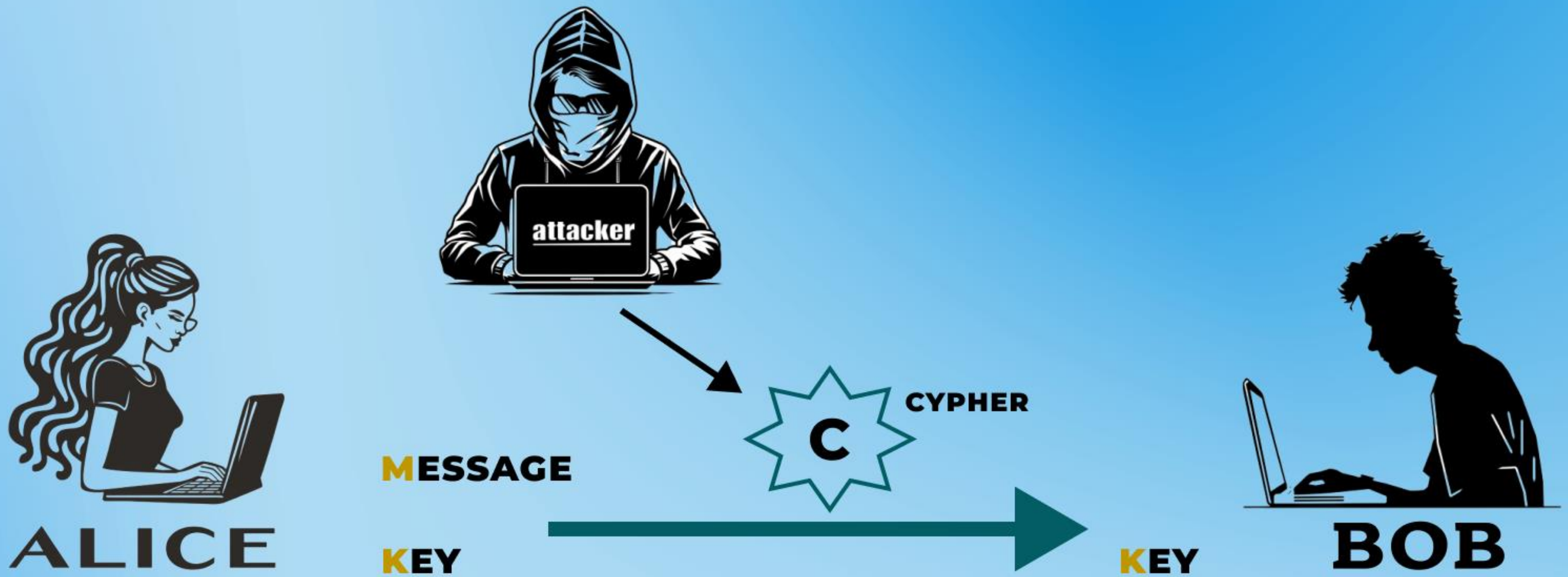
miavich@cu.edu.ge

Is Post Quantum Standard "Kyber" Broken?

