Cybersecurity in quantum era

Kostas Draziotis

ΣΦΗΜΜΥ 12
Apr.21 – Apr.23 , 2021
Thessaloniki

Introduction

- First we need to understand what is cybersecurity in the current era!

Introduction

- First we need to understand what is cybersecurity in the current era!
- So before we continue, we provide some necessary definitions.

Introduction

- First we need to understand what is cybersecurity in the current era!
- So before we continue, we provide some necessary definitions.
- *Cybersecurity* is the protection of computer systems and networks from information disclosure, theft or damage from malicious attack (cyberattacks).

Introduction

- First we need to understand what is cybersecurity in the current era!
- So before we continue, we provide some necessary definitions.
- *Cybersecurity* is the protection of computer systems and networks from information disclosure, theft or damage from malicious attack (cyberattacks).
- Also, we provide some definitions concerning cryptography.

ALICE, BOB AND EVE

- Usually Alice and Bob want to have a secure communication.

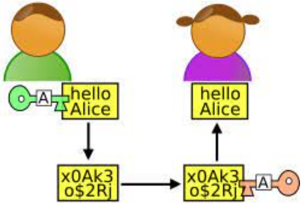


FIGURE: Bob encrypts the message *Hello Alice* and he sends it to Alice.

Alice, Bob and Eve

- Usually Alice and Bob want to have a secure communication.

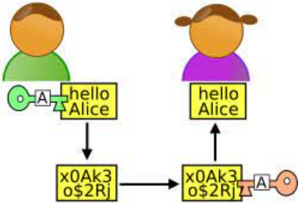


Figure: Bob encrypts the message *Hello Alice* and he sends it to Alice.

- Although, their friend Eve , sometimes, tries to intercept their communication and if she is lucky or smart enough she may decrypt the message. Usually, Eve has enough resources, sophisticated algorithms, very powerful computers and she is very skilled in social engineering.

Three cryptographic primitives

- There two basic 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, sometimes instead of a PkC we use a key agreement protocol, such as Diffie-Hellman.

Three cryptographic primitives

- There two basic 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, sometimes instead of a PkC we use a key agreement protocol, such as Diffie-Hellman.

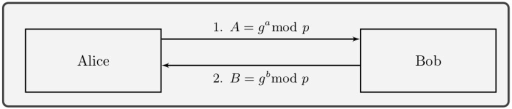
  - 

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

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

Three cryptographic primitives

- There two basic 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, sometimes instead of a PkC we use a key agreement protocol, such as Diffie-Hellman.

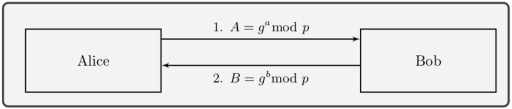


FIGURE: Diffie-Hellman, p : *prime*, $0 < g < p$, A, B are public.

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

Three cryptographic primitives

- There two basic 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, sometimes instead of a PkC we use a key agreement protocol, such as Diffie-Hellman.

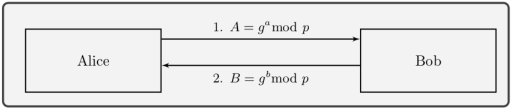
- 

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 $g^{ab} \pmod p$, which they combine it with a symmetric algorithm.
- Here Eve, if somehow discovers a or b she will compromise all the communication.

- Also, instead of Diffie-Hellman key agreement protocol the PkCs based on a notion called trapdoor function. These functions were first presented by the pioneers cryptographers, Whit Diffie and Martin Hellman, where they discovered Public Key Cryptography.

- Also, instead of Diffie-Hellman key agreement protocol the PkCs based on a notion called trapdoor function. These functions were first presented by the pioneers cryptographers, Whit Diffie and Martin Hellman, where they discovered Public Key Cryptography.
- Public Key Cryptography, as well as Key agreement protocols, as we use them today, are based on the following number theoretic problems : Factorization and Discrete Logarithm Problem.

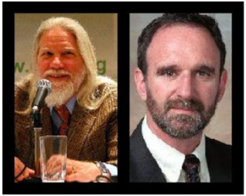
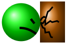
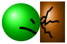


FIGURE: Whit Diffie and Martin Hellman. ACM Turing Medal 2015.

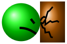
What about quantum computers?

- *disclaimer* : Since I am not a physicist I can't say much for Quantum Computers, because I don't understand how they work! 

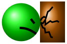
What about quantum computers?

- *disclaimer* : Since I am not a physicist I can't say much for Quantum Computers, because I don't understand how they work! 
- But we can easily explain, their relation with Cryptography.

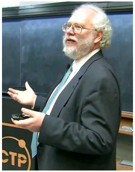
What about quantum computers?

- *disclaimer* : Since I am not a physicist I can't say much for Quantum Computers, because I don't understand how they work! 
- But we can easily explain, their relation with Cryptography.
- The key word here is : *Shor's Algorithm*.

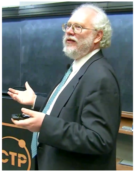
What about quantum computers?

- *disclaimer* : Since I am not a physicist I can't say much for Quantum Computers, because I don't understand how they work! 
- But we can easily explain, their relation with Cryptography.
- The key word here is : *Shor's Algorithm*.
- It runs only in quantum computers (since it exploits quantum properties) and solves the problem of factorization and DL problem in polynomial time.

