Post-quantum Encryption System for 5G

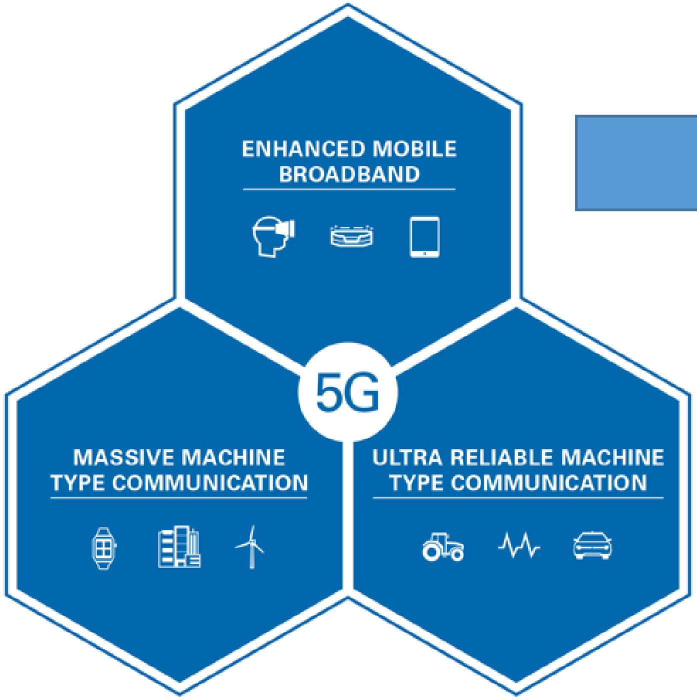
Maksim Iavich

კავკასიის უნივერსიტეტი
CAUCASUS UNIVERSITY

DEEPSEC

SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Actuality of the research


ENHANCED MOBILE BROADBAND
5G
MASSIVE MACHINE TYPE COMMUNICATION
ULTRA RELIABLE MACHINE TYPE COMMUNICATION

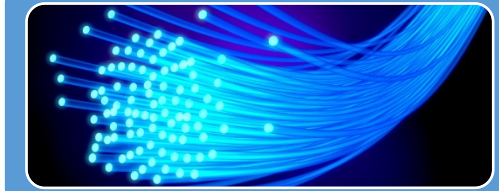
5G WORLD

Actuality of the research

5G is more vulnerable to cyber-attacks in the following

Because the network also operates on software, protecting software vulnerabilities within the network is not an efficient means to provide security.

Spectrum Sharing capability, where various streams of information share the bandwidth in slices, and every slice has its varying degree of cyber risk.

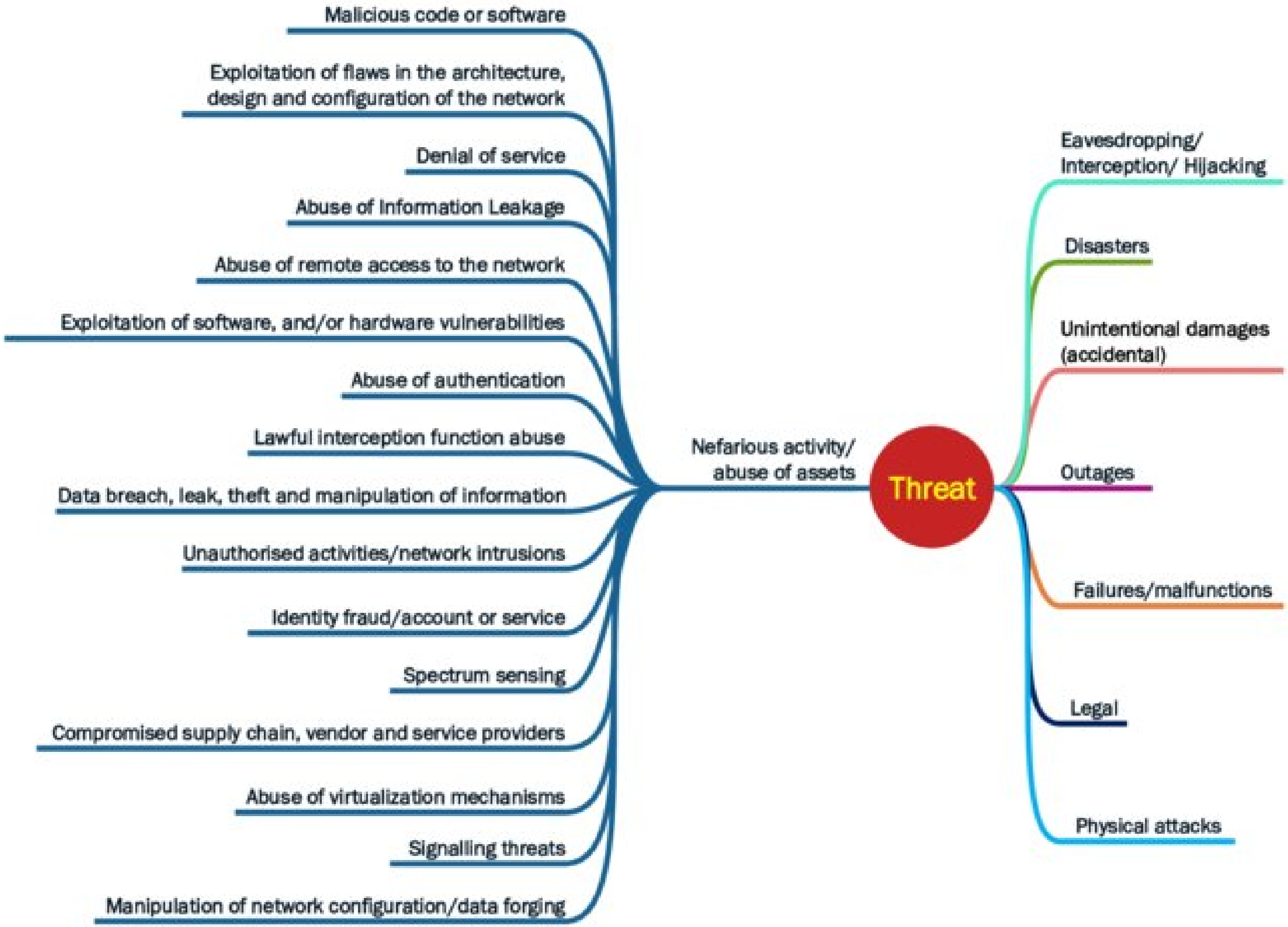


Additional venues of attack are created due to the expansion of bandwidth that makes 5G possible.