Prof. Maksim Iavich

miavich@cu.edu.ge

PRIVATE-KEY CRYPTOGRAPHY



$C := ENC_K(M)$

ENCRYPTION

$DEC_K(ENC_K(M)) = M$

$M := DEC_K(C)$

DECRYPTION

miavich@cu.edu.ge

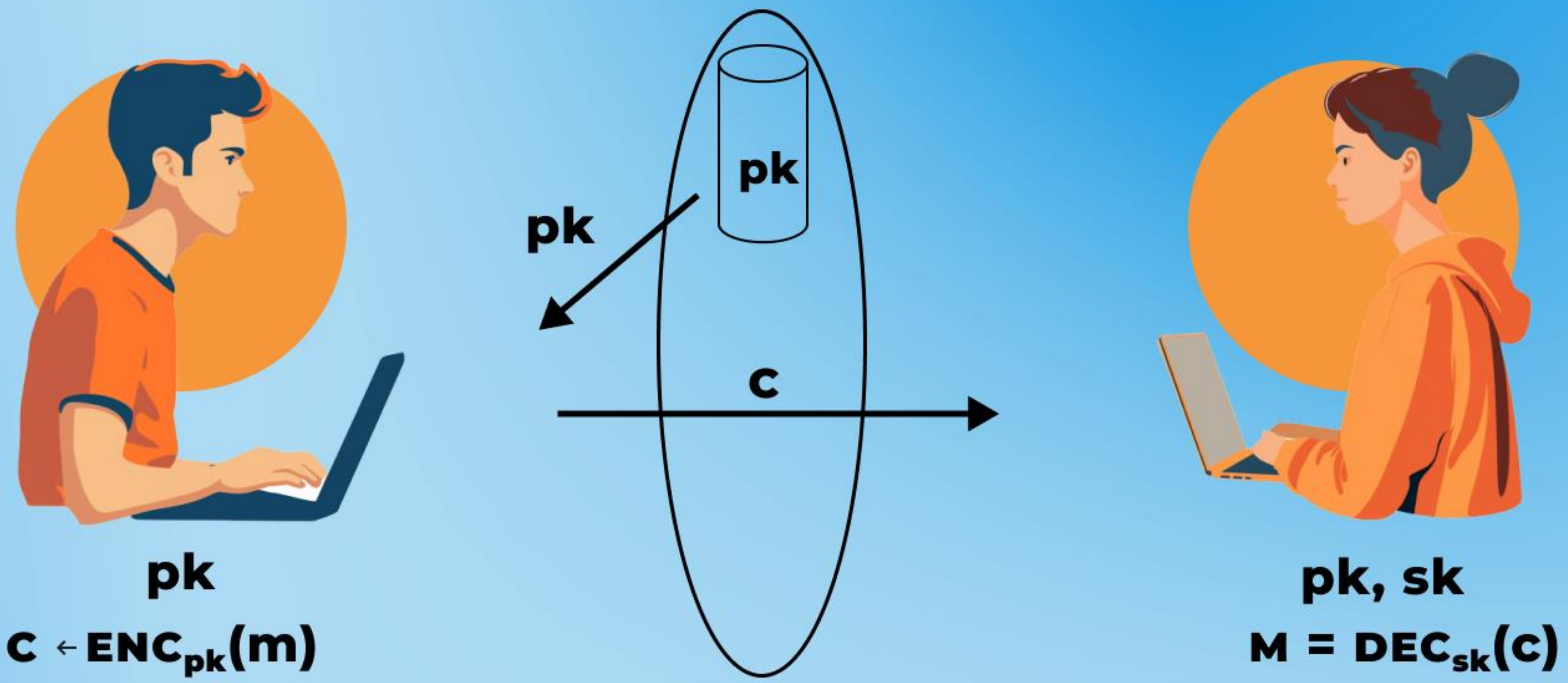
AES

- **Advanced encryption standard (AES)**
  - Standardized by NIST in 2000 based on a public, worldwide competition lasting over 3 years
  - Block length = 128 bits
  - Key length = 128, 192, or 256 bits

- **No real reason to use anything else**

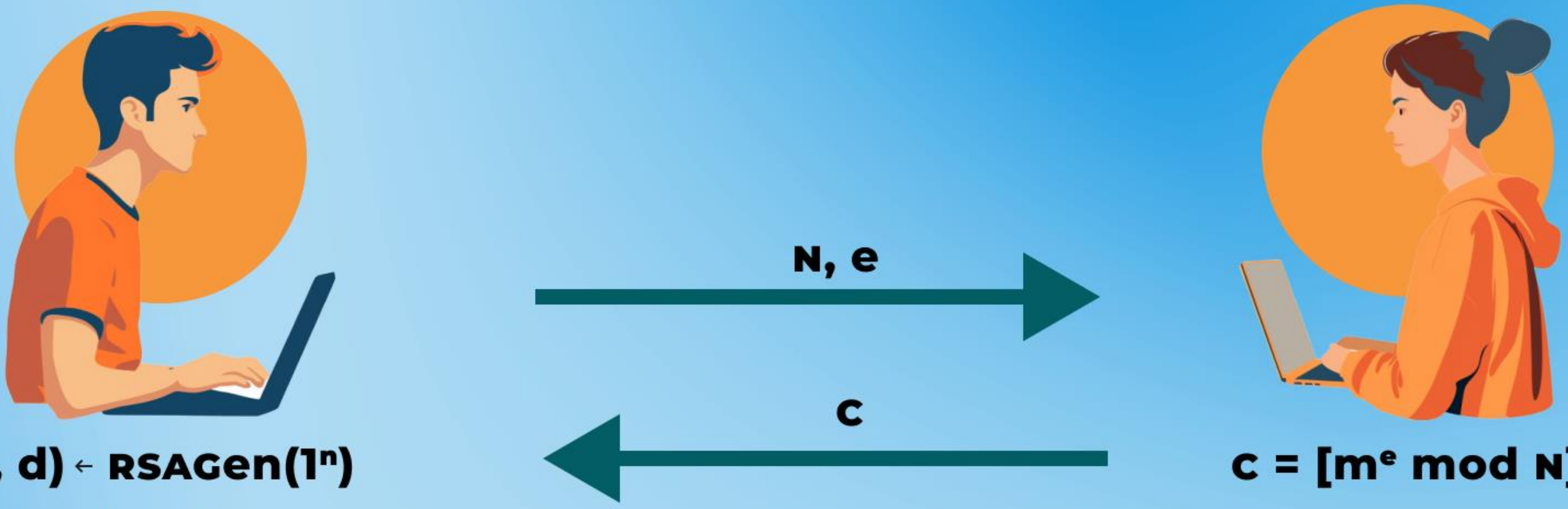
miavich@cu.edu.ge

PUBLIC-KEY ENCRYPTION



miavich@cu.edu.ge

"PLAIN" RSA ENCRYPTION



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

$pk = (N, e)$

$sk = d$

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

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

miavich@cu.edu.ge

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.

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.

Google made a huge revelation on October 23, 2019, when it announced that it had reached something called **"quantum supremacy"**- Sycamore.

In 2021 Chinese research teams have made marked progress in superconducting quantum computing and photonics quantum computing technology. **"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.

miavich@cu.edu.ge

RSA ALTERNATIVES

1. **Hash-based Digital Signature Schemes:** The safety of these systems depends on the security of cryptographic hash functions.
2. **A code-based public-key encryption system:** McEliece example.
3. **Lattice-based Cryptography:** proofs are based on worst-case hardness.
4. **Multivariate public key cryptosystem – MPKCs:** have a set of (usually) quadratic polynomials over a finite field.

