-D V and Rabin scheme | 3360                     | 1536                   |
The advantage of this method can be attributed to the increased level of security due to the use of a random error vector $e$ [11]. However, such schemes can be created exclusively on the basis of Discreet Log Problem. The resulting public key and signature lengths are shown in Table 2.

**Table 2.** Estimation of public key and private key lengths and signature length of developed scheme using method 3 at different security levels.

| Security level | Scheme                                      | Public key length, byte | Signature length, byte |
|----------------|----------------------------------------------|-------------------------|------------------------|
| 1              | Crystals-Dilithium I                         | 1312                    | 2420                   |
| 1              | Elgamal scheme                               | 256                     | 512                    |
|                | Combination of C-D I and Elgamal scheme      | 1568                    | 2932                   |
As we can see from table 2, it was not possible to get the final gain in length in such kind of scheme.

5. Conclusion
In this paper, 2 new hybrid electronic signature schemes were proposed. They were created on the basis of previously published methods of combining several tasks in a single signature scheme. Inevitably, there is the lengths increase as a result hybrid schemes creating, regardless of the combination method. As already mentioned earlier the combining classic asymmetric schemes with post-quantum scheme have already been made in [10-13]. In these works the Falcon [4] was used as a post-quantum scheme. Since it has the shortest sum of the public key and the signature lengths.

In this work we use Crystals-Dilithium scheme. It has the smallest public key + signature size of any lattice-based signature scheme that only uses uniform sampling [3]. As a result of the present work, we can observe increased lengths of keys and signatures. This is due to the initial difference in the parameters lengths in Falcon and Crystals-Dilithium schemes. The main reason between them is that in Crystals-Dilithium signing uses only uniform sampling in a (power-of-2) range, easier to detect bugs. Falcon uses a trapdoor sampler called “fast Fourier sampling”. It’s too fast, but hard to find leaks.

It’s also should be mentioned that in this article, only two combining methods from four were used: the first and the third methods from the article [10]. The fourth method cannot be used when creating a hybrid signature with Crystals-Dilithium scheme, since it uses the Fiat-Shamir model. As for the second method from [10], the results of its application when creating a hybrid scheme will be considered in the following works.

References
[1] Post-Quantum Cryptography Retrieved from: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[2] Chen L, Jordan S, Liu Y K, Moody D, Peralta R, Perlner R and Smith-tone D 2016 Report on Post-Quantum Cryptography, NISTIR 8105 (Gaithersburg, Maryland: National Institute of Standards and Technology) 10
[3] Crystals-Dilithium Retrieved from: https://pq-crystals.org
[4] FALCON Retrieved from: https://falcon-sign.info
[5] Rainbow Retrieved from: https://www.pquerainbow.org
[6] GeMSS Retrieved from: https://www-polsys.lip6.fr/Links/NIST/GeMSS.html
[7] Picnic Retrieved from: https://microsoft.github.io/Picnic
[8] SPHINCS+ Retrieved from: https://sphincs.org
[9] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, Yi-Kai Liu, Miller C, Moody D, Peralta R, Perlner R, Robinson A and Smith-Tone D 2020 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8309 (Gaithersburg, Maryland: National Institute of Standards and Technology) 39
[10] Komarova A V 2019 Generalized methods of increasing resistance of authentication schemes Scientific and Technical herald of Volga region 7 146-8
[11] Komarova A and Korobeinikov A 2019 Combining problems of lattice theory and number theory in schemes, algorithms and authentication protocols Herald of the Ural Federal District
Security in the field of information 2 138-40

[12] Komarova A V and Korobeynikov A G 2019 Combined authentication schemes with increasing level of resistance and methods for improving the security of electronic signature schemes: kombinirovannye skhemy autentifikacii povyshennym urovnem stojkosti metody povysheniya bezopasnosti skhem elektronnoj podpisi ACM International Conference Proceeding Series 3 1-8

[13] Komarova A V, Menshchikov A A, Korobeynikov A G, Kalinkina M E, Tkalich V L and Pirozhnikova O I 2020 Parameters evaluation of the developed combined authentication schemes with increasing level of resistance Journal of Physics: Conference Series 1679(3) 032101

[14] Rabin M O 1979 Digitalized signatures and public-key functions as intractable as factorization Technical report MIT LCS TR-212 MIT Laboratory for Computer Science

[15] Schnorr C P 1990 Efficient identification and signatures for smart cards Advances in Cryptology - CRYPTO’89 Lecture Notes in Computer Science 435 239-52

[16] Elgamal T 1985 A public-key cryptosystem and a signature scheme based on discrete logarithms IEEE Trans. Inf. Theory 31 469-72

[17] Gosstandart of Russia 2013 nformation technology. Cryptographic data security. Generation and verification processes of electronic digital signature GOST 34.10-2012 STANDARTINFORM Publ.18

[18] Lyubashevsky V 2009 Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2009: Advances in Cryptology 598-616

[19] Dernova E S, Moldovyan N A 2007 A new EDS algorithm, the disclosure of which requires the simultaneous solution of two difficult tasks Innovative activity in the Armed Forces of the Russian Federation: Proceedings of the All-Army scientific and practical conference 224-9