The last threat is caused by several devices that are part of the system.

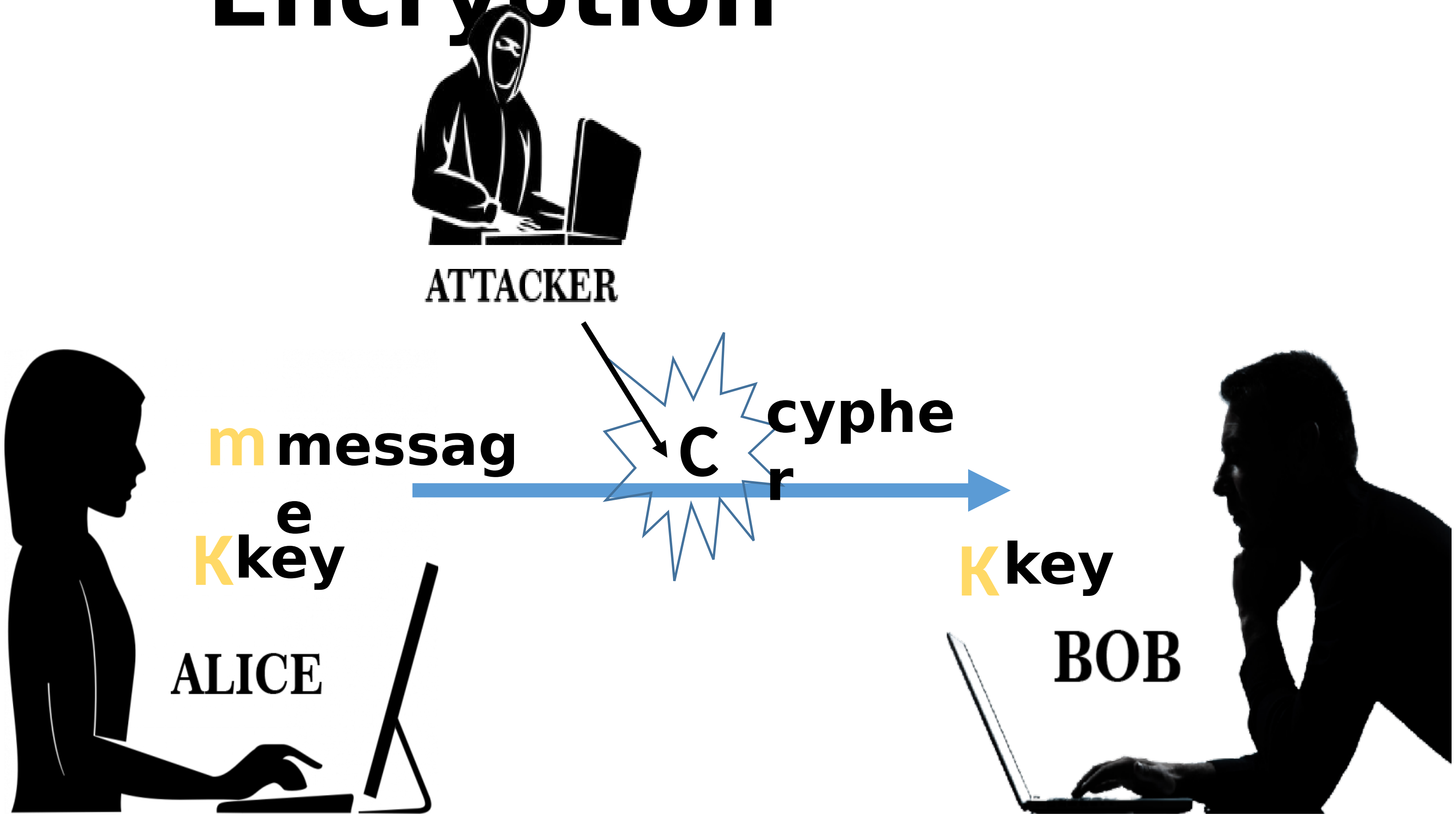
Actuality of the research

New 5G Threat Landscape


Threat
Nefarious activity/ abuse of assets
Malicious code or software
Exploitation of flaws in the architecture, design and configuration of the network
Denial of service
Abuse of Information Leakage
Abuse of remote access to the network
Exploitation of software, and/or hardware vulnerabilities
Abuse of authentication
Lawful interception function abuse
Data breach, leak, theft and manipulation of information
Unauthorised activities/network intrusions
Identity fraud/account or service
Spectrum sensing
Compromised supply chain, vendor and service providers
Abuse of virtualization mechanisms
Signalling threats
Manipulation of network configuration/data forging
Eavesdropping/ Interception/ Hijacking
Disasters
Unintentional damages (accidental)
Outages
Failures/malfunctions
Legal
Physical attacks

The 3rd Generation Partnership Project (3GPP) offered a standard for 5G networks. It contains the identity protection scheme, which addresses the important privacy problem of permanent subscriber-identity disclosure. This offer contains the identification stage, which is followed by providing the security context between service providers and mobile subscribers using the authenticated key agreement with the symmetric key. 3GPP offers to protect the identification stage by means of a public-key scheme. They offer to use Elliptic Curve Integrated Encryption Scheme (ECIES). The offered scheme is not secure against the attacks of quantum computers. It is important to integrate the quantum resistant scheme to 5G networks.