miavich@cu.edu.ge

NIST

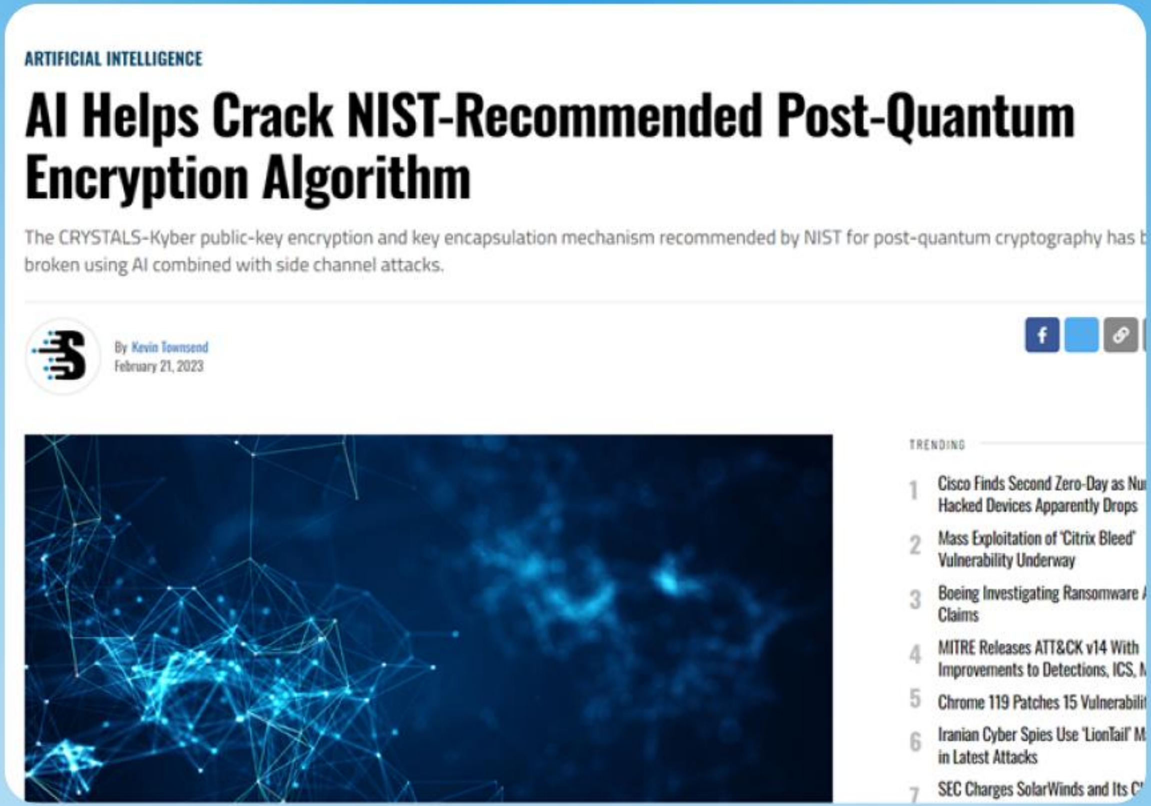
For general encryption, NIST has selected the CRYSTALS-Kyber algorithm

For digital signatures, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+

ATTACK: AI HELPS CRACK NIST-RECOMMENDED POST-QUANTUM ENCRYPTION ALGORITHM

The **CRYSTALS-Kyber** public-key encryption and key encapsulation mechanism recommended by NIST in July 2022 for post-quantum cryptography has been broken.

Researchers from the KTH Royal Institute of Technology, Stockholm, Sweden, **used recursive training AI** combined with side channel attacks.


ARTIFICIAL INTELLIGENCE

AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm

The CRYSTALS-Kyber public-key encryption and key encapsulation mechanism recommended by NIST for post-quantum cryptography has b
broken using AI combined with side channel attacks.

By Kevin Townsend
February 21, 2023

TRENDING

1 Cisco Finds Second Zero-Day as Nu Hacked Devices Apparently Drops
2 Mass Exploitation of 'Citrix Bleed' Vulnerability Underway
3 Boeing Investigating Ransomware Claims
4 MITRE Releases ATT&CK v14 With Improvements to Detections, ICS,
5 Chrome 119 Patches 15 Vulnerabili
6 Iranian Cyber Spies Use 'LionTail' in Latest Attacks
7 SEC Charges SolarWinds and Its

miavich@cu.edu.ge

KYBER: INTRODUCTION

Kyber is an IND-CCA2-secure key encapsulation mechanism (KEM), whose security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices.

