II INTERNATIONAL CONFERENCE
KRASNOYARSK, RUSSIA
25-27 September 2020

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-2020

«Parameters evaluation of the developed combined authentication schemes with increasing level of resistance»

A V Komarova, A A Menshchikov, A G Korobeynikov, M E Kalinkina, V L Tkalich and O I Pirozhnikova

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 additional parameter estimates of previously developed combined electronic signature schemes in the specific (first) security level.

Parameters evaluation of the developed schemes at the first security level

$$\text{the Falcon} + \begin{matrix}\text{the Rabin scheme}\\ \text{the El-Gamal scheme}\\ \text{the Schnorr scheme}\\ \text{the GOST 34.10-2012}\end{matrix} = \text{the combined scheme}$$

Table 1. Estimation of public key and private key lengths and signature length of developed schemes at the first security level

Scheme	Private key length, byte	Public key length, byte	Signature length, byte
Falcon512	4097	897	617
Rabin scheme	384	384	768
Combination of Falcon512 and Rabin scheme	4481	1281	768
El-Gamal scheme	384	384	768
Combination of Falcon512 and El-Gamal scheme	4481	1281	1385
the Schnorr scheme	384	384	768
Combination of Falcon512 and Schnorr schem	4481	1281	1001
the Russian Standard GOST 34.10-2012	32	32	64
Combination of Falcon512 and GOST 34.10-2012	4129	929	681

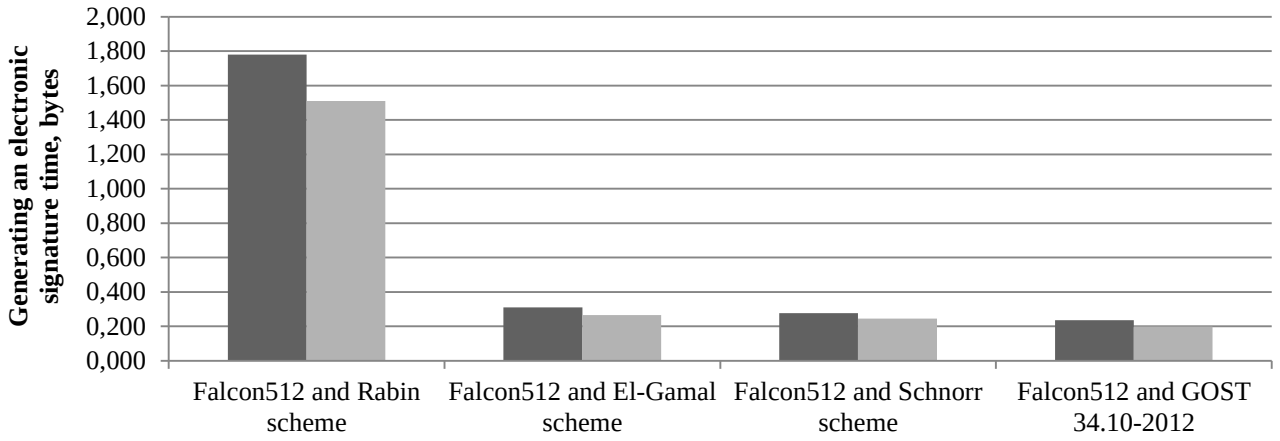

Figure 1. The time estimation spent on the signature generation at the first security level

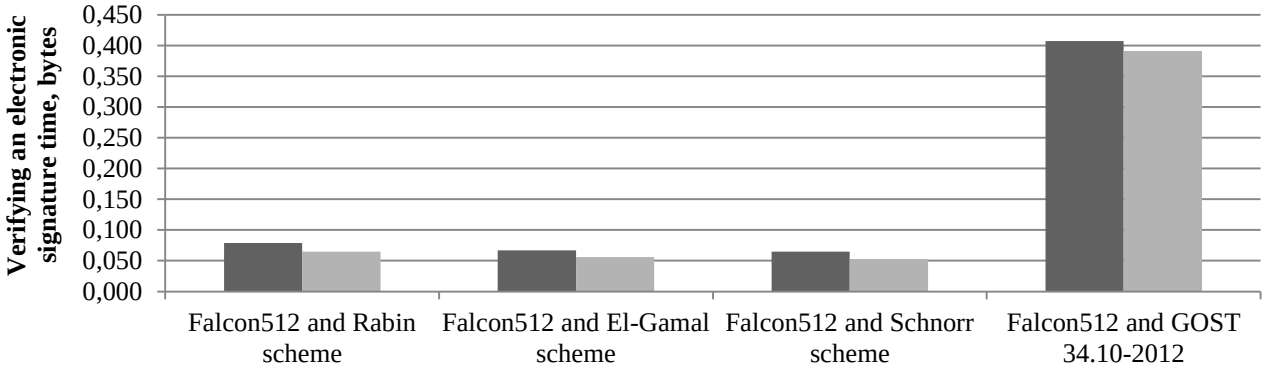

Figure 2. The time estimation spent on the signature verification at the first security level

APITECH
Прикладная физика, информационные технологии и инжиниринг

APITECH
Applied Physics, Information Technologies and Engineering

The final estimates of computational complexity of the developed combined schemes

the Falcon512 and Rabin schemes combination: $$W_1 = \exp\left(\left(\sqrt[3]{\frac{64}{9}} + O(1)\right)(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right) + O\left(\left(\frac{\beta}{2\pi e}\right)^{(1-n/\beta)}\sqrt{q}\right)$$

the Falcon512 and El-Gamal schemes combination and the Falcon512 and Schnorr schemes combination: $$W_2 = \exp\left((\log p \log\log p)^{\frac{1}{2}}\right) + O\left(\left(\frac{\beta}{2\pi e}\right)^{(1-n/\beta)}\sqrt{q}\right)$$

the Falcon512 and the GOST 34.10-2012 combination: $$W_3 = O(\sqrt{r}) + O\left(\left(\frac{\beta}{2\pi e}\right)^{(1-n/\beta)}\sqrt{q}\right)$$

Conclusions:

- Such schemes significantly increase the security level with a relatively small increase in key and signature lengths, as well as time characteristics.
- Such schemes can be used by private companies and government organizations.

Contacts

A V Komarova, A A Menshchikov, A G Korobeynikov, M E Kalinkina, V L Tkalich and O I Pirozhnikova

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

II INTERNATIONAL CONFERENCE
KRASNOYARSK, RUSSIA
25-27 September 2020

Conference on Applied Physics, Information Technologies and Engineering - APITECH-2020