Private Key Encryption



$c := \text{Enc}_k(m)$

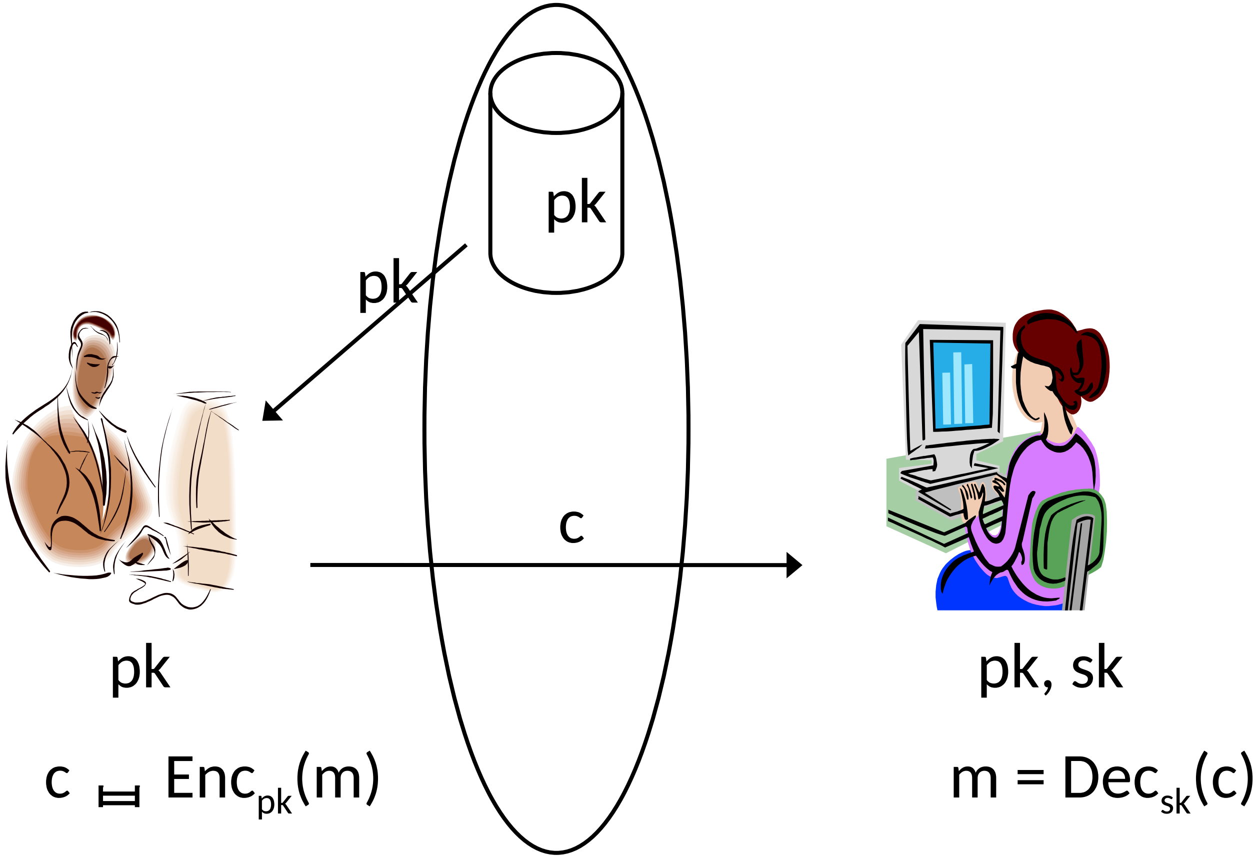
Encryption

$\text{Dec}_k(\text{Enc}_k(m)) = m$

$m := \text{Dec}_k(c)$

Decryption

Public-key encryption



pk

pk

c

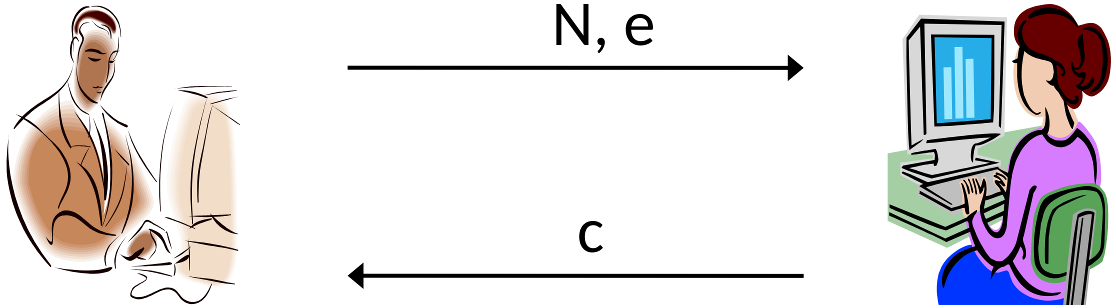
pk

pk, sk

$c \leftarrow \text{Enc}_{pk}(m)$

$m = \text{Dec}_{sk}(c)$

“Plain” RSA encryption



N, e

c

$(N, e, d) \leftarrow \mathrm{RSAGen}(1^n)$

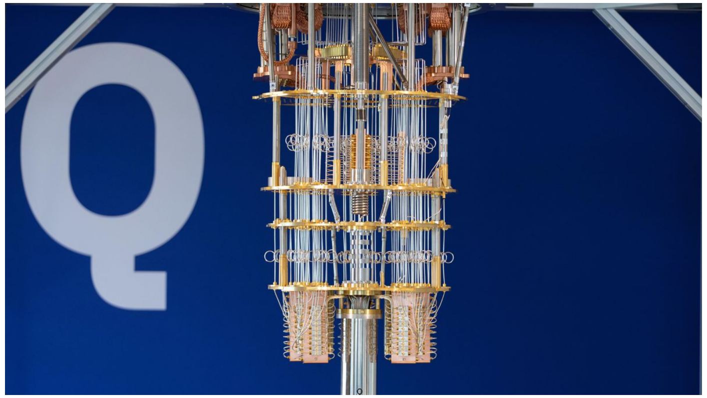
$pk = (N, e)$

$sk = d$

$c = [m^e \bmod N]$

$m = [c^d \bmod N]$

Quantum computers



- GOOGLE Corporation, in conjunction with with the company D-Wave signed contract about creating quantum computers. D-Wave 2X - is the newest quantum processor, which contains physical qubits.
- Each additional qubit doubles the data search area, thus is also significantly increased the calculation speed. Quantum computers will destroy systems based on the problem of factoring integers (e.g., RSA). RSA cryptosystem is used in different products on different platforms and in different areas.

