Defending and Attacking Embedded Systems

Modern Cybersecurity in IoT Devices:

Cryptography & Computer Engineering/Sciences

REU Scholars: Isaac Merlin & Emily Wayne
Mentor: Dr. Reza Azarderakhsh
Research Assistants: Aimee Laclaustra, Rabih El Khatib, Daniel Owens

Objective

- Classic Cryptography shift to Post Quantum Cryptography (PQC)
- Modern implementations of cryptography
- National Institute of Science and Technology (NIST)

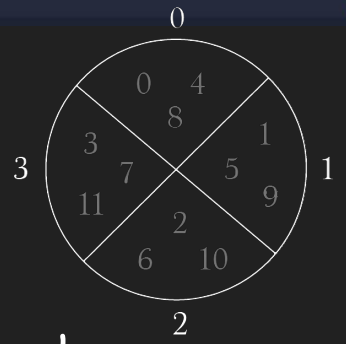
  standardized post-quantum algorithm, KYBER.
- Embedded systems; Hardware and Software Implementations

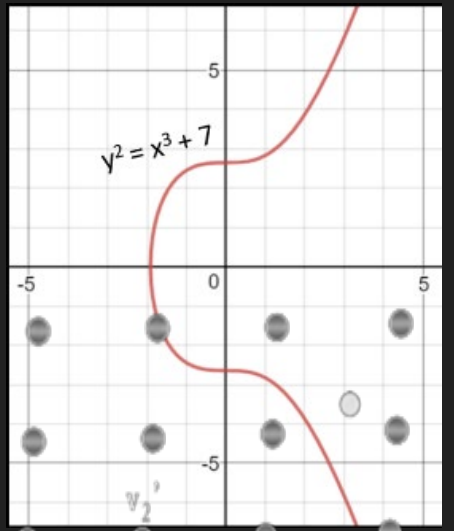
Timeline

```
const bigint256 PRIME          =
{0xffed,0xffff,0xffff,0xffff,0xffff,0xffff,0xffff,0xffff,
0xffff,0xffff,0xffff,0xffff,0xffff,0xffff,0xffff,0x7fff};
                                  // equivalent to 2^255 - 19
```

June - Learning Classical Cryptography

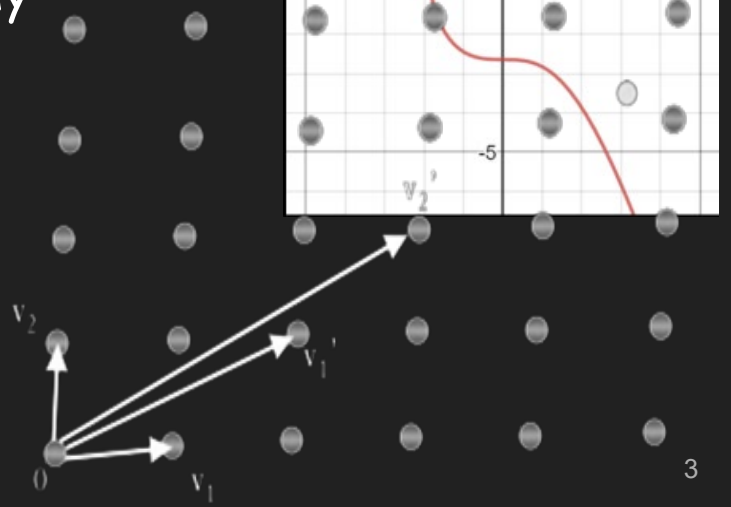
- Modular Arithmetic, Large Primes
- Algorithms, 512-bit integers key size
- Points on Elliptic Curves





July - Researching Post-Quantum Cryptography

- KYBER
- Lattices
- Learning With Errors and its variants
- Side-Channel Attacks
- Interactive KYBER



General Idea of Cryptography

Sender Alice

plaintext

key_A

Encryption algorithm

cipher text

Unsecure channel

Attacker Eve

key_B

Decryption algorithm

plaintext

Receiver Bob

- Read data
- Modify data
- Inject data
- Delete data

Classical Cryptography

- Encrypting a plaintext to create ciphertext, and using a key to decrypt it.
- Most Classical Cryptography is based on the Discrete Logarithm Problem
  - Choose e from group G and integer k. Then compute $e^k = e \circ e \circ \ldots \circ e$ where there are *k* es
  - Given e and e^k, there is no efficient algorithm to find k
- RSA
  - Uses the Discrete Log problem on a multiplication group modulo pq
- Elliptic Curve Cryptography
  - Uses the Discrete Log problem on an elliptic curve group