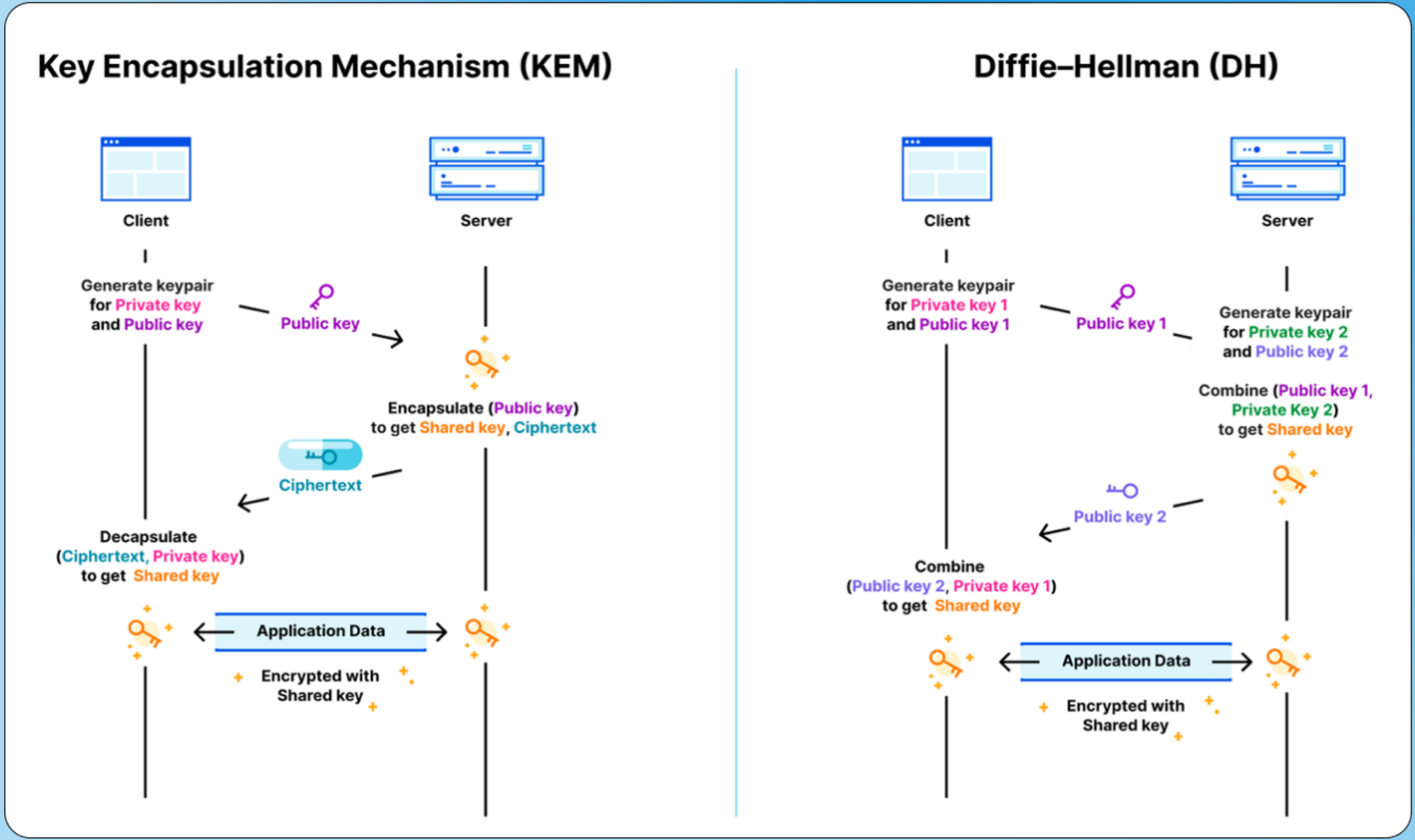
Kyber is one of the finalists in the NIST post-quantum cryptography project.

Specifically, Kyber-512 aims at security roughly equivalent to AES-128, **Kyber-768** aims at security roughly equivalent to **AES-192**, and Kyber-1024 aims at security roughly equivalent to AES-256.

It is recommended to use the Kyber-768 parameter set, which—according to a very conservative analysis—achieves more than 128 bits of security against all known classical and quantum attacks.

miavich@cu.edu.ge

KYBER



miavich@cu.edu.ge

CPAPKE ALGORITHMS

CPAPKE.KeyGen()

seed $_A \leftarrow \mathcal{U}(\{0,1\}^{256})$

$A \leftarrow \mathcal{U}\left(R_q^{k\times k}; seed_A\right)$
$s \leftarrow \mathcal{B}_{\eta_1}\left(R_q^{k\times 1}\right)$
$e \leftarrow \mathcal{B}_{\eta_1}\left(R_q^{k\times 1}\right)$
$b = As + e_{p_1}$
$pk = (seed_A, b), sk = s$
return (pk, sk)

CPAPKE. $\mathbf{Enc}(\boldsymbol{pk} = (\boldsymbol{seed_A}, \boldsymbol{b}), \boldsymbol{m}, \boldsymbol{r})$

$A \leftarrow \mathcal{U}\left(R_q^{k\times k}; seed_A\right)$
$s' \leftarrow \mathcal{B}_{\eta_1}\left(R_\eta^{k\times 1}; r\right)$
$e' \leftarrow \mathcal{B}_{\eta_2}\left(R_q^{k\times 1}; r\right)$
$e'' \leftarrow \mathcal{B}_{\eta_2}\left(R_q^{1\times 1}; r\right)$
$u = \lceil (As' + e') \cdot 2^{d_u}/q \rfloor$
$v = \lceil (b \cdot s' + e'' + encode(m)) \cdot 2^{d_v}/q \rfloor$
return $c = (u, v)$

CPAPKE.Dec(s, $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$**)**

$y = \lceil v \cdot q/2^{d_v} \rfloor - s\lceil u \cdot q/2^{d_u} \rfloor$
$m' = decode(y)$
return m'

miavich@cu.edu.ge

CCAKEM ALGORITHMS

Kyber.KeyGen()

$z \leftarrow \mathcal{U}(\{0,1\}^{256})$

$(pk, s) = \text{CPAPKE.KeyGen()}$

$sk = (s, pk, \mathcal{H}(pk), z)$

return (pk, sk)

Kyber.Encaps $(\boldsymbol{pk})$

$m \leftarrow \mathcal{U}(\{0,1\}^{256})$

$(\hat{K}, r) = \mathcal{G}(m, \mathcal{H}(pk))$

$c = \text{CPAPKE.Enc}(pk, m, r)$

$K = \text{KDF}(\hat{K}, \mathcal{H}(c))$

return (c, K)

Kyber.Decaps $(\boldsymbol{sk} = (\mathbf{s}, \boldsymbol{pk}, \boldsymbol{\mathcal{H}}(\boldsymbol{pk}), \boldsymbol{z}), \boldsymbol{c})$

$m' = \text{CPAPKE.Dec(s, } c)$

$(\hat{K}', r') = \mathcal{G}(m', \mathcal{H}(pk))$

$d' = \text{CPAPKE.Enc}\ (pk, m', r')$

if $c = c'$ then

return $K = \text{KDF}(\hat{K}, \mathcal{H}(c))$

else

return $K = \text{KDF}(z, \mathcal{H}(c))$

end if

miavich@cu.edu.ge

SIDE-CHANNEL ATTACKS

Although **cryptographic systems** appear to be resistant to mathematical assaults, side-channel attacks that use data that is mistakenly exposed when using a device can nevertheless have an impact.

