Advantages of Logarithmic Signatures in the Implementation of Crypto Primitives

Yevgen Kotukh
ORCID: https://orcid.org/0000-0003-4997-620X
Dnipro Polytechnic University, Dnipro, Ukraine

Gennady Khalimov
ORCID: https://orcid.org/0000-0002-2054-9186
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

Introduction

Computationally complex tasks, or "hard problems" for brevity, is a broad term that encompasses problems that require a significant number of resources to solve. Cryptography uses them by establishing an equivalence between the security of a scheme and the intractability of a complex problem. Two hard problems have been widely used in public-key cryptography: integer factorization and the discrete logarithm problem. In 1994, Shor [1] showed that these classical complex problems can be easily solved on a large-scale quantum computer. Progress in the creation of quantum computers is becoming more and more tangible. This has prompted the cryptographic community, industry, and many standards organizations to plan to replace the public-key cryptography in widespread use today with a quantum-secure alternative: post-quantum cryptography.

Quantum-resistant cryptosystems based on lattices, linear codes with error correction, multidimensional polynomial equations, one-sided functions, on isogeny of elliptic curves, on non-commutative groups also exploit computationally complex tasks.

Objective and Tasks

The quantum security evaluations of the cryptosystems submitted to the NIST competition and pre-selected as candidates for post-quantum cryptography are constantly being revised and refined. The latest results on the construction of a polynomial quantum algorithm for solving the LWE problem with polynomial modulus-noise relations are exit. Despite the error found in the algorithm, new ideas regarding the application of the complex Gaussian function and the windowed quantum Fourier transform, in the author's opinion, will be able to find new applications in quantum computing or develop new ways to solve the LWE problem. We would venture to assume that any

crypto-algorithm that has regularity properties in its structured data will be broken by a quantum computer. The properties of superposition and quantum entanglement make it possible to perform calculations on all states of the qubit register simultaneously. This property models the full set of states of a classical computer. The presence of regularity in the computational data of the algorithm, for example, periodicity (frequency resonances) in algebraic structures (rings, groups, lattices, etc.) can potentially be filtered by some algorithm with a complexity less than Grover's algorithm. We propose to change the approach to the design of cryptosystems. We replace the concept of a problem that is difficult to solve by a problem that has many equivalent solutions without regularities, when all solutions are equally likely. In this case, quantum cryptanalysis is reduced to Grover's scheme with exponential implementation complexity. We will set linear equations with respect to the unknowns for which we use the values of the logarithmic signatures. The number of equations for secret values of logarithmic signatures is less than their number. This leads to an incomplete system of linear equations with respect to unknowns and the impossibility of solving it in polynomial time. The only attack on a cryptosystem comes down to sorting and defining variables. The secrecy of the cryptosystem of the constructed problem with incompletely determined equations is determined by the power of many solutions.

MATERIALS AND METHODS

The logarithmic signature in the algorithm is a basic cryptographic primitive with excellent cryptographic properties of non-linearity, non-commutability, unidirectionality, and factorability by key. Below we will consider the basic information about cryptosystems with logarithmic signatures. The representation of the logarithmic signature is associated with the positional numbering system. Let $G$is a finite group. The logarithmic signature $\alpha$for a group $G$is a sequence of subsets $A_i \subseteq G$of the form $\alpha = [A_1, \ldots, A_s]$, such that for each element g of the group G there is only one factorization $(*)$ $g = a_q \cdot a_2 \cdot \ \ldots \ \cdot a_s$, where $a_i \in A_i$for $i = 1, \ldots, s$. Sets $A_i$are called blocks. The size of the list of blocks is denoted by $r_i := |A_i|$. For simplicity, we call the elements $A_i \cup \ \ldots \ \cup A_s$logarithmic signature elements α. Under certain conditions, we consider the ordering of the elements of the block, then $k_i = 0, \ldots, r_i - 1$we denote through a_{ik_i}every $(k_i + 1)$-th element of the block A_i. A vector $(r_1, \ldots, r_s)$is called a type α, a

$$\ell(\alpha) = \sum_{i=1}^{s} r_i -$$

with the length of the logarithmic signature. The set of logarithmic signatures of the group is denoted by $\Lambda(G)$. The logarithmic signature is formed from subblocks. Each subblock contains vectors/strings that can be represented as numbers. A cryptogram is determined by the sum of vectors selected by a key (number). The problem of the complexity of the computational security of the cipher lies in the difficulty of finding the decomposition of the cryptogram into vectors, if the correspondence between the positions of the vectors and its values is not known. From the definition, we obtain certain properties of logarithmic signatures.