RSA system is widely used in operating systems from Microsoft, Apple, Sun, and Novell. In hardware performance RSA algorithm is used in secure phones, Ethernet, network cards, smart cards, and is also widely used in the cryptographic hardware. Along with this, the algorithm is a part of the underlying protocols protected Internet communications, including S / MIME, SSL and S / WAN, and is also used in many organizations, for example, government, banks, most corporations, public laboratories and universities.

News from Google

- Google made a huge revelation on October 23, 2019, when it announced that it had reached something called “quantum supremacy.” Via an article in the journal Nature, Google said their quantum computer, called Sycamore, solved a particularly difficult problem in 200 seconds. For comparison, Google said the world’s current fastest classical computer — one called Summit owned by IBM that’s as big as two basketball courts — would take 10,000 years to solve that same problem. This is what “quantum supremacy” means. It’s when a quantum computer — one that runs on the laws of quantum physics as opposed to the classical computers we’re familiar with (i.e. phones and laptops), which run on classical physics like Newton’s laws of motion — does something that no conventional computer could do in a reasonable amount of time.

IBM’s answer

- IBM responded to Google’s news to say that actually, Summit could solve the quantum computers’ problem in two and a half days — not 10,000 years as Google had suggested. In this episode of Recode’s Reset podcast, host Arielle Duhaime-Ross and Kevin Hartnett, a senior writer for the math and physics magazine Quanta, break down exactly what quantum computing is and why Google dunking on IBM both was and wasn’t a huge deal.

Chinese researchers achieve quantum advantage in two mainstream routes

- Chinese research teams have made marked progress in superconducting quantum computing and photonics quantum computing technology, making China the only country to achieve quantum computational advantage in two mainstream technical routes, while the US has only achieved a "quantum advantage" in superconducting quantum computing, analysts say.
- "Zuchongzhi 2.1," is 10 million times faster than the current fastest supercomputer and its calculation complexity is more than 1 million times higher than Google's Sycamore processor. It's the first time that China has reached quantum advantage in a superconducting quantum computing system.

- Pan's team also built a new light-based quantum computer prototype, "Jiuzhang 2.0," with 113 detected photons, which can implement large-scale Gaussian boson sampling (GBS) 1 septillion times faster than the world's fastest existing supercomputer, according to the Xinhua News Agency.

  Yuan said that the number of detected photons for "Jiuzhang 2.0" increased to 113 from the previous 76 when the quantum computer prototype "Jiuzhang" first came out, which was a major technical breakthrough, as the difficulty increases exponentially with each additional detected photon.

  The light-based quantum computer prototype "Jiuzhang" was built in December 2020, led by Pan and Lu, and demonstrated a quantum advantage.

RSA ALTERNATIVES

Hash-based Digital Signature Schemes: One of RSA alternatives are Hash-based Digital Signature Schemes. The safety of these systems depends on the security of cryptographic hash functions.

A code-based public-key encryption system: McEliece example. In this system the public key is (G_{new}, t), and the private key is (S, G, P), where G is k x n generator matrix for the code C. C is random binary (n, k)-linear code, that is capable to improve t errors. N is the number of code words, k is dimension of C. S is a random k x k binary nonsingular matrix. P is a random n x n binary permutation matrix. $G_{new\ =}$ S * G * P; k x n matrix. To encrypt the message we must encrypt message m as a binary string with the length k; cyp = m x G_{new}; is generated random n-bit error vector v with the weight t. The cypher is calculated as c= cyp+v. For decoding is calculated cyp = c*P^{-1}; Using decryption algorithm of C is calculated m_{new}= m*S => m= m_{new}*S^{-1}

RSA ALTERNATIVES

- **Lattice-based Cryptography:** proofs are based on worst-case hardness.
- **Multivariate public key cryptosystem – MPKCs:** have a set of(usually) quadratic polynomials over a finite field. Security assumption is backed by the NP-hardness of the problem to solve nonlinear equations over a finite field.

Successful attacks

- To date are already found successful attacks on this crypto system.
- The Ph.D. candidate of Dublin City University (DCU) Neill Costigan with the support of Irish Research Council for Science, Engineering and Technology (IRCSET), together with professor Michael Scott, Science Foundation Ireland (SFI) member successfully were able to carry out an attack on the algorithm. To do this they needed 8,000 hours of CPU time. In the attack representatives of four other countries took part. Scientists have discovered that the initial length of the key in this algorithm is insufficient and should be increased.
- This system cannot be also used to encrypt the same message twice and to encrypt the message when is known it’s relation with the other message.

- Should be noted the importance of efficiency spectrum. To date experts have reached quite good results in the speed algorithm processing. According to the investigation results it becomes clear that the proposed post-quantum cryptosystems are relatively little effective. Implementation of the algorithms requires much more time for their processing and verification.
- Inefficient cryptography may be acceptable for the general user, but it cannot be acceptable for the internet servers that handle thousands of customers in the second. Today, Google has already has problems with the current cryptography. It is easy to imagine what will happen when implementing crypto algorithms will take more time.
- The development and improvement of modern cryptosystems will take years. Moreover, all the time are recorded successful attacks on them. When is determined the encryption function, and it becomes standard, it needs the appropriate implementation of the corresponding software, and in most cases, hardware.

