

The need for post-quantum encryption methods, The features of
the proposed systems TANIA-SK, TANIA-PK, TANIA-DS
(TANIA-SECRETE-KEY, TANIA-PUBLIC-KEY, TANIA-
DIGITAL-SIGNATURE)
and the requirements for their implementation
02/04/2024

The need:

The encryption systems currently used e.g. RSA, DSA, ECC (and generally, systems based on number-factorization, discrete-logarithm and elliptic-curves) can be cracked by quantum computers (P. Shor 1994). Because there are secrets (military, medical, financial, industrial, etc.) those who one wants to keep them for at least 50 years and since it is expected that within 10-15 years, there will be quantum-computers with the required computing-power and since the communication traffic that went through public-channels can be stored in memory - this information may be revealed before the expiration expected-time. Quantum-computers will be available (at least in their early years), but to governments and large corporations and therefore ordinary people will be exposed and transparent to governments and giant corporations. Therefore, the ordinary person must be provided with effective protection against attacks affordable by quantum-computers.

Features of the proposed systems:

1. The systems are based on problems proved to be in the complexity-class *NP-complete* (Quadratic Matrix Equations Over Finite Fields) and under the widespread belief that $BQP \cap NP-complete = \emptyset$ (where *BQP* = Bounded-Error Quantum Polynomial-Time Problems), they are considered as having proved security.
2. The systems have the forward-security feature, that is, all encryption in the systems involves random bits, so that future use of the same information will be encrypted with different random bits in such a way that the keys cannot be revealed from known encryption / decryption pairs and no original information can be revealed - without knowing what the keys are - from linear or differential attacks, etc. that assume knowledge of encryption / decryption pairs and stationarity of the encryption systems. Thus, the lifetime of the keys can be infinite in principle.
3. In systems that are using random bits, sometimes decryption errors occur or the decryption process fails - with low probability but not with zero probability - and therefore it is sometimes necessary to send the information again, when the decryption was not done accurately or when the decryption was not successful. The proposed systems do not have such a problem as they are constructed in such a way that they are always reversible with a one-to-one relation between the encrypted information and the plain text.

4. In the context of digital signatures, there are attacks based on having multiple solutions for the quadratic system on which the digital-signature is built and therefore it is sufficient for an attacker to find one other alternative solution for documents he is interested in and forge a signature - even without knowing the secret key. In the proposed systems there is a single solution for the quadratic system and therefore the systems are immune to such attacks.
5. As far as I know, today there are no asymmetric-encryption systems using public-key (i.e. Post-Quantum Public-Key Cryptography) which are also immune to attacks by quantum computers - with proven immunity. Although a number of symmetric-encryption systems using a secret-key and digital-signature systems with proven immunity to attacks by quantum-computers are known today, the encryption systems offered are faster relative to the plain text size, with a small key size - relative to the level of security.
6. For similar systems - the level of immunity is unknown as they are not chosen completely randomly - as they must contain a certain structure - so that they can be reversible and the particular system selected may not be sufficiently immune and therefore vulnerable to attack. The proposed systems although have a known structure for guaranteeing the reversibility, are chosen randomly.
7. Regarding the systems efficiency: the systems are based on simple matrix operations over the finite field \mathbf{F}_2 (where the addition operation there is XOR between bits and the multiplication operation there is AND between bits) and

can therefore be implemented simply and immediately without the need for tables to store the addition and multiplication operations or the need of using algorithms for these operations as is needed in large fields. The systems can be implemented over any other finite field, if needed.

8. Most of the system's operations can be performed by parallel algorithms with optimal-work and optimal-time and therefore the systems achieve fantastic runtime (encryption-time, decryption-time and key-generation-time) and are expected to achieve optimal-cost - relative to the required security level and relative to source size.
9. All 3 proposed systems (asymmetric-encryption using public-key, symmetric encryption using shared secret-key and digital-signature) can be implemented on a single platform in an integrated implementation and therefore costs are expected to be reduced with respect to systems that use different encryption systems for the above functionalities.

Remark: Disclosure of the systems will be made only after signing a confidentiality document!

Document of requirements for the implementation of the systems:

1. Market survey, market value.
2. Finding investors.
3. Collaboration with companies.
4. International patent registration for the theoretical method as IP (Intellectual Property) and for the realization in a chip.
5. Development of the algorithms on FPGA (Field-Programmable Gate-Array) first, to test the feasibility of obtaining theoretical run-times and possibly also improve them by working with non-standard computation models that include different operators from AND and XOR and by using multiplexed operators as above. Improving running-times by improving memory readings and writings. Improving running-times by identifying additional operations that can be done in parallel - as much as possible.
6. The development of the algorithms on FPGA will be done on one platform that will combine the common algorithms for the different methods such as: multiplication of matrices, inversion of matrices and generation of keys.
7. Comparison of performance (in terms of encryption-time, decryption-time, key-generation-time, encrypted-message-size versus source-size, key-size, number of operators, cost, etc.) vs. immunity level with "similar" systems such as UOV, Rainbow and other systems.
8. At the stage when the system is working on FPGA, immunity tests must be performed as usual by 500 hackers who will try to crack the system. For this purpose, it is needed to work with factors such as: Microsoft Research, Google New-Hope, Open Quantum-Safe Project.
9. International recognition must be obtained from factors such as: NIST (National Institute for Standards and Technology), European Telecommunication Standards Institute (ETSI), Institute for Quantum Computing, European Commission for Post-Quantum Cryptography.
10. Implementation of the systems on chips and miniaturized chips - for medical and military uses.

11. Finding potential customers such as: cellular companies, car companies, military and civilian communication companies, medical equipment companies and aircraft building companies.

12. Production line design, marketing and sales.

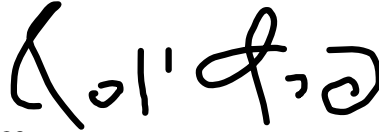
Dr. Yossi Peretz,

Department of Computer Science,

Lev Academic Center, Jerusalem.

Email: yosip@g.jct.ac.il

Tel: 972-50-7496244

A handwritten signature in black ink, appearing to read 'Yossi Peretz' in a stylized, cursive script.