III INTERNATIONAL CONFERENCE
KRASNOYARSK, RUSSIA
24-26 September 2021

APITECH
Прикладная физика, информационные технологии и инжиниринг

APITECH
Applied Physics, Information Technologies and Engineering

Science & Technology City Hall
Krasnoyarsk

«Conference on Applied Physics, Information Technologies and Engineering» APITECH-2021

«New hybrid signature schemes with increasing level of resistance»

A V Komarova, A A Menshchikov and A G Korobeynikov

Motivation and relevance

Problem statements:

- The potential appearance of a quantum computer.
- The need to increase the size of keys, which negatively affects performance.
- The appearance of effective methods for solving a complex computable problem leads to a decrease in the stability of the entire crypto algorithm.
- The emergence of legislative initiatives to create new post-quantum standards (National Institute of Standards and Technology, NIST).
- Post-quantum approaches are less proven in practice compared to existing asymmetric schemes.
- There is a need to develop double - security schemes based simultaneously on several complex computable problems
- Combined algorithms and electronic signature protocols will improve the security of existing systems.

The main purpose of this paper is the creating new combined signature schemes with increasing level of resistance .

Combining the Crystals-Dilithium scheme and Rabin scheme

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
3	Crystals-Dilithium III	1952	3293
	Rabin scheme	576	1152
	Combination of C-D III and Rabin scheme	2528	1152
5	Crystals-Dilithium V	2592	4595
	Rabin scheme	768	1536
	Combination of C-D V and Rabin scheme	3360	1536

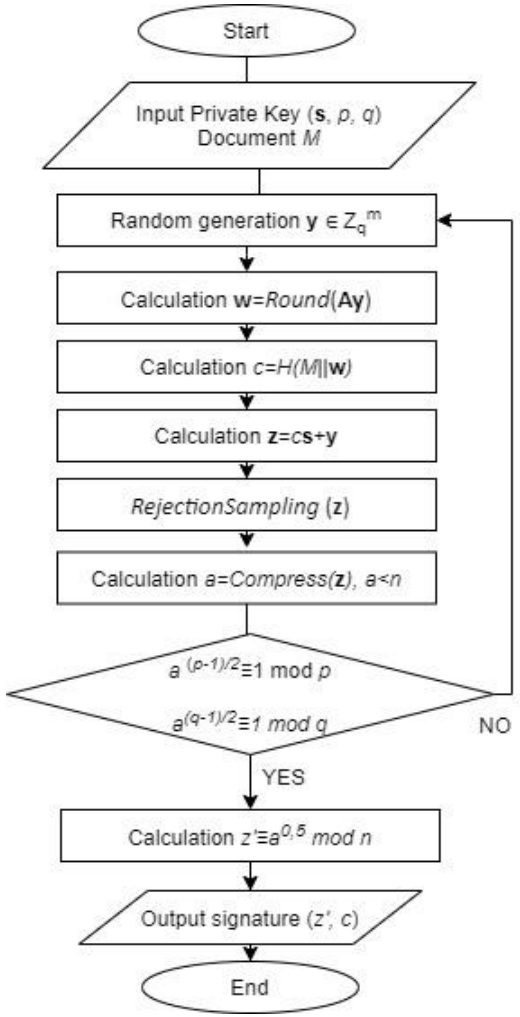

Figure 1. Signature generation algorithm using method 1.

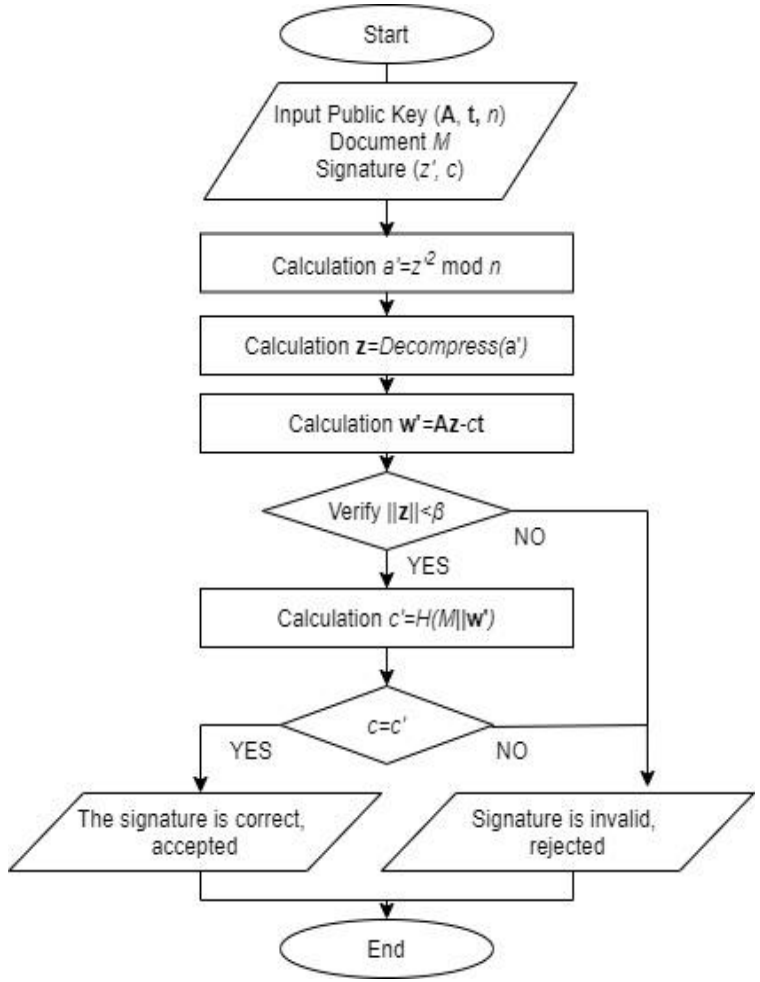

Figure 2. Signature verification algorithm using method 1.