Attack : Shor's Algorithm

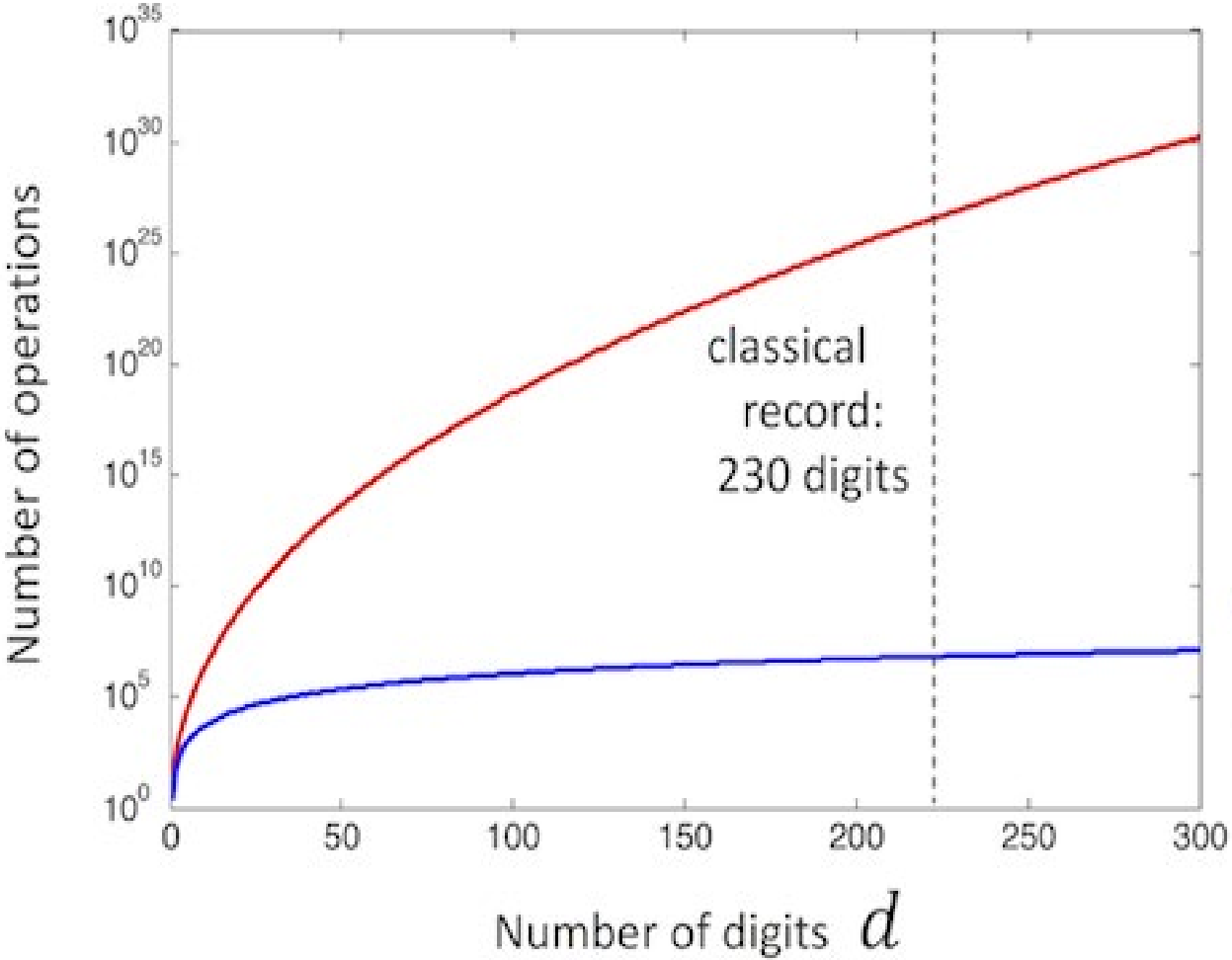
On a classical computer, it takes subexponential time to break algorithms like RSA, using the general number field sieve.