- During the implementation it is necessary to ensure not only correct work of the function and the speed of its efficiency, but also to prevent any kind of leaks. Recently have been recorded successful «cache-timing» attacks on RSA and AES system, as a result of that Intel has added the AES instructions to its processors.
- McEliece system is vulnerable to attacks, related to side channel attacks. Was shown the successful timing attack on Patterson algorithm. This attack does not detect the key, but detects an error vector that can successfully decrypt the message cipher.
- As we can see, for the creation and implementation of safe and effective post-quantum cryptosystems it is necessary to fulfill the rather big work. From the foregoing it is clear that today we are not ready to transfer cryptosystems into post-quantum era. In the near future we cannot be sure in the reliability of the systems.

RSA ALTERNATIVES – HASH BASED

- Traditional digital signature systems that are used in practice are vulnerable to quantum computers attacks. The security of these systems is based on the problem of factoring large numbers and calculating discrete logarithms. Scientists are working on the development of alternatives to RSA, which are protected from attacks by quantum computer. One of the alternatives are hash based digital signature schemes. These systems use a cryptographic hash function. The security of these digital signature systems is based on the collision resistance of the hash functions that they use.

LAMPORT–DIFFIE ONE-TIME SIGNATURE SCHEME (KEY GENERATION)

- Keys generation in this system occurs as follows: the signature key X of this system consists of 2n lines of length n, and is selected randomly.
- $X= (x_{n-1}[0], x_{n-1}[1], \dots, x_0[0], x_0[1]) \in \{0,1\}^{n,2n}$
- Verification key Y of this system consists of 2n lines of length n.
- $Y= (y_{n-1}[0], y_{n-1}[1], \dots, y_0[0], y_0[1]) \in \{0,1\}^{n,2n}$
- This key is calculated as follows:
- $y_i[j] = f(x_i[j]), 0<=i<=n-1, j=0,1$
- f – is one-way function:
- $f\colon \{0,1\}^{n} \; \square \; \{0,1\}^{n};$

DOCUMENT SIGNATURE

- To sign a message m of arbitrary size, we transform it into size n using the hash function:
- $h(m)=hash = (hash_{n-1}, \dots , hash_{0})$
- Function h- is a cryptographic hash function:
- $h: \{0,1\}^{*} \to \{0,1\}^{n}$
- The signature is done as follows:
- $sig= (x_{n-1}[hash_{n-1}], \dots, x_{0}[hash_{0}]) \in \{0,1\}^{n,n}$
- i-th string in this signature is equals to $x_i[0]$, if i-th bit in sign is equal to 0. The string is equal to $x_i[1]$, if i-th bit in sign is equal to 1.
- Signature length is **n²**.

DOCUMENT VERIFICATION

To verify the signature sig = (sig_{n-1}, …, sig_0), is calculated hash of the message hash = ($hash_{n-1}$, … , $hash_0$) and the following equality is checked:

$$(f(sig_{n-1}), \ldots, f(sig_0)) = (y_{n-1}[hash_{n-1}], \ldots, y_0[hash_0])$$

If the equation is true, then the signature is correct.

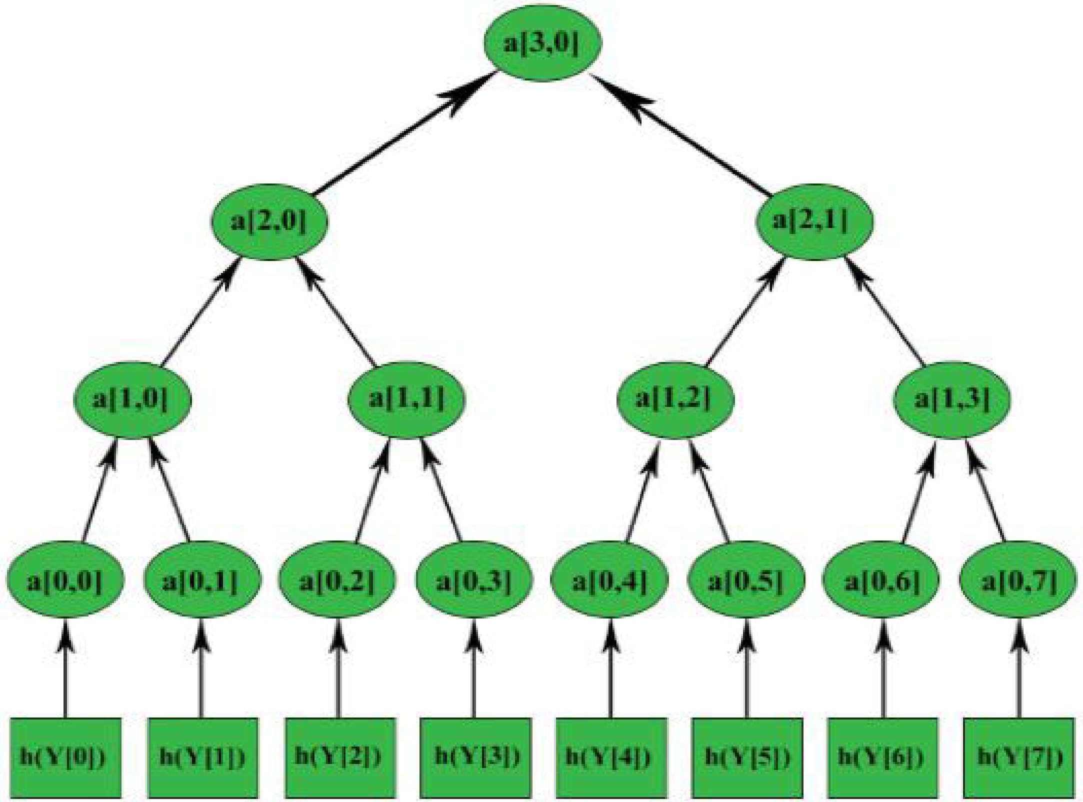
WINTERNITZ ONE TIME SIGNATURE SCHEME.
KEY GENERATION

To achieve security $O(2^{80})$, the total size of public and private keys must be 160∗2∗160 bits = 51200 bits, that is 51200/1024=50 times larger than in the case of RSA. We must also note that the size of the signature in the given scheme is much larger than in the case of RSA. Winternitz One-time Signature Scheme was proposed to reduce the size of the signature.

