

WHY THE CURRENT ENCRYPTION STANDARDS MUST BE UPDATED? THE CASE OF POST QUANTUM CRYPTOGRAPHY.

Kostas Draziotis

ΣΦΗΜΜΥ 14
Volos

This work is licensed under a Creative Commons "Attribution-ShareAlike 4.0 International" licence.



INTRODUCTION

- First we need to see, what are the current encryption standards we use in order to secure our communication.

INTRODUCTION

- First we need to see, what are the current encryption standards we use in order to secure our communication.
- So before we continue, we provide some necessary definitions.

INTRODUCTION

- First we need to see, what are the current encryption standards we use in order to secure our communication.
- So before we continue, we provide some necessary definitions.
- Also, we provide some definitions concerning cryptography.

THE HEROES OF CRYPTOGRAPHY

- Alice and Bob is the most famous couple in the world of crypto. They were invented in 1978. Usually they want to exchange messages using some cryptographic protocol.

THE HEROES OF CRYPTOGRAPHY

- Alice and Bob is the most famous couple in the world of crypto. They were invented in 1978. Usually they want to exchange messages using some cryptographic protocol.

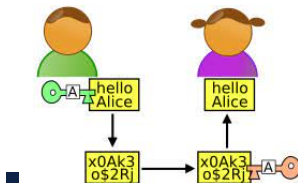


FIGURE: Bob encrypts the message *Hello Alice* and he sends it to Alice.

Licence: BY-SA 3.0

THE HEROES OF CRYPTOGRAPHY

- Alice and Bob is the most famous couple in the world of crypto. They were invented in 1978. Usually they want to exchange messages using some cryptographic protocol.

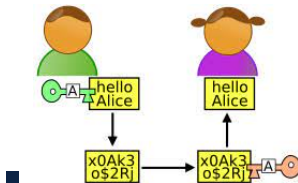


FIGURE: Bob encrypts the message *Hello Alice* and he sends it to Alice.

Licence: BY-SA 3.0

- Although, their friend Eve 🧐, sometimes, tries to intercept their communication and if she is lucky or smart enough she may decrypt the message.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- There are two main schemes in cryptography. Symmetric and Public key cryptography.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- There are two main schemes in cryptography. Symmetric and Public key cryptography.
- In symmetric crypto Alice and Bob use a common private key. I.e. we encrypt and decrypt messages with the same secret key.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- There are two main schemes in cryptography. Symmetric and Public key cryptography.
- In symmetric crypto Alice and Bob use a common private key. I.e. we encrypt and decrypt messages with the same secret key.
- No one can decrypt or encrypt without the key.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- There are two main schemes in cryptography. Symmetric and Public key cryptography.
- In symmetric crypto Alice and Bob use a common private key. I.e. we encrypt and decrypt messages with the same secret key.
- No one can decrypt or encrypt without the key.
- It is called symmetric since both entities uses the same key.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- There are two main schemes in cryptography. Symmetric and Public key cryptography.
- In symmetric crypto Alice and Bob use a common private key. I.e. we encrypt and decrypt messages with the same secret key.
- No one can decrypt or encrypt without the key.
- It is called symmetric since both entities uses the same key.
- Some symmetric schemes are : AES,DES,Blowfish,Serpent etc

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- Also, there are "asymmetric" cryptographic protocols, also called public key cryptosystems.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- Also, there are "asymmetric" cryptographic protocols, also called public key cryptosystems.
- In these schemes Alice and Bob use different keys. If Alice has a public key say P_A then anyone (not only Bob) can send encrypted messages to Alice.

SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY

- Also, there are "asymmetric" cryptographic protocols, also called public key cryptosystems.
- In these schemes Alice and Bob use different keys. If Alice has a public key say P_A then anyone (not only Bob) can send encrypted messages to Alice.
- Now, the public key of Alice is related with some specific private key, known only to Alice. So, only Alice can decrypt the messages.

A THIRD CRYPTOGRAPHIC PRIMITIVE

- So, there are two basic cryptographic schemes. **Symmetric cryptosystems** (Scs) and **Public key Cryptosystems** (PkCs). We use both of them to build security protocols, such as SSL/TLS or IPsec or ssh.