General number field sieve : $O(e^{((64/9)^{1/3} \cdot \log(n)^{1/3} \cdot \log(\log(n))^{2/3})})$ to factor n

But on a quantum computer, any discrete logarithm based cryptographic scheme can be broken in polylogarithmic time, using shor's algorithm.

Shor's Algorithm: $O(\log(n)^2 \cdot \log(\log(n)) \cdot \log(\log(\log(n))))$ to factor n

This difference is huge, it is the difference between computing for millenia and seconds.



$\exp(\text{const} \times d^{1/3})$

best classical
algorithm
(number field sieve)

$\text{const} \times d^3$

Shor's algorithm

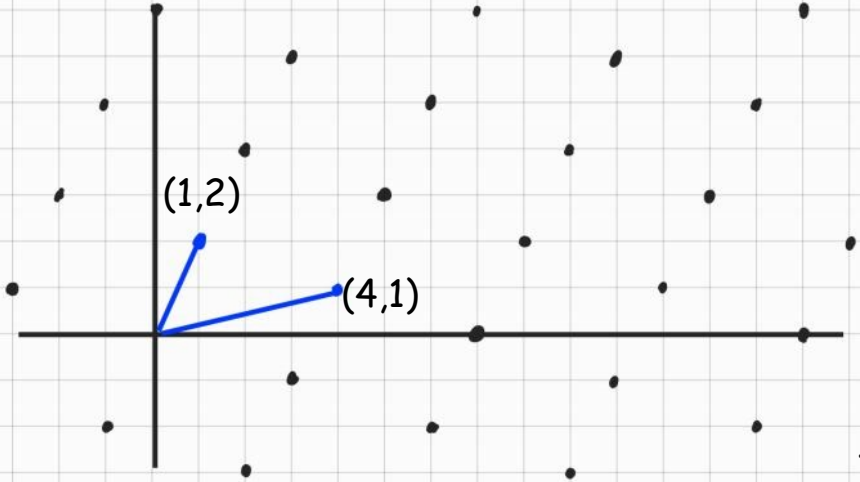
Post-Quantum Cryptography - NIST Standards

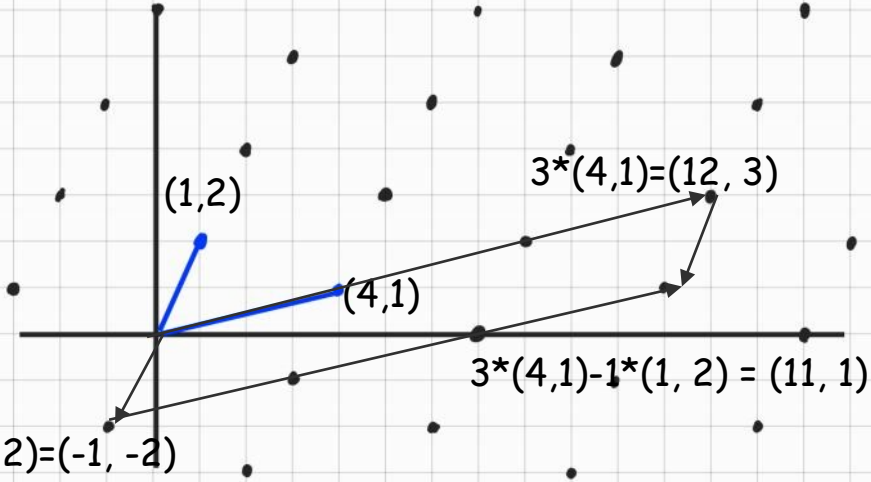
- According to National Institute of Science and Technology, they identified algorithms to be standardized including CRYSTALS-KYBER
- Need to learn about contemporary cryptographic algorithms that protect data and communications
- Current standards
  - General Encryption: CRYSTALS-Kyber
  - Digital Signatures: CRYSTALS-Dilithium
- These are both based on Lattices, and more specifically LWE.