Side-channel attacks are particularly dangerous for embedded systems because they use exposed information, such power usage or electromagnetic radiation.

Side-channel techniques remain a danger even if some contenders for post-quantum cryptography (PQC) are designed to withstand timing attacks. **According to NIST,** continuous research aims to strengthen PQC defense against many side-channel attacks.

miavich@cu.edu.ge

SIDE-CHANNEL ATTACKS

- Researchers study the side-channel attack vulnerability of **lattice-based Key Encapsulation Mechanisms (KEMs)**, specifically side-channel assisted chosen-ciphertext attacks (CCAs).
- Attackers take use of the Fujisaki-Okamoto transform, message encoding/decoding, Number Theoretic Transform (NTT), and error-correcting codes, among other operations within **lattice-based KEMs**.

- In order to find weaknesses, researchers looked into **CRYSTALS-Kyber's decryption algorithm** employing vertical side-channel leakage detection.
- Attackers were able to fully recover keys using basic queries.
- They were able to target clean and m4 schemes in particular by utilizing strategies such **targeted bit flipping and message rotation**.

miavich@cu.edu.ge

SIDE-CHANNEL ATTACKS

Message recovery techniques have to take countermeasures like masking and shuffling into account, along with the possibility of a vulnerability to countermeasure disabling.

In order to emphasize the necessity for more meticulously constructed ciphertexts and adjustments to noise levels in CRYSTALS-Kyber specifications, **researchers devised** a recovered message-based key recovery attack.

miavich@cu.edu.ge

MASKING

- In order to implement this countermeasure, a **secret is divided into** several partially-randomized shares, each of which represents a different percentage of the original secret.
- Masking is the idea of arbitrarily splitting a concealed value into many parts. **At every level,** these shares are treated separately, and the ultimate output is the consequence of combining their individual processing.
- A sensitive variable **x** is divided into $\omega+1$ shares in an ω - order masking,

  $x = x_1 \circ x_2 \circ \ldots \circ x_{(\omega+1)}$

miavich@cu.edu.ge

MASKING

- Arithmetic and Boolean masking are the two options available. Depending on the masking technique, ***"o"*** might represent different operations. In arithmetic masking, ***"o"*** is the arithmetic addition, whereas in Boolean masking, it is the ***XOR***.

  The computations avoid involving $\boldsymbol{x}$ directly by carrying out operations on shares independently, which theoretically prevents side-channel information about $\boldsymbol{x}$ from leaking. Every time a share is executed, **it is randomly assigned**. Randomization is usually accomplished by allocating random masks $x_1, x_2, \ldots, x_\omega$ to ω shares and calc ulating the final share as $x - (x_1 + x_2 + \ldots + x_\omega)$ for arithmetic masking or $x \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_\omega$ for Boolean masking.

miavich@cu.edu.ge

ATTACKS AGAINST CRYSTALS-KYBER

- AI can be used to launch attacks on disguised Kyber implementations; more recently, deep learning and message rotations have been used **to increase attack success rates**.

  The attack focuses on recovering shared keys from cryptographic operations — even in masked implementations — **by using machine learning models built on power traces**.

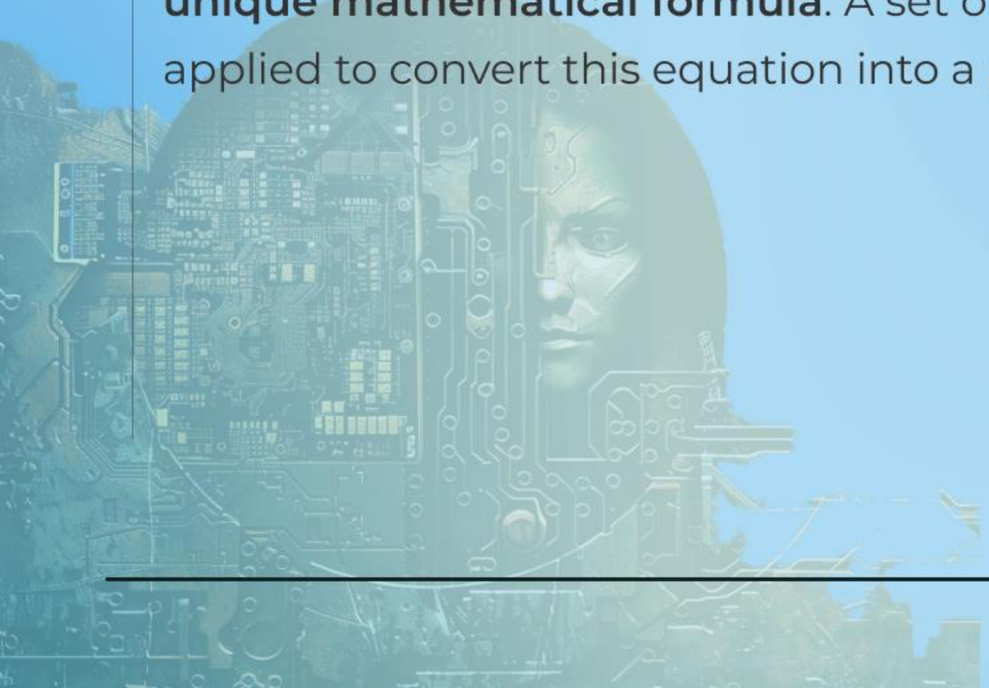
An attacker's chances of successfully retrieving shared keys from masked Kyber implementations can be greatly increased by **recursive learning techniques** and **ciphertext rotation**.