A THIRD CRYPTOGRAPHIC PRIMITIVE

- So, there are two basic cryptographic schemes. **Symmetric cryptosystems** (Scs) and **Public key Cryptosystems** (PkCs). We use both of them to build security protocols, such as SSL/TLS or IPsec or ssh.
- Also, seemingly there is one more scheme : **key agreement protocol**, such as Diffie-Hellman.

A THIRD CRYPTOGRAPHIC PRIMITIVE

- So, there are two basic cryptographic schemes. **Symmetric cryptosystems** (Scs) and **Public key Cryptosystems** (PkCs). We use both of them to build security protocols, such as SSL/TLS or IPsec or ssh.
- Also, seemingly there is one more scheme : **key agreement protocol**, such as Diffie-Hellman.
- In this protocol Alice and Bob want to end up with a common number (key), after having some short communication.

DIFFIE-HELLMAN

- For instance, say that Bob and Alice agree to a prime number p and a positive integer $< p$. Say $g = 2$.

DIFFIE-HELLMAN

- For instance, say that Bob and Alice agree to a prime number p and a positive integer $< p$. Say $g = 2$.
- Then Alice picks a random positive number $< p$ say a . Similar Bob picks b .

DIFFIE-HELLMAN

- For instance, say that Bob and Alice agree to a prime number p and a positive integer $< p$. Say $g = 2$.
- Then Alice picks a random positive number $< p$ say a . Similar Bob picks b .
- Alice sends $2^a \pmod{p}$ to Bob, and Bob sends $2^b \pmod{p}$ to Alice.

DIFFIE-HELLMAN

- For instance, say that Bob and Alice agree to a prime number p and a positive integer $< p$. Say $g = 2$.
- Then Alice picks a random positive number $< p$ say a . Similar Bob picks b .
- Alice sends $2^a \pmod{p}$ to Bob, and Bob sends $2^b \pmod{p}$ to Alice.

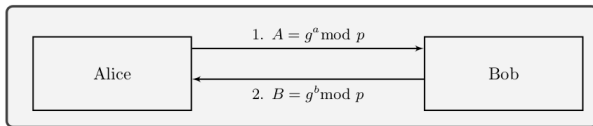


FIGURE: Diffie-Hellman, p : prime, $0 < g < p$, A, B are public.

DIFFIE-HELLMAN

- For instance, say that Bob and Alice agree to a prime number p and a positive integer $< p$. Say $g = 2$.
- Then Alice picks a random positive number $< p$ say a . Similar Bob picks b .
- Alice sends $2^a \pmod{p}$ to Bob, and Bob sends $2^b \pmod{p}$ to Alice.

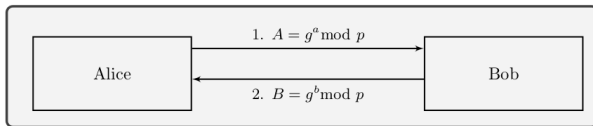


FIGURE: Diffie-Hellman, p : prime, $0 < g < p$, A, B are public.

- a is known only to Alice and b only to Bob.

DIFFIE-HELLMAN

- For instance, say that Bob and Alice agree to a prime number p and a positive integer $< p$. Say $g = 2$.
- Then Alice picks a random positive number $< p$ say a . Similarly Bob picks b .
- Alice sends $2^a \pmod{p}$ to Bob, and Bob sends $2^b \pmod{p}$ to Alice.

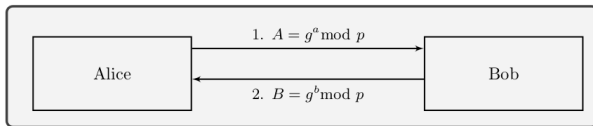


FIGURE: Diffie-Hellman, p : prime, $0 < g < p$, A, B are public.

- a is known only to Alice and b only to Bob.
- After this exchange, they end up with the common key $2^{ab} \pmod{p}$, which they combine it with a symmetric algorithm.

- Whit Diffie and Martin Hellman discovered Public Key Cryptography.

- Whit Diffie and Martin Hellman discovered Public Key Cryptography.
- For this invention they got Turing medal in 2015.