MERKLE

- One-time signature schemes are very inconvenient to use, because to sign each message, you need to use a different key pair. Merkle crypto-system was proposed to solve this problem. This system uses a binary tree to replace a large number of verification keys with one public key, the root of a binary tree. This cryptosystem uses an one-time Lamport or Winternitz signature scheme and a cryptographic hash function:
- $h:\{0,1\}*$ ▭ $\{0,1\}^{n}$
- **Key generation:** The length of the tree is chosen H>=2, with one public key it is possible to sign 2^H documents. 2^H signature and verification key pairs are generated; X_i, Y_i, $0<=i<=2^H$. X_i- is signature key**,** Y_i- is verification key. $h(Y_i)$ are calculated and are used as the leaves of the tree. Each tree node is a hash value of concatenation of its children.

MERKLE TREE


a[3,0]
a[2,0]
a[2,1]
a[1,0]
a[1,1]
a[1,2]
a[1,3]
a[0,0]
a[0,1]
a[0,2]
a[0,3]
a[0,4]
a[0,5]
a[0,6]
a[0,7]
h(Y[0])
h(Y[1])
h(Y[2])
h(Y[3])
h(Y[4])
h(Y[5])
h(Y[6])
h(Y[7])

- Another alternatives of post-quantum systems are **systems based on lattices.**
- **Collision resistant hash functions** based on lattices were proposed. Ajtai suggested the family of one-way functions , the security of which is based on the worst case, the SVP with approximation ratio of n^c, where n is constant. To construct a family of hash functions as parameters are used integers: n, m, q and d.
- Parameter n defines the safety of hash function. The key to a hash function specified by the matrix M, chosen uniformly from $Z_q^{n\times m}$. Hash function is
- $f_M : \{0, . . . , d-1\}^m \rightarrow Z_q^n$. The function maps mlogd bits to nlogq bits for input compression, m> log q / log d. This hash function is very easy to implement, because we use only addition and multiplication modulo q, which size is O (log n). But should be noted the problem of the effectiveness of these functions, the size of their key grows quadratically in n, so these functions are ineffective. Due to the attacks on these functions by combinatorial method , for the security of 100-bit, you need to use a key of 500,000 bits size.

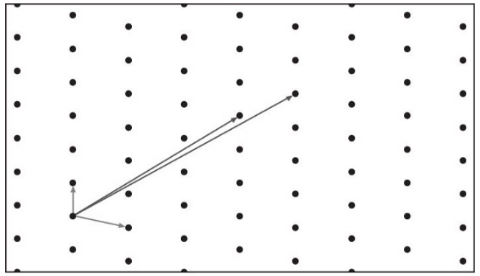


Figure 5-11 Lattice-based cryptography

- To increase effectiveness, matrix M can be change by block matrix, each block of which is circulant matrix:
- $M = [M^{(1)} \mid . . . \mid M^{(m/n)}]$.
- This structure reduces the size, required for key storage, from nm to m elements and also reduces the execution time of the algorithm required to calculate the product of matrix on vector M mod q.
- Changing the structure of the matrix let to find the collision. It can be solved, using **a ideal matrixes**.
- As a key are taken m/n vectors $a_1, . . . ,a_{m/n}$, chosen uniformly from Z^n_q. Hashing takes place as following:
- $f_M : \{0, . . . , d - 1\}^m \to Z_q{}^n$, where $f_M(y) = [F\ast a_1 \mid . . . \mid F\ast a_{m/n}]y \bmod q$.
- As M is taken as a block matrix with structured blocks $M^{(i)} = F\ast a^{(i)}$.
- For security, based on the "worst case", vector f must satisfy the following conditions:
- 1. for two unit vectors u_1, u_2 vector $[F\ast u_1]\, u_2$ must have a small norm.
- 2. The polynomial $f(x) = x^n + f_n x^{n-1} + \cdots + f_1 \in Z[x]$ should be irreducible over integers.

- Values of f, satisfying the both conditions:
- $f = (1, . . . , 1) \in Z_n$, where n + 1 is prime
- $f = (1, 0, . . . , 0) \in Zn$, where n is power of two.

- The family of hash functions **SWIFFT** is an optimized version of the hash function described above, and is rather efficient due to the use of FFT in Z_q. A vector f = (1, 0, . . . , 0) ∈ Zn, where n is a power of two.
- To construct a family of hash functions as parameters are used integers: n, m, d, and the parameter q - prime number such that 2n divides q-1.
- As the key are taken m / n vectors $b_1, . . . ,b_{m/n}$ chosen uniformly from Z^n_q.
- Are accepted m / n vectors: $y_1, . . . , y_{m/n} \in \{0, . . . , d - 1\}^n$
- At the output we get a vector: $\sum_{i=1}^{m/n} b^{(i)} \circ Wy^{(i)} \in Z_n{}^q$; ∘ - component wise vector product.
- $W \in Z^{n\times n}_q$, is invertible matrix in Z_q.
- The hash function transfers a key and input of function into $W^*f_M(y)$ mod q,
- where $M = F\ast a_1 \mid . . . \mid F\ast a_{m/n}]$; $a^{(i)}= W^{-1} b^{(i)}$.
- The multiplicative group of integers modulo q, Z_q^* has an element w of order 2n. For W we will take Vandermonde matrix with elements:
- $w, w^3,w^5, ... , w^{2n-1}$; $W = [w^{(2i-1)(j-1)}]^{n,n}{}_{i=1,j=1.}$
- To avoid attacks by combinatorial method and attacks based on lattice, are recommended the following parameters: n = 64; q = 257; m = 254; d = 2; w = 42; the key size - 8192 bits; input size - 1024 bits; output size - 513 bits.