miavich@cu.edu.ge

ATTACKS AGAINST CRYSTALS-KYBER

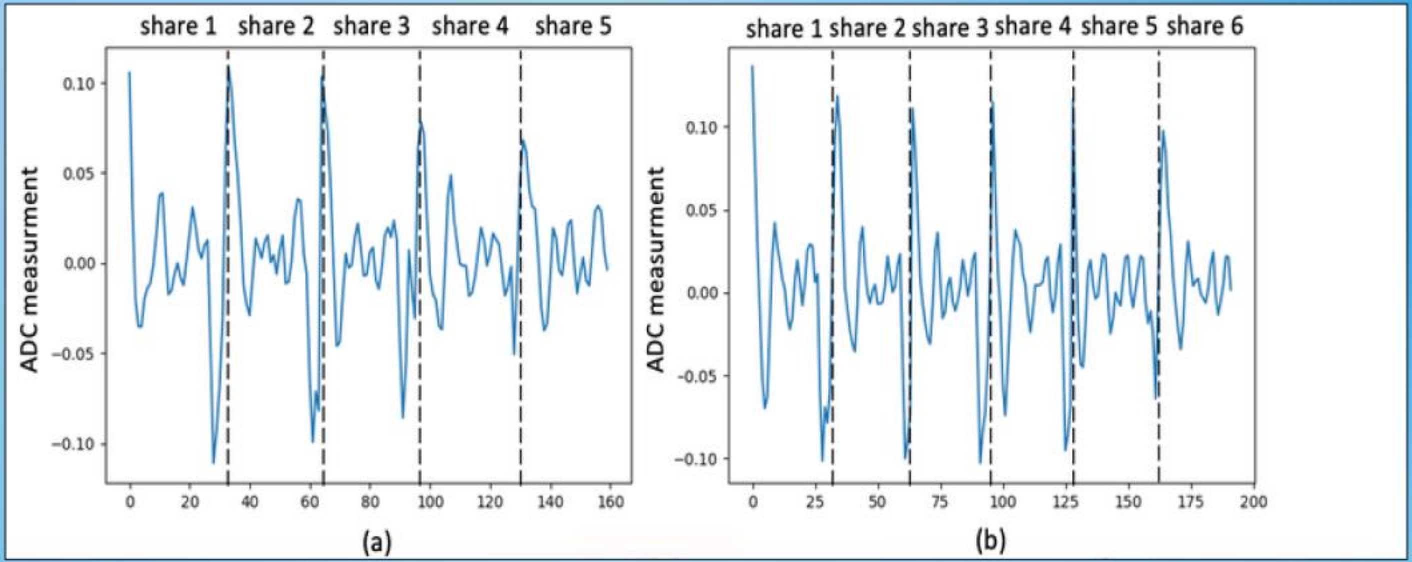
- **The decapsulation step** of the encryption procedure was the attackers' main target. Once the shared key has been obtained, it is verified that it hasn't been altered. The secret key is gradually encoded into a **unique mathematical formula**. A set of rules is then applied to convert this equation into a pattern.

Their method of breaking into the system involved using a unique type of learning that examines the many stages of computer operation. Many examples were provided to it so that it could learn **how the encryption functions**.