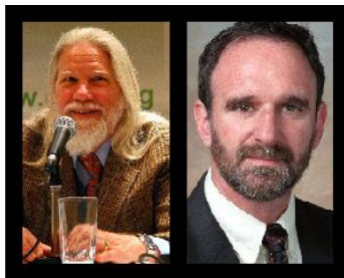


FIGURE: Whit Diffie and Martin Hellman. ACM Turing Medal 2015.

WHAT ABOUT QUANTUM COMPUTERS AND POST QUANTUM CRYPTOGRAPHY?

- So far, so good.


WHAT ABOUT QUANTUM COMPUTERS AND POST QUANTUM CRYPTOGRAPHY?

- So far, so good.
- What role do quantum computers play in cryptography?

WHAT ABOUT QUANTUM COMPUTERS AND POST QUANTUM CRYPTOGRAPHY?

- So far, so good.
- What role do quantum computers play in cryptography?
- Why is cryptography affected by quantum computers?

WHAT ABOUT QUANTUM COMPUTERS AND POST QUANTUM CRYPTOGRAPHY?

- So far, so good.
- What role do quantum computers play in cryptography?
- Why is cryptography affected by quantum computers?
- Also, what is a quantum computer? 

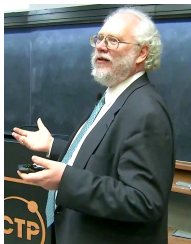
WHAT ABOUT QUANTUM COMPUTERS?

- There are algorithms that *run* in a quantum computer, much more faster in the classic computers. They exploit quantum properties that a classic computer can not do.

WHAT ABOUT QUANTUM COMPUTERS?

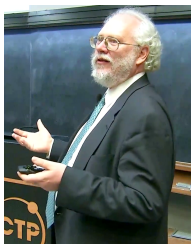
- There are algorithms that *run* in a quantum computer, much more faster in the classic computers. They exploit quantum properties that a classic computer can not do.
- There are many quantum algorithms. For instance see, <http://quantumalgorithmzoo.org/>

PETER SHOR'S QUANTUM ALGORITHM



license: CC BY-SA 3.0

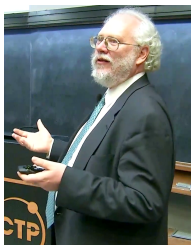
PETER SHOR'S QUANTUM ALGORITHM



license: CC BY-SA 3.0

- Peter Shor discovered a polynomial time (probabilistic) **quantum** algorithm that solves DLP in a generic group G (1994). The same algorithm can be used for factoring large integers.

PETER SHOR'S QUANTUM ALGORITHM



license: CC BY-SA 3.0

- Peter Shor discovered a polynomial time (probabilistic) **quantum** algorithm that solves DLP in a generic group G (1994). The same algorithm can be used for factoring large integers.
- If a quantum computer with large memory ever constructed, then the most well known public key cryptosystem, RSA (and also Diffie-Hellman), shall break and all the current security in Internet will be compromised.

CRYPTOSYSTEMS VULNERABLE BY QUANTUM COMPUTERS

- So, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.

CRYPTOSYSTEMS VULNERABLE BY QUANTUM COMPUTERS

- So, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.
- For instance, today IBM Osprey quantum computer has 433 qubits memory. Although, IBM promises 4000-qubit quantum computer by 2025.

CRYPTOSYSTEMS VULNERABLE BY QUANTUM COMPUTERS

- So, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.
- For instance, today IBM Osprey quantum computer has 433 qubits memory. Although, IBM promises 4000-qubit quantum computer by 2025.
- To factor a 2048-bit RSA modulus we need about 6000 (perfectly) stable qubits. Although, a landmark paper of [Gidney and Ekerä](#), suggests that we need 20million noisy qubits to factor 2048-bit modulus in 8 hours

CRYPTOSYSTEMS VULNERABLE BY QUANTUM COMPUTERS

- So, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.
- For instance, today IBM Osprey quantum computer has 433 qubits memory. Although, IBM promises 4000-qubit quantum computer by 2025.
- To factor a 2048-bit RSA modulus we need about 6000 (perfectly) stable qubits. Although, a landmark paper of [Gidney and Eker](#), suggests that we need 20million noisy qubits to factor 2048-bit modulus in 8 hours
- The current quantum computers are noisy

FINALLY...