- Lattice based public key encryption schemes: Goldreich, Goldwasser, and Halevi offered cryptosystem: GGH, which is analogous of the cryptosystem McEliece.
- The private key is the secret matrix S, which columns form a basis of the lattice L, this basis consists of short, almost orthogonal vectors.
- The public key is an open matrix B, which forms a bad basis of the same matrix. Micciancio suggested to use HNF (Hermite Normal Form) of matrix S.
- To encrypt a message, we encrypt it as a vector m, generate a random error vector v and calculate the cipher: c = Bm + v
- v is generated from $\{-p,p\}^n$. p – is security parameter.
- For decryption we compute: $m = B^{-1}S\ [S^{-1}c]$.
- The system can be attacked because of two vulnerabilities:
- 1. error vectors are always very short compared to the lattice vectors. It makes easier to solve the closest vector problem, CVP.
- 2. choice of the error vector. Correcting the second vulnerability, but they all increase the first one.
- So we have to increase the size of the matrix, which makes the system inefficient.
- It should be also noted that this system is not semantically secure.

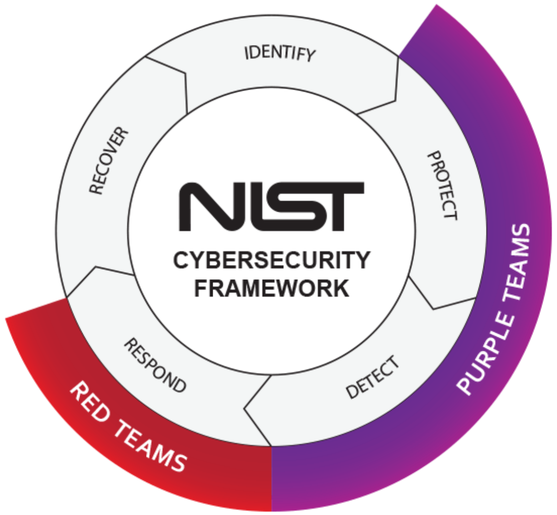
- Hoffstein, Pipher and Silverman offered cryptosystem **NTRU**.
- NTRU is a ring polynomials cryptosystem. Nevertheless, the relationship between the public and private keys determines the grid, which is called a lattice NTRU. It is not necessary to use the lattice during encryption and decryption.
- The private key is a short vector (f , g) $\in Z^{2n}$. Public Key - h = $p[R*f\ ]^{-1}g$ mod q, where p - is a small modulus, R is a cyclic rotation, transforming the vector $(x_1, x_2, \dots , x_n)^T$ to $(x_n, x_1, \dots , x_{n-1})^T$, p - is a big modulus.
- Encryption : a message is encrypted as a vector m $\in \{1,0,-1\}^n$, for randomness is used vector r $\in \{1,0,-1\}^n$, containing
- d_r records - 1, and all the rest - 0. d_r is the boundary of an integer for r.
- Cypher is calculated: c = m + $[R\ast h]r$ mod q
- To decrypt:
- red = $[R*f\ ]c$ (mod q); all red coefficients should lie in the range: [-q / 2; q / 2].
- The message we calculate: m = $[R*f\ ]_p^{-1}$red (mod p);

Bernstein D.J., Chuengsatiansup C., Lange T., van Vredendaal C. (2018) NTRU Prime: Reducing Attack Surface at Low Cost. In: Adams C., Camenisch J. (eds) Selected Areas in Cryptography – SAC 2017. SAC 2017. Lecture Notes in Computer Science, vol 10719. Springer, Cham. https://doi.org/10.1007/978-3-319-72565-9_12

1. NTRU Prime tweaks NTRU to use rings with edited structures;
2. Proposes Streamlined NTRU Prime;
3. A public-key cryptosystem optimized from an implementation perspective;
4. Finds high-security post-quantum parameters for Streamlined NTRU Prime;
5. Optimizes a constant-time implementation of those parameters.

The resulting sizes and speeds show that reducing the attack surface has very low cost.

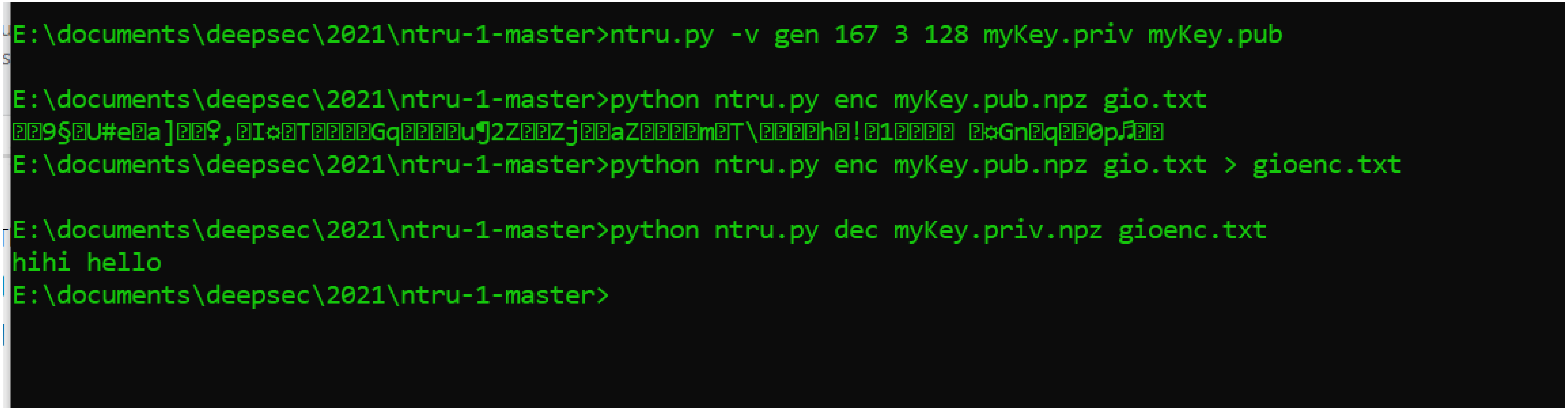
NTRU Prime is a third-round candidate in NIST's
Post-Quantum Cryptography Standardization Proje