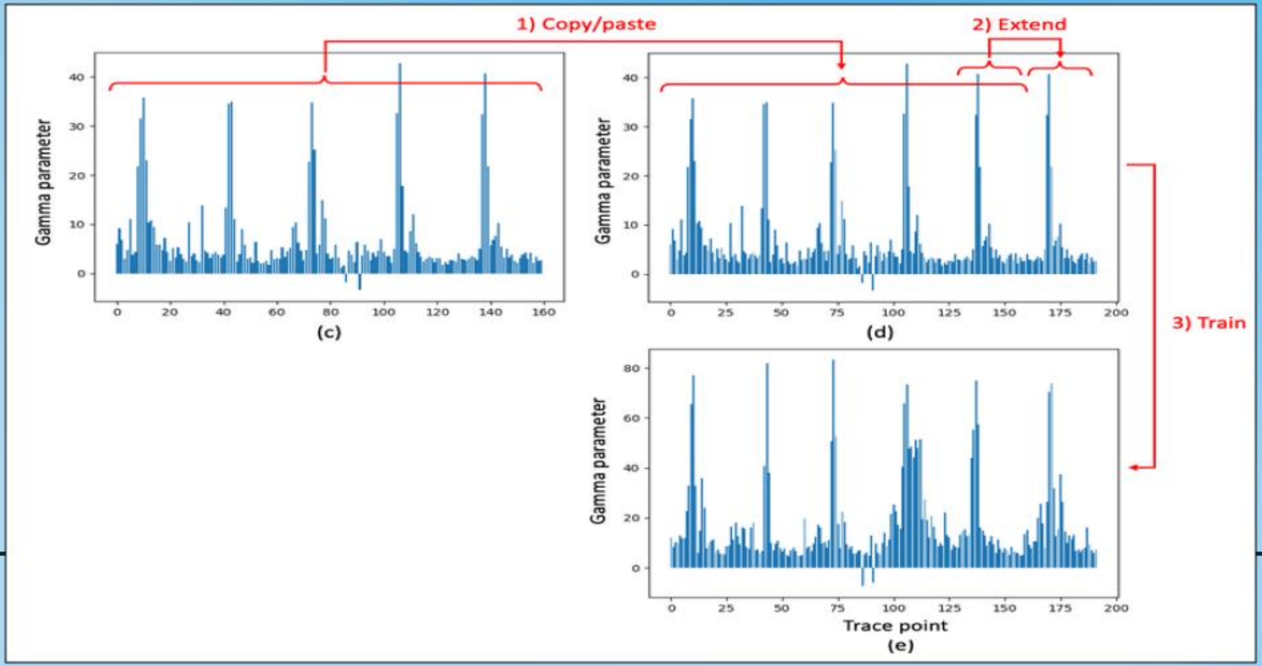


miavich@cu.edu.ge

RECURSIVE LEARNING



(a,b) Power traces given as input to neural networks for attacks on fourth-and fifth-order masked implementations, respectively;
(c) Weights of input Batch Normalization layer after training for fourth-order;
(d) Batch Normalization extended to fifth-order;
(e) Batch Normalization after training for fifth-order.



miavich@cu.edu.ge

CONTRIBUTIONS

- Another novel contribution is a message recovery **method using cyclic rotations**.
- In the procedure that is our attack point, **the first bit** of each message byte leak considerably stronger than the last one.
- The messages are rotated **by manipulating** the corresponding ciphertexts.
- The leakage of message bits in **masked_poly_frommsg()** procedure is non-uniform.
- The first-order masked implementation, the difference between the mean empirical probabilities to recover the bit **0** and the bit **7 is 9%**.

miavich@cu.edu.ge

POINT OF ATTACK

This is the two-shares implementation of the conversion that the paper's attacks.

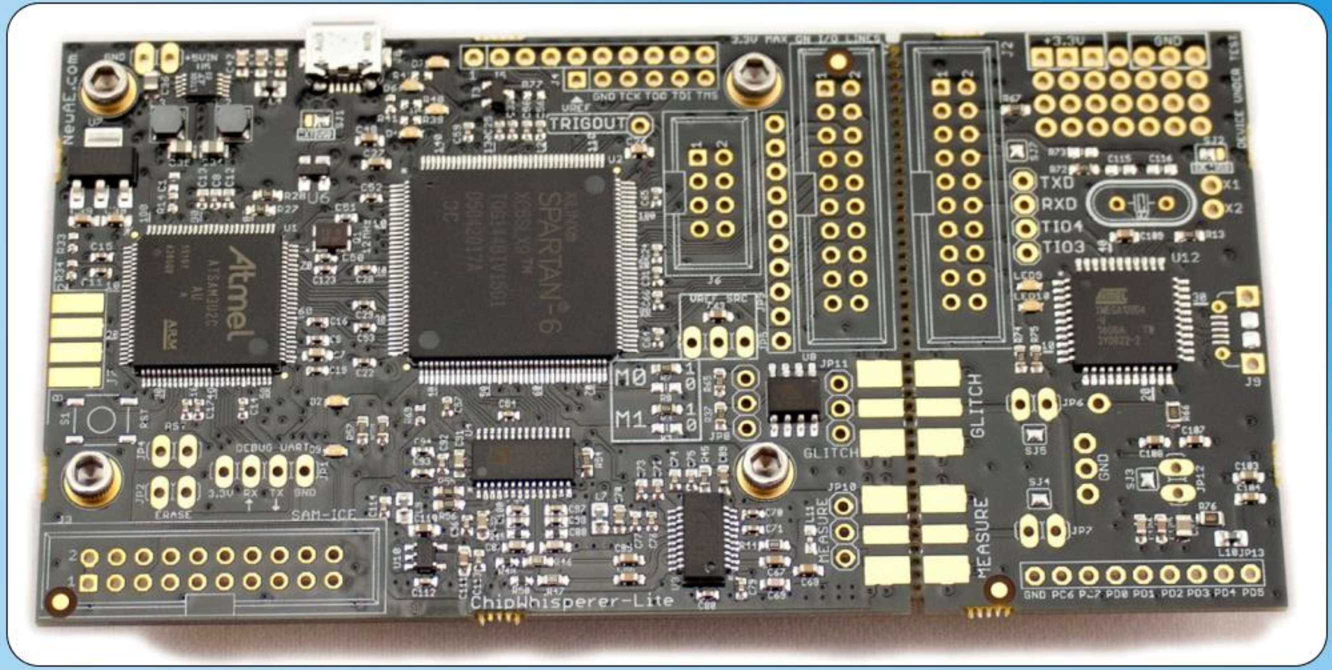
```
void masked_poly_frommsg(uint16 poly[2][256], uint8
msg[2][32])
uint16 c[2];

for (i = 0; i < 32; i++) do
  for (j = 0; j < 8; j++) do
    mask = -((msg[0][i] >> j) & 1);
    poly[0][8*i+j] += (mask&((KYBER_Q+1)/2));
  end for
end for
for (i = 0; i < 32; i++) do
  for (j = 0; j < 8; j++) do
    mask = -((msg[1][i] >> j) & 1);
    poly[1][8*i+j] += (mask&((KYBER_Q+1)/2));
  end for
end for
...
```

Fig. 3: C code of masked_poly_frommsg() procedure of CRYSTALS-Kyber [16].

miavich@cu.edu.ge

EFFECTIVENESS



To test the attack, they use a ***Chipwhisperer-lite board****, which has a Cortex M4 CPU, which they downclock to 24Mhz. Power usage is sampled at 24Mhz, with high 10-bit precision.*

miavich@cu.edu.ge

EFFECTIVENESS

- To train the neural networks **150 000 power traces** are collected for decapsulation of different ciphertexts (with known shared key) for the same KEM keypair.