- ...we learned that, the current cryptographic standards are based in Diffie-Hellman, RSA and symmetric cryptosystems, such as AES system.

FINALLY...

- ...we learned that, the current cryptographic standards are based in Diffie-Hellman, RSA and symmetric cryptosystems, such as AES system.
- However, post quantum attacks are dangerous only for DH and RSA, and in general all cryptographic primitives based on factorization and discrete logarithms. For instance ECDSA, the digital signature used in bitcoin, is vulnerable to quantum attacks.

harvest now, decrypt later ATTACK

Dystopia Scenario : Say, all the encrypted data you have exchanged the previous year were collected and kept in some data center. They will be kept and decrypted when a large memory quantum computer will be built.

harvest now, decrypt later ATTACK

Dystopia Scenario : Say, all the encrypted data you have exchanged the previous year were collected and kept in some data center. They will be kept and decrypted when a large memory quantum computer will be built.



license:public domain

harvest now, decrypt later ATTACK

Dystopia Scenario : Say, all the encrypted data you have exchanged the previous year were collected and kept in some data center. They will be kept and decrypted when a large memory quantum computer will be built.



license:public domain

Attackers are capable of storing today's encrypted communication, which can later be decrypted with the use of quantum computers. This includes sensitive information such as corporate/state secrets, medical records etc.

harvest now, decrypt later ATTACK

- But, what about forward secrecy? Since, SSL/TLS offers forward secrecy, this implies that someone can not compromise my future connections with a secure server having only the private key from one session.

harvest now, decrypt later ATTACK

- But, what about forward secrecy? Since, SSL/TLS offers forward secrecy, this implies that someone can not compromise my future connections with a secure server having only the private key from one session.
- In order to achieve forward secrecy, SSL/TLS uses Ephemeral DH or ECDH. Therefore, having all the transactions and using a quantum computer we can decrypt all the collected data.

WHERE ARE MY BTCs?

- In the beginning of Bitcoin the addresses, called p2pk, were used. Having a quantum computer someone can find the private key (bitcoin uses ECDSA for signing the transactions), so anyone can steal all the BTCs that are kept in such addresses. There are $\sim 1.000.000$ BTC in such addresses.

WHERE ARE MY BTCs?

- In the beginning of Bitcoin the addresses, called p2pk, were used. Having a quantum computer someone can find the private key (bitcoin uses ECDSA for signing the transactions), so anyone can steal all the BTCs that are kept in such addresses. There are $\sim 1.000.000$ BTC in such addresses.
- The newer addresses, called p2pkh :pay to public key hashed, are not vulnerable, unless you have use them at least one time, and you continue to accept bitcoins to these addresses.

WHERE ARE MY BTCs?

- In the beginning of Bitcoin the addresses, called p2pk, were used. Having a quantum computer someone can find the private key (bitcoin uses ECDSA for signing the transactions), so anyone can steal all the BTCs that are kept in such addresses. There are $\sim 1.000.000$ BTC in such addresses.
- The newer addresses, called p2pkh :pay to public key hashed, are not vulnerable, unless you have use them at least one time, and you continue to accept bitcoins to these addresses.
- Cybercriminals are storing data, for the day when a quantum computer can be used as cloud-based service.

NEW POST QUANTUM CRYPTO PRIMITIVES?

- NIST, the American organization which promotes innovation and industrial competitiveness, in 20 Dec. 2016 made the first announcement for Public-Key Post-Quantum Cryptographic Algorithms.

NEW POST QUANTUM CRYPTO PRIMITIVES?

- NIST, the American organization which promotes innovation and industrial competitiveness, in 20 Dec. 2016 made the first announcement for Public-Key Post-Quantum Cryptographic Algorithms.
- When we are talking about PQC we (usually) mean cryptography which is **not** based on Factorization and Discrete Logarithm Problem (DLP).