Ability to switch to post-quantum cryptography

Classic cryptography ○ ● Post-quantum cryptography

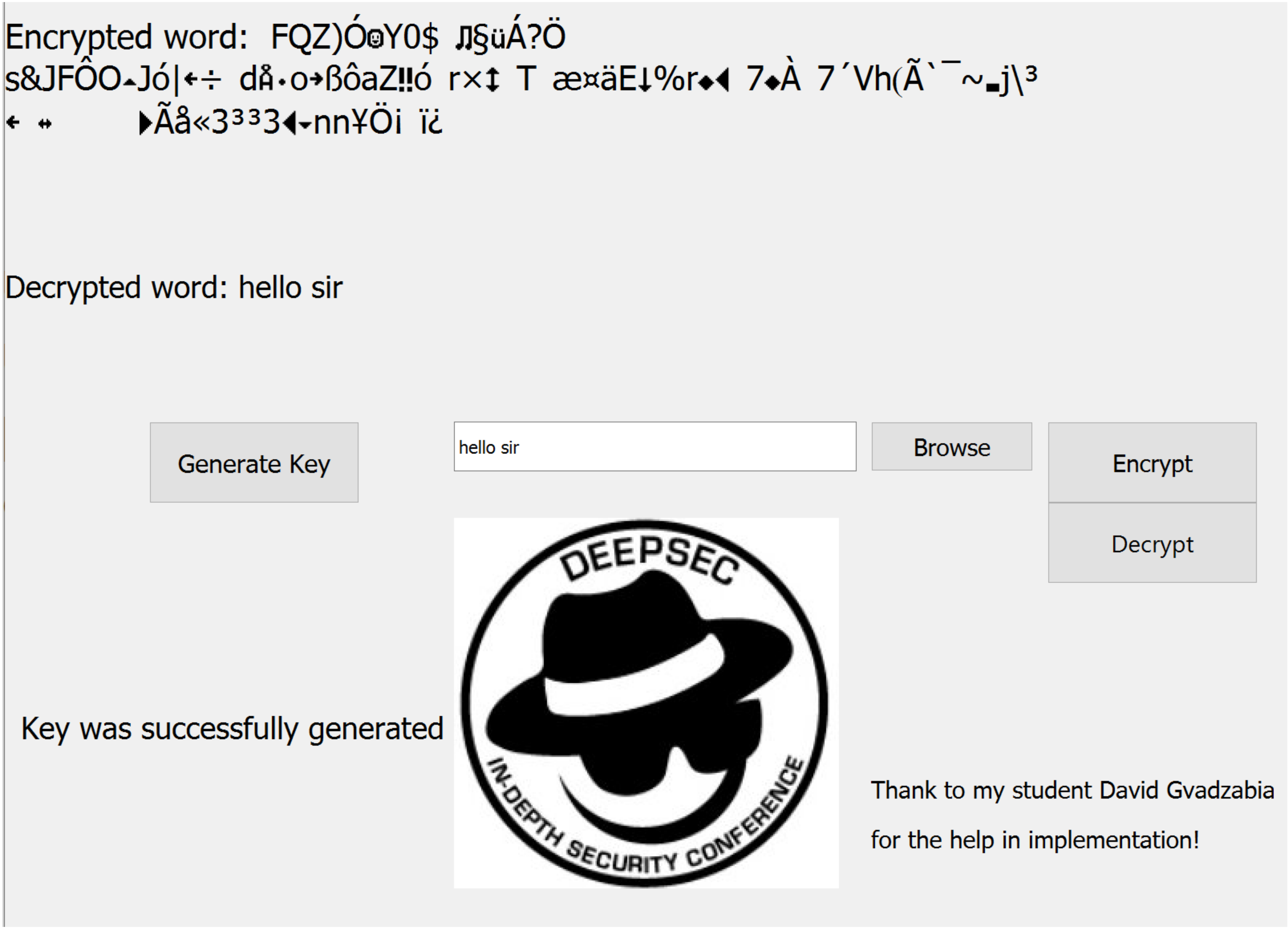
◄ Quantum attack



```
E:\documents\deepsec\2021\ntru-1-master>ntru.py -v gen 167 3 128 myKey.priv myKey.pub

E:\documents\deepsec\2021\ntru-1-master>python ntru.py enc myKey.pub.npz gio.txt
⍰⍰9§⍰U#e⍰a]⍰⍰♀,⍰I☼⍰T⍰⍰⍰⍰Gq⍰⍰⍰⍰u¶2Z⍰⍰Zj⍰⍰aZ⍰⍰⍰⍰m⍰T\⍰⍰⍰⍰h⍰!⍰1⍰⍰⍰⍰ ⍰☼Gn⍰q⍰⍰0p♫⍰⍰
E:\documents\deepsec\2021\ntru-1-master>python ntru.py enc myKey.pub.npz gio.txt > gioenc.txt

E:\documents\deepsec\2021\ntru-1-master>python ntru.py dec myKey.priv.npz gioenc.txt
hihi hello
E:\documents\deepsec\2021\ntru-1-master>
```



```
Encrypted word:  FQZ)Ó☻Y0$ ♫§üÁ?Ö
s&JFÔO▲Jó|←÷ dÅ∙o→ßôaZ‼ó r×↕ T æ¤äE↓%r♦◄ 7♦À 7´Vh(Ã`¯~▬j\³
← ↔      ►Ãå«3³³3◄▼nn¥Öi ï¿
```

Decrypted word: hello sir

hello sir

Key was successfully generated

Thank to my student David Gvadzabia

for the help in implementation!

Questions?

Maksim Iavich
T. (+995 595) 511355
Email. miavich@cu.edu.ge
www.scsa.ge
www.journal.scsa.ge

კავკასიის უნივერსიტეტი
CAUCASUS UNIVERSITY

DEEPSEC

SCIENTIFIC
CYBER SECURITY
ASSOCIATION