  This is already a somewhat **unusual situation for a real-world attack**: for key agreement KEM keypairs are ephemeral; generated and used only once. Still, there are certainly legitimate use cases for long-term KEM keypairs, such as for authentication, Hybrid Public Key Encryption(HPKE), and in particular Encrypted Client Hello (ECH).

The training is a key step: different devices even from the same manufacturer can have wildly different power traces running the same code. Even if two devices are of the same model, their power traces **might still differ significantly**.

miavich@cu.edu.ge

CRYSTALS - KYBER IS NOT BROKEN

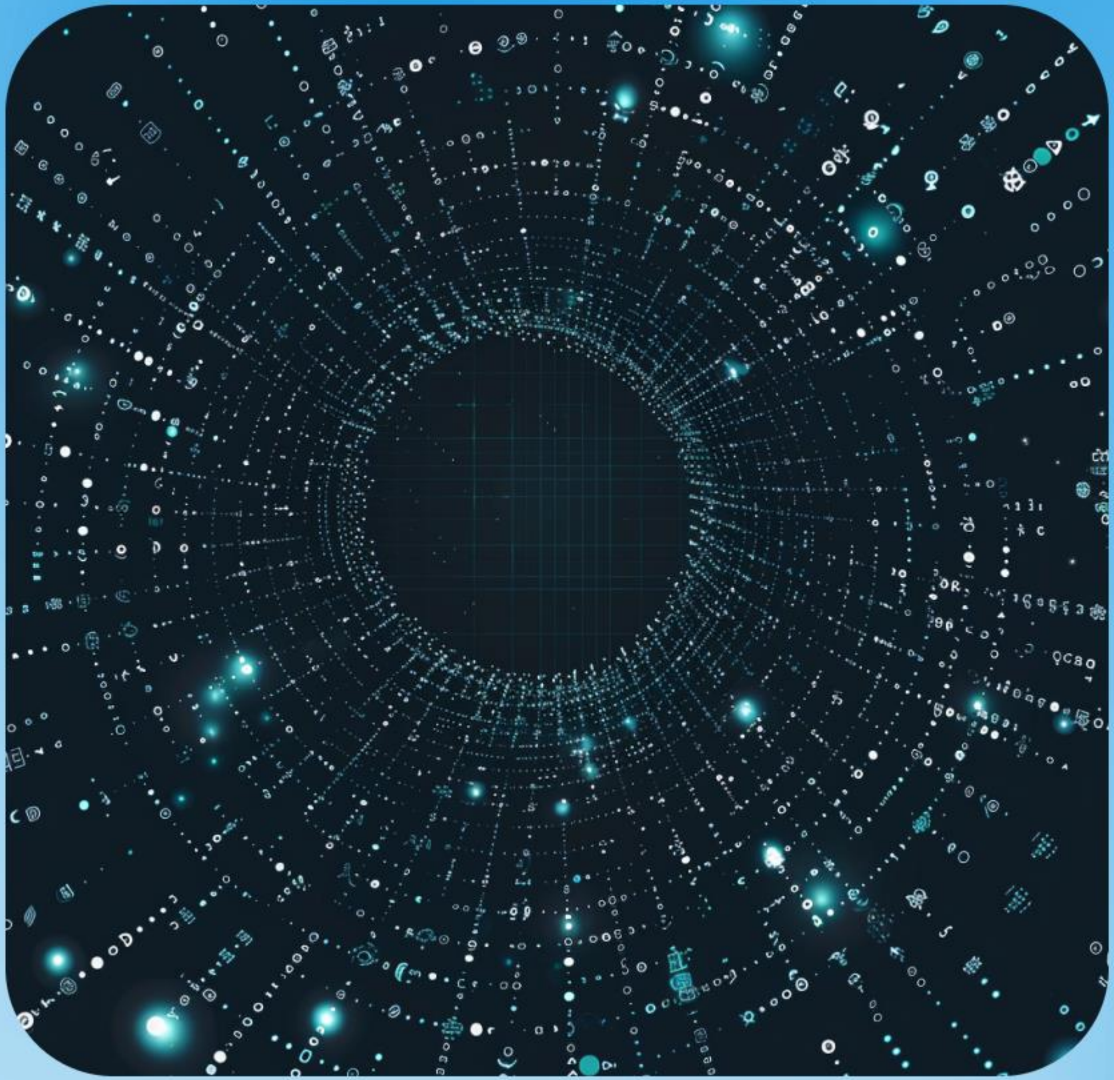
- The attack targeted the implementation and not algorithm
- The attackers implemented some codes
- The attack was successful on the concrete device
- Key Encapsulation Mechanism (KEM) pair was the same

! This attack must be still taken into the account

miavich@cu.edu.ge

COUNTERMEASURES

- **Reducing the duration of the application's secret key** is the best defense against the majority of existing assaults.
- If it were not feasible to repeatedly perform the decapsulation procedure, the attack that was given **would not succeed**. Limiting how many times the same ciphertext may be decapsulated with the same secret key can help achieve this.
- Stronger defenses against power analysis assaults - **duplication with clock randomization approach**, can be used as an alternative.



miavich@cu.edu.ge

ANSWER FROM NIST

CS

csrc-inquiry

Thu, Apr 25, 5:39 PM (4 days ago)

to pqc-comments, me

Maksim Iavich,

Hi again. I received a reply from one of my colleagues and they provided me the following response to send to you. See below:

Response to your inquiry:

The CRYSTALS-Kyber algorithm was selected for standardization in July 2022. Last August we put out a draft specification for it, with the new name of ML-KEM. We hope to publish the final version of the standard for Kyber (aka ML-KEM) this summer.

THANK YOU

Professor Maksim Iavich
miavich@cu.edu.ge