SUITABLY PROBLEMS FOR THE POST QUANTUM ERA

- Code based crypto 1978, McEliece

SUITABLY PROBLEMS FOR THE POST QUANTUM ERA

- Code based crypto 1978, McEliece
- Hash based crypto 1979, Lamport and Diffie and Merkle

SUITABLY PROBLEMS FOR THE POST QUANTUM ERA

- Code based crypto 1978, McEliece
- Hash based crypto 1979, Lamport and Diffie and Merkle
- Multivariate Quadratic (MQ) system 1996

SUITABLY PROBLEMS FOR THE POST QUANTUM ERA

- Code based crypto 1978, McEliece
- Hash based crypto 1979, Lamport and Diffie and Merkle
- Multivariate Quadratic (MQ) system 1996
- Lattice based crypto 1998 : e.g. NTRU, LWE

SUITABLY PROBLEMS FOR THE POST QUANTUM ERA

- Code based crypto 1978, McEliece
- Hash based crypto 1979, Lamport and Diffie and Merkle
- Multivariate Quadratic (MQ) system 1996
- Lattice based crypto 1998 : e.g. NTRU, LWE
- Supersingular Isogeny Diffie Hellman (SIDH)

SUITABLY PROBLEMS FOR THE POST QUANTUM ERA

- Code based crypto 1978, McEliece
- Hash based crypto 1979, Lamport and Diffie and Merkle
- Multivariate Quadratic (MQ) system 1996
- Lattice based crypto 1998 : e.g. NTRU, LWE
- Supersingular Isogeny Diffie Hellman (SIDH)
- The previous scheme uses Elliptic curves and it is mathematically very elegant. However it broke in July 2022.

3RD ROUND

- **Seven** finalists are being considered for initial standardization.

3RD ROUND

- **Seven** finalists are being considered for initial standardization.
- **Three Lattice based**, **PKE** : CRYSTALS-KYBER, NTRU, SABER

3RD ROUND

- **Seven** finalists are being considered for initial standardization.
- **Three Lattice based, PKE** : CRYSTALS-KYBER, NTRU, SABER
- **One code based, PKE** : Classic McEliece

3RD ROUND

- **Seven** finalists are being considered for initial standardization.
- **Three Lattice based, PKE** : **CRYSTALS-KYBER**, **NTRU**, **SABER**
- **One code based, PKE** : Classic McEliece
- **Two lattice based digital signatures** : Falcon and Crystals-Dilithium

3RD ROUND

- **Seven** finalists are being considered for initial standardization.
- **Three Lattice based, PKE** : **CRYSTALS-KYBER**, **NTRU**, **SABER**
- **One code based, PKE** : Classic McEliece
- **Two lattice based digital signatures** : Falcon and Crystals-Dilithium
- **One MQ, digital signature** : Rainbow

3RD ROUND

- **Seven** finalists are being considered for initial standardization.
- **Three Lattice based, PKE** : CRYSTALS-KYBER, NTRU, SABER
- **One code based, PKE** : Classic McEliece
- **Two lattice based digital signatures** : Falcon and Crystals-Dilithium
- **One MQ, digital signature** : Rainbow
- What is more, there are eight alternate candidate algorithms.

3RD ROUND

- **Seven** finalists are being considered for initial standardization.
- **Three Lattice based, PKE** : CRYSTALS-KYBER, NTRU, SABER
- **One code based, PKE** : Classic McEliece
- **Two lattice based digital signatures** : Falcon and Crystals-Dilithium
- **One MQ, digital signature** : Rainbow
- What is more, there are eight alternate candidate algorithms.
- For more information <https://csrc.nist.gov/projects/post-quantum-cryptography>

4TH ROUND

- In July 05, 2022, NIST announced the following.

4TH ROUND

- In July 05, 2022, NIST announced the following.
- **PKE, One Lattice based : CRYSTALS-KYBER**

4TH ROUND

- In July 05, 2022, NIST announced the following.
- **PKE, One Lattice based** : **CRYSTALS-KYBER**
- **Three Digital Signatures**, Falcon, Crystals-Dilithium and SPHINCS.