do it

Lattices

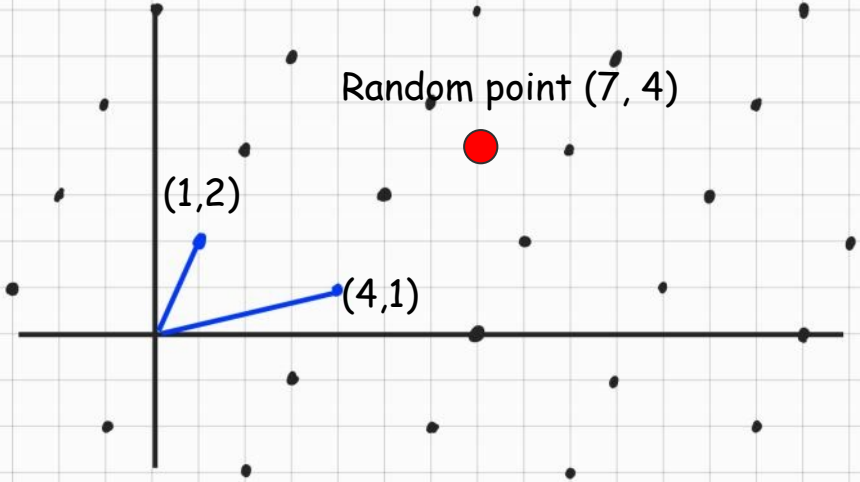
- A lattice is an infinite field of points produced by combinations of integral multiples of vectors
- Example: In the lattice with basis vectors (1, 2) and (4, 1), 3*(4,1)-1*(1, 2) = (11, 1) is on the lattice

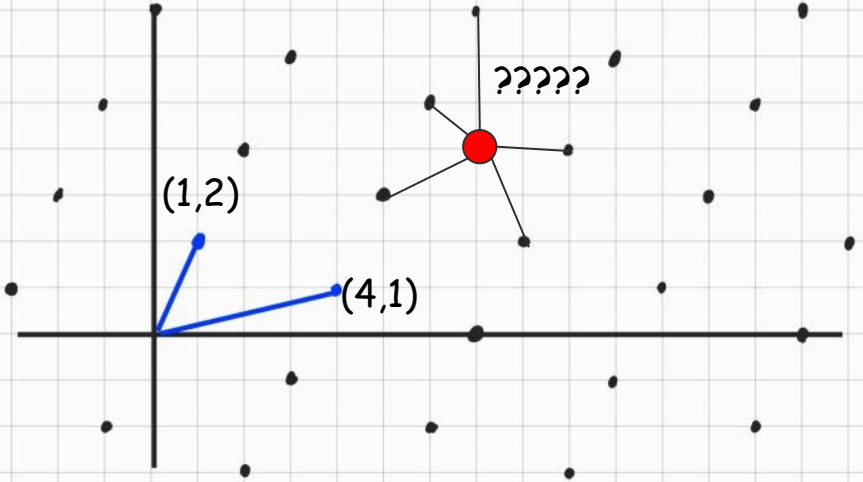




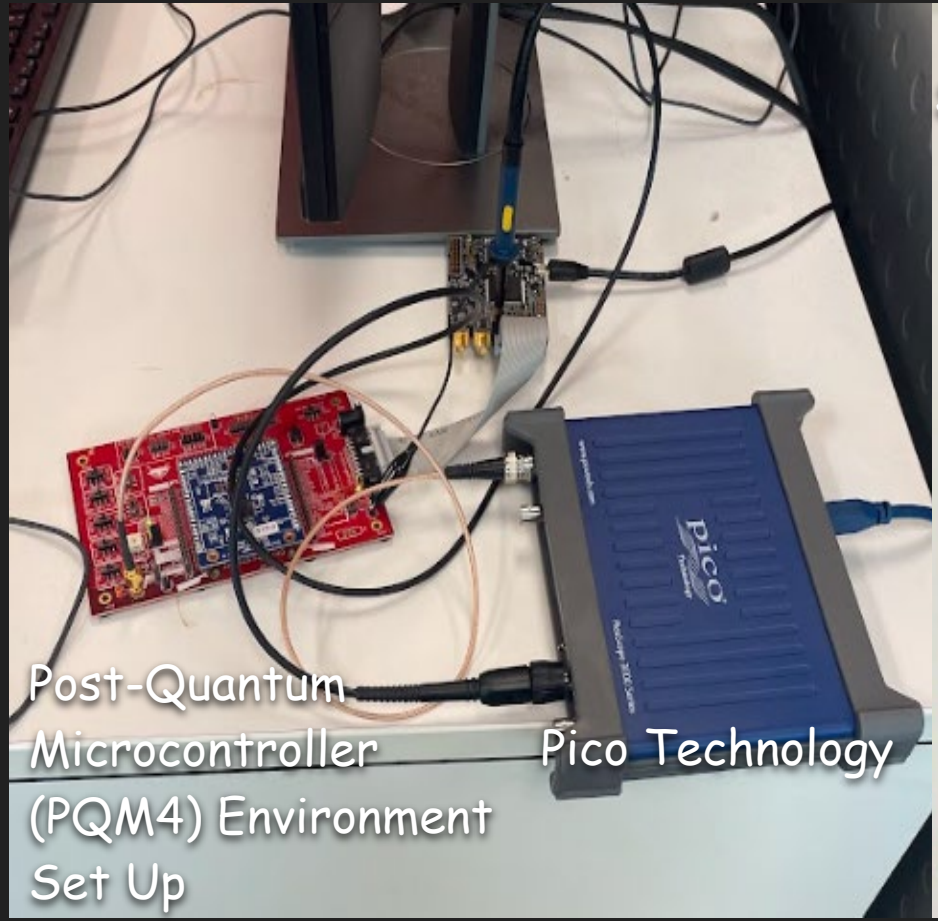
Learning with Errors (LWE) Problem & KYBER