Combining the Crystals-Dilithium scheme and Elgamal scheme

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
	Elgamal scheme	256	512
	Combination of C-D I and Elgamal scheme	1568	2932
3	Crystals-Dilithium III	1952	3293
	Elgamal scheme	384	768
	Combination of C-D III and Elgamal scheme	2336	4061
5	Crystals-Dilithium V	2592	4595
	Elgamal scheme	512	1024
	Combination of C-D V and Elgamal scheme	3104	5619

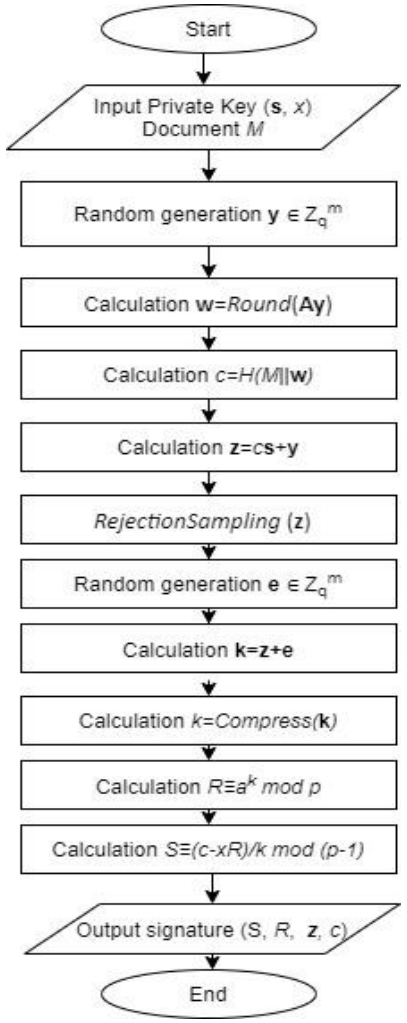

Figure 3. Signature generation algorithm using method 3.

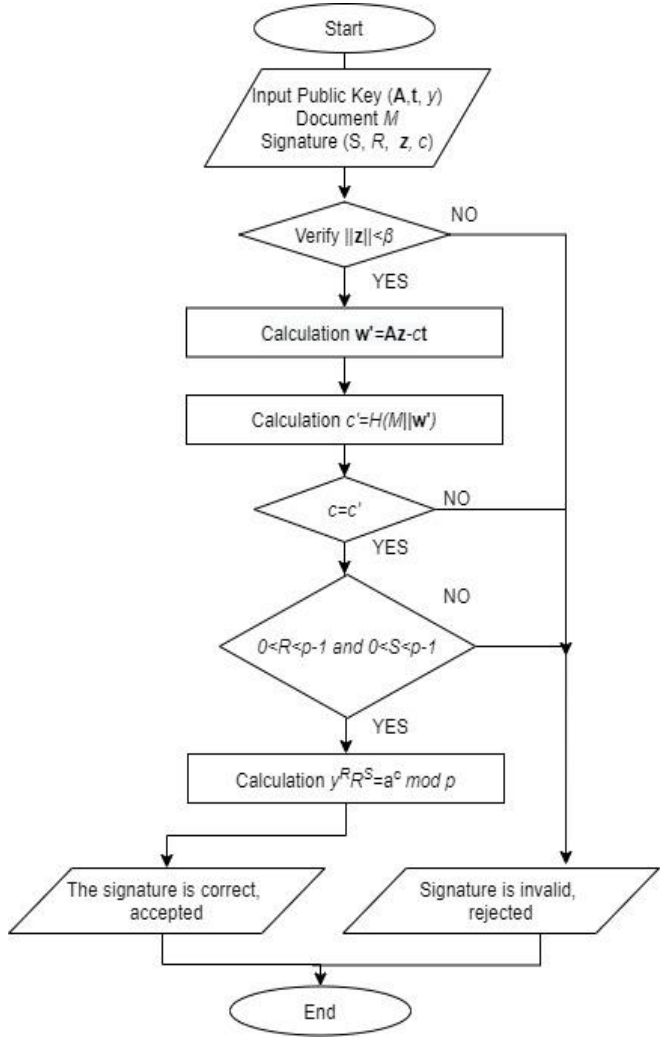

Figure 4. Signature verification algorithm using method 3.

Conclusions:

- In this article the methods of combining signature schemes proposed by the authors earlier were successfully used to create new schemes.
- Two new hybrid electronic signature schemes were constructed in this paper.
- Such schemes significantly increase the security level.
- The first scheme has relatively small increase in key and signature lengths, but scheme performance is reduced on the average of four times.
- In the second scheme there is the lengths increase but it greatly complicate the hacking process for a cryptanalyst.

Contacts

A V Komarova, A A Menshchikov and A G Korobeynikov

Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverksky Prospekt, Saint-Petersburg, Russia, 197101

Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation of the Russian Academy of Sciences (IZMIRAN), 5 lit. B Universitetskaya embankment, Saint-Petersburg, Russia, 199034

E-mail: piter-ton@mail.ru

III INTERNATIONAL CONFERENCE
KRASNOYARSK, RUSSIA
24-26 September 2021

Conference on Applied Physics, Information Technologies and Engineering - APITECH-2021