4TH ROUND

- In July 05, 2022, NIST announced the following.
- **PKE, One Lattice based** : **CRYSTALS-KYBER**
- **Three Digital Signatures**, Falcon, Crystals-Dilithium and SPHINCS.
- All the previous algorithms will be standardized by NIST

LATTICE BASED PQC

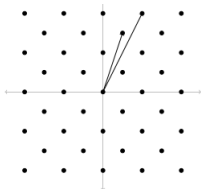
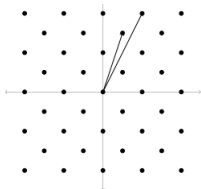


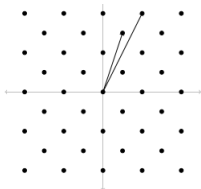
FIGURE: The 2 dimensional lattice \mathbb{Z}^2

LATTICE BASED PQC

FIGURE: The 2 dimensional lattice \mathbb{Z}^2

- Usually PQC is based on lattice problems.

LATTICE BASED PQC

FIGURE: The 2 dimensional lattice \mathbb{Z}^2

- Usually PQC is based on lattice problems.
- The problem of finding a shortest vector (which always exists) is called Shortest Vector Problem (SVP).

LATTICE BASED PQC



- In 2 dimensions the SVP is very easy. But if we increase the dimension, this problem becomes harder. In fact only exponential algorithms with respect the dimension are known for this problem.

LATTICE BASED PQC



- In 2 dimensions the SVP is very easy. But if we increase the dimension, this problem becomes harder. In fact only exponential algorithms with respect the dimension are known for this problem.
- It was proved in 1998, by Ajtai, that it is NP-hard under randomized reductions.

LATTICE BASED PQC



- In 2 dimensions the SVP is very easy. But if we increase the dimension, this problem becomes harder. In fact only exponential algorithms with respect the dimension are known for this problem.
- It was proved in 1998, by Ajtai, that it is NP-hard under randomized reductions.
- Randomized karp reductions (instead of deterministic Karp reductions), means that if you solve SVP, then you get a randomized algorithm for any problem in NP.

LATTICE BASED PQC



- In 2 dimensions the SVP is very easy. But if we increase the dimension, this problem becomes harder. In fact only exponential algorithms with respect the dimension are known for this problem.
- It was proved in 1998, by Ajtai, that it is NP-hard under randomized reductions.
- Randomized karp reductions (instead of deterministic Karp reductions), means that if you solve SVP, then you get a randomized algorithm for any problem in NP.
- Many PQC are based on problems that in order to solve them, we need to solve a SVP in a large dimensional lattice.

LATTICE BASED PQC



- In 2 dimensions the SVP is very easy. But if we increase the dimension, this problem becomes harder. In fact only exponential algorithms with respect the dimension are known for this problem.
- It was proved in 1998, by Ajtai, that it is NP-hard under randomized reductions.
- Randomized karp reductions (instead of deterministic Karp reductions), means that if you solve SVP, then you get a randomized algorithm for any problem in NP.
- Many PQC are based on problems that in order to solve them, we need to solve a SVP in a large dimensional lattice.
- A famous example in this class of problems is the Ring Learning with Errors RLWE.

LATTICE BASED PQC



- In 2 dimensions the SVP is very easy. But if we increase the dimension, this problem becomes harder. In fact only exponential algorithms with respect the dimension are known for this problem.
- It was proved in 1998, by Ajtai, that it is NP-hard under randomized reductions.
- Randomized karp reductions (instead of deterministic Karp reductions), means that if you solve SVP, then you get a randomized algorithm for any problem in NP.
- Many PQC are based on problems that in order to solve them, we need to solve a SVP in a large dimensional lattice.
- A famous example in this class of problems is the Ring Learning with Errors RLWE.
- Another example is the Short Integer Problem (SIS).

CRYPTANALYSIS WITH QUANTUM COMPUTERS

- Is it possible to solve it efficiently using quantum algorithms?

CRYPTANALYSIS WITH QUANTUM COMPUTERS

- Is it possible to solve it efficiently using quantum algorithms?
- The best result until now, provides an algorithm with complexity $2^{0.268n+o(n)}$ instead of $2^{0.298n+o(n)}$ in classic computers.

KYBER

- Crystals-Kyber is the winner of the previous competition and is based on hard problem on lattices.

KYBER

- Crystals-Kyber is the winner of the previous competition and is based on hard problem on lattices.
- This is the algorithm that will replace RSA.