The LWE problem states that given a lattice and a point somewhere not on the lattice, it is hard to find the point on the lattice with the minimum distance to that point. There are other variants like Ring and Module-LWE

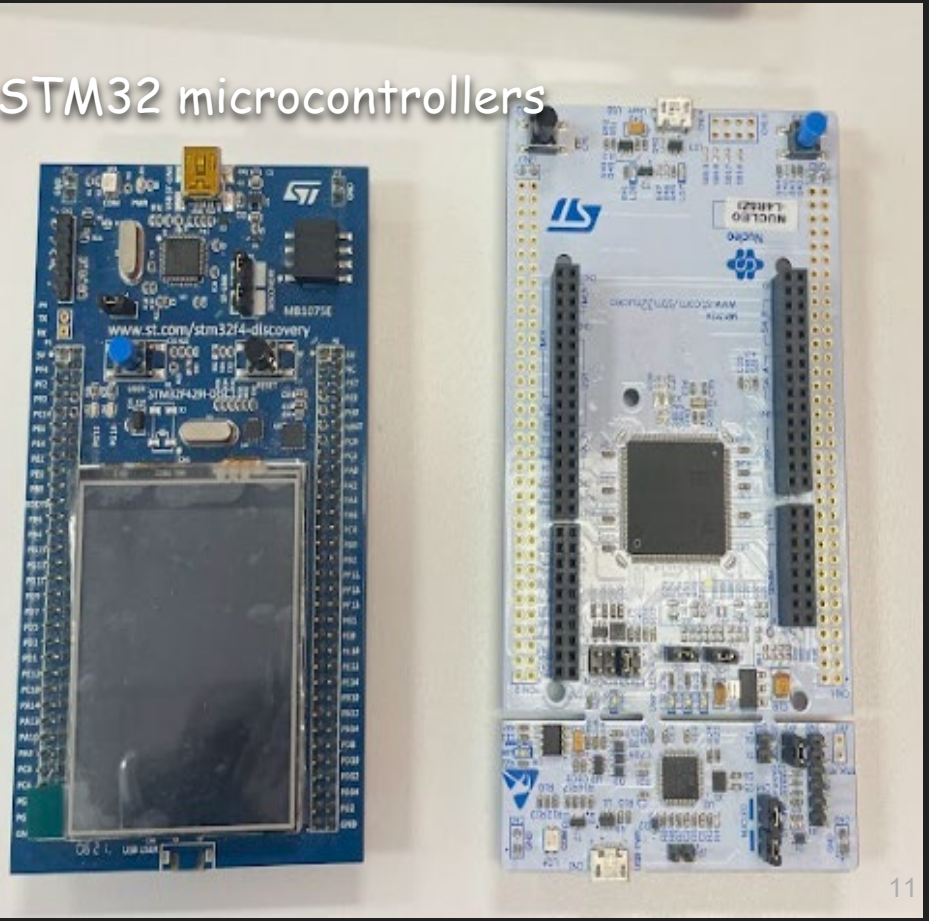




Hardware Implementation: Side-Channel Attacks

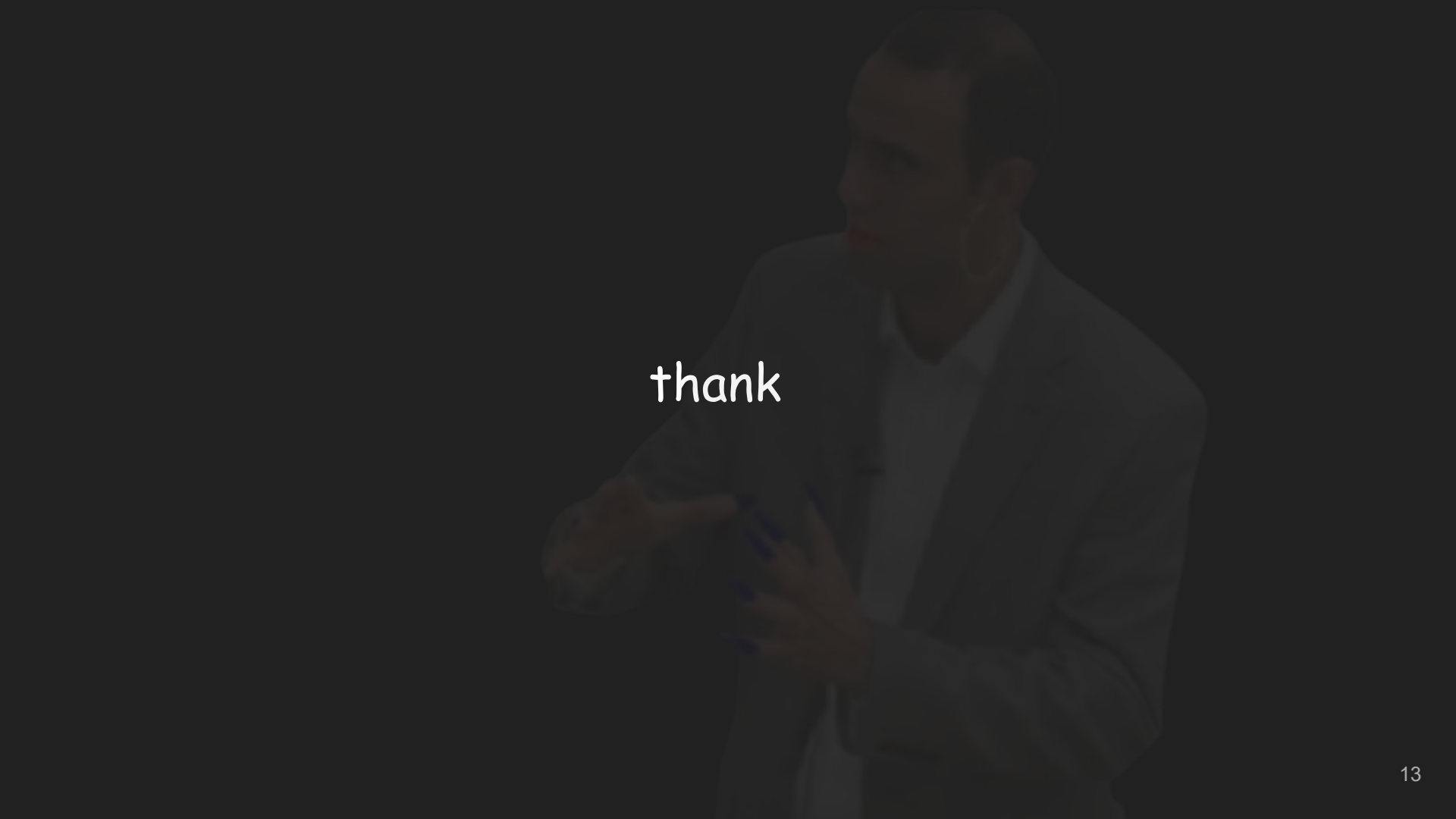


STM32 microcontrollers



Conclusion

- Classical cryptography may no longer be secure with computational advancements in computers
- Newer implementations including KYBER involve the study of lattices and Learning With Errors (and its variants)
- It is important to continue to be secure from side-channel attacks when updating to new quantum-resistant cryptographic algorithms
- Improvements: make cryptography more interactive for younger audience to understand importance of data and communications


thank