RESULTS

Let $n \in \mathbb{N}$ For a cyclic group, $(\mathbb{Z}_{2^n}, +)$a sequence of the form $\alpha = [[0, 2^{n-1}], [0, 2^{n-2}], \ \dots \ , \ [0,2], [0,1]]$is a normalized logarithmic signature of the type $(2, \ \dots \ , 2)$. Computing the factorization of an element is equivalent to computing its binary mapping, in particular, if $n = 4$, $9 = 1001$has the factorization of $2^3 + 0 + +0 + 2^0$. Consider the possibility of calculating the factorization of a group element for the specified logarithmic signature and a certain element of the group. For example, an exhaustive search attack by finding all possible factorizations represented by the logarithmic signature $\alpha = [A_1, \ \dots, \ A_s]$of the group G, constitutes $|G| \times (s-1)$group operations in the worst case. Such an iterative finds the correct factorization for any logarithmic signature, but is not possible in the general case. The example demonstrates that for certain logarithmic signatures it is easy to compute factorizations. For practical use in cryptosystems, MSTit is necessary to define logarithmic signatures for which factorization is computationally infeasible, as well as signatures for which there are efficient decomposition algorithms. Mostly, the terms "simple" and "complex" logarithmic signatures are used to denote the difference between logarithmic signatures, for which it is computationally easy and difficult to obtain factorizations, respectively.

CONCLUSIONS

One of the first constructions of a logarithmic signature for finite groups of permutations was proposed for the construction of a symmetric cryptosystem. The basic property of this construction is the possibility of factorization by key. In 2002, Magliveras developed two public key cryptosystems MST1 and MST2 [2]. Lempken used logarithmic signatures and random overlays to create a general MST3 encryption scheme. In this scheme, the public key consists of common logarithmic signatures and some random numbers, and the secret key consists of a random overlay

and a sandwich transform. The assumption of the undecidability of this scheme is the problem of group factorization on non-Abelian groups [3,4,5]. Also, motivated by attacks, Svaba and van Trung reviewed an extended version of the general scheme called eMST3 cryptosystems [6]. Further development of the MST3 cryptosystem was proposed on the basis of high-order groups of generalized Suzuki groups, small Ree groups, three parametric groups, groups of automorphisms of the Suzuki functional field and automorphisms of the Ree functional field [7].

The advantage of logarithmic signatures is that the calculation of ciphertexts is implemented by a simple addition operation with bitwise XOR. The disadvantage is the large size of signature - logarithmic arrays of arrays to ensure a high level of secrecy. A promising direction is the use of logarithmic signatures as a basic crypto primitive, which implements keyless encryption and factorization by the logarithmic signature key.

References

1. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In 35th FOCS, pages 124–134. IEEE Computer Society Press, November 1994

2. SS Magliveras , "A cryptosystem from logarithmic signatures of finite groups," in Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.

3. SS Magliveras and ND Memon, " Algebraic properties of cryptosystem PGM," Journal of Cryptology, vol.5, no.3, pp.167–183, 1992.

4. A. Caranti and F. Dalla Volta, "The round functions of cryptosystem PGM generate the symmetric group," Designs, Codes and Cryptography, vol.38, no.1, pp.147–155, 2006.

5. S. S. Magliveras , P. Svaba , T. van Trung , and P. Zajac, "On the security of a realization of cryptosystem MST3", Tatra Mountains Mathematical Publications, vol.41, pp.65– 78, 2008.

6. P. Svaba and T. van Trung, "Public key cryptosystem MST3 cryptanalysis and realization", Journal of Mathematical Cryptology, vol. 4, no. 3, pp. 271–315, 2010.

7. Gennady Khalimov, Yevgen Kotukh, Oleksandr Sievierinov , Svitlana Khalimova , Sang-Yoon Chang, Yaroslav Balytskyi , Strong Encryption Based on the small Ree groups International Conference "Problems of Infocommunications. Science and Technology" (PIC S&T′2022) October 10 – 12, 2022 Kyiv – Kharkiv.