LEARNING WITH ERRORS

Kyber is based on the LWE problem. To understand this problem consider the following system in \mathbb{Z}_{11} .

$$\begin{cases} 2s_1 + 3s_2 + 4s_3 &= 16 \\ 4s_1 + s_2 + s_3 &= 8 \\ -s_1 + 2s_2 - s_3 &= -1 \end{cases}$$

This is very easy and with Gauss reduction we get the solution $\mathbf{s} = (1, 2, 2)$.

LEARNING WITH ERRORS

Consider now the same system but we have added some noise, given by a vector $\mathbf{e} = (e_1, e_2, e_3)$ chosen from some distribution over $\{-1, 0, 1\}$.

$$\begin{cases} 2s_1 + 3s_2 + 4s_3 + e_1 & = & 16 \\ 4s_1 + s_2 + s_3 + e_2 & = & 8 \\ -s_1 + 2s_2 - s_3 + e_3 & = & -1 \end{cases}$$

The second system is much harder than the first one.

LEARNING WITH ERRORS

LWE problem, is the following : Let A be a randomly chosen $n \times m$ matrix, $\mathbf{e} \xleftarrow{\chi} \{-1, 0, 1\}^n$ chosen from some distribution χ , \mathbf{s} random from \mathbb{Z}_q^m , and the pair $(A, A\mathbf{s}^T + \mathbf{e}^T)$, then compute the vector \mathbf{s} .

LEARNING WITH ERRORS AND KYBER

- Kyber is based on Module-LWE. In module LWE instead of the ring \mathbb{Z}_q we use the module $\mathbb{Z}_q[x]/\langle x^N + 1 \rangle$. For instance $(N, q) = (256, 7681)$.

LEARNING WITH ERRORS AND KYBER

- Kyber is based on Module-LWE. In module LWE instead of the ring \mathbb{Z}_q we use the module $\mathbb{Z}_q[x]/\langle x^N + 1 \rangle$. For instance $(N, q) = (256, 7681)$.

LEARNING WITH ERRORS AND KYBER

- Kyber is based on Module-LWE. In module LWE instead of the ring \mathbb{Z}_q we use the module $\mathbb{Z}_q[x]/\langle x^N + 1 \rangle$. For instance $(N, q) = (256, 7681)$.
- First time in 2012 Brakerski, Gentry, and Vinod Vaikuntanathan suggested Module LWE (which is more efficient than LWE and RLWE).

AJTAI'S LANDMARK RESULT

- First time in 1996 Ajtai found a reduction from a hard problem in lattices to a SIS (a similar problem with LWE)

AJTAI'S LANDMARK RESULT

- First time in 1996 Ajtai found a reduction from a hard problem in lattices to a SIS (a similar problem with LWE)
- Then in 2005, Regev, suggested LWE and proved a quantum reduction from a hard lattice problem to LWE

AJTAI'S LANDMARK RESULT

- First time in 1996 Ajtai found a reduction from a hard problem in lattices to a SIS (a similar problem with LWE)
- Then in 2005, Regev, suggested LWE and proved a quantum reduction from a hard lattice problem to LWE
- In 2010, Lyubashevsky, Peikert, and Regev O introduce RLWE and showed that there is a quantum reduction from a hard problem on (ideal) lattices to RLWE.

THE FUTURE

- The implementation of post-quantum cryptography is crucial to protect against future quantum computer attacks, but it requires a massive undertaking to update infrastructure and devices.

THE FUTURE

- The implementation of post-quantum cryptography is crucial to protect against future quantum computer attacks, but it requires a massive undertaking to update infrastructure and devices.
- Attackers can store encrypted information for future decryption, making the adoption of post-quantum cryptography necessary to prevent future attacks.

THE FUTURE

- The implementation of post-quantum cryptography is crucial to protect against future quantum computer attacks, but it requires a massive undertaking to update infrastructure and devices.
- Attackers can store encrypted information for future decryption, making the adoption of post-quantum cryptography necessary to prevent future attacks.
- NIST's role in setting these standards is essential not just for the US but also for the global cybersecurity community. Adoption of these standards is crucial, and while some European government agencies support NIST-selected schemes, they may still consider using other algorithms. Nonetheless, it is expected that the NIST standard will become a worldwide standard.

Thank you!