Peter Shor's quantum algorithm

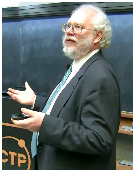
- 

Peter Shor's quantum algorithm

- 

- 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

- 
- 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.

Cybersecurity in quantum Era?

- So, we can explain now the title of the talk 🙂.

Cybersecurity in quantum Era?

- So, we can explain now the title of the talk ☺.
- This is the era where Eve has a large memory quantum computer in her possession but also Alice and Bob have the cryptosystems to protect their communication from quantum attacks.

Cybersecurity in quantum Era?

- So, we can explain now the title of the talk 🙂.
- This is the era where Eve has a large memory quantum computer in her possession but also Alice and Bob have the cryptosystems to protect their communication from quantum attacks.
- The algorithms that Alice and Bob use are called *Post Quantum Cryptosystems*.

Cybersecurity in quantum Era?

- So, we can explain now the title of the talk ☺.
- This is the era where Eve has a large memory quantum computer in her possession but also Alice and Bob have the cryptosystems to protect their communication from quantum attacks.
- The algorithms that Alice and Bob use are called *Post Quantum Cryptosystems*.
- Also, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.

Cybersecurity in quantum Era?

- So, we can explain now the title of the talk ☺.
- This is the era where Eve has a large memory quantum computer in her possession but also Alice and Bob have the cryptosystems to protect their communication from quantum attacks.
- The algorithms that Alice and Bob use are called *Post Quantum Cryptosystems*.
- Also, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.
- For instance, today IBM-Q, the quantum computer of IBM, has 65 qubits memory. Although, IBM promises 1000-qubit quantum computer by 2023.

Cybersecurity in quantum Era?

- So, we can explain now the title of the talk ☺.
- This is the era where Eve has a large memory quantum computer in her possession but also Alice and Bob have the cryptosystems to protect their communication from quantum attacks.
- The algorithms that Alice and Bob use are called *Post Quantum Cryptosystems*.
- Also, Eve needs a quantum computer with enough memory. We measure the memory of quantum computers in qubits.
- For instance, today IBM-Q, the quantum computer of IBM, has 65 qubits memory. Although, IBM promises 1000-qubit quantum computer by 2023.
- *Bristlecone*, the google's quantum computer, it has 72 qubits

Cybersecurity in quantum Era?

- To factor a 2048-bit RSA modulus we need about 6000 (perfectly) stable qubits. Although, a landmark paper of Gidney and Ekera, suggests that we need 20million noisy qubits to factor 2048-bit modulus in 8 hours

Cybersecurity in quantum Era?

- To factor a 2048-bit RSA modulus we need about 6000 (perfectly) stable qubits. Although, a landmark paper of Gidney and Ekera, suggests that we need 20million noisy qubits to factor 2048-bit modulus in 8 hours
- The current quantum computers are noisy

Cybersecurity in quantum Era?

- To factor a 2048-bit RSA modulus we need about 6000 (perfectly) stable qubits. Although, a landmark paper of Gidney and Ekera, suggests that we need 20million noisy qubits to factor 2048-bit modulus in 8 hours
- The current quantum computers are noisy
- How large is a 2048-bit integer?

How large is a 2048 or 4096 bits integer?

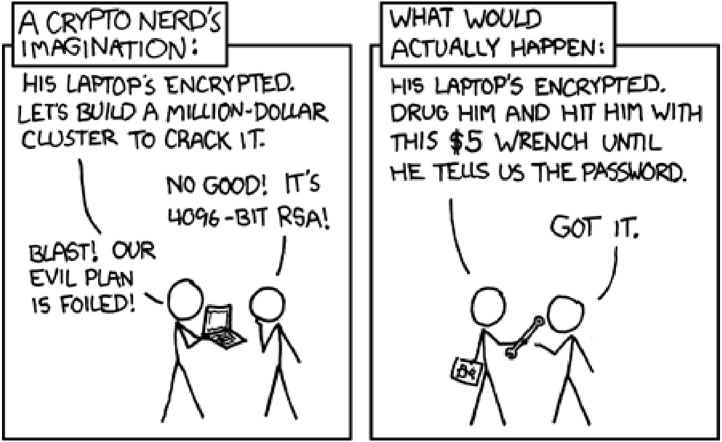


FIGURE: Licence:xkcd.com, CC BY-NC 2.

How large is a 2048 bits integer?

- Here is the number you have to factor in order to break the security of `https://www.sfhmmy.gr/`

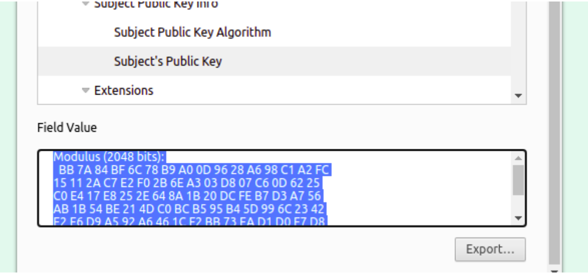


Figure: RSA public key

How large is a 2048 bits integer?

- ...and if we represent it as an integer

```
23666979175373978402499286868963481586560385165620924550890379288111O423\
23840415206673135015487368492305895934209556109741650992666805206719 4395\
```

How large is a 2048 bits integer?

- ...and if we represent it as an integer

```
23666979175373978402499286868963481586560385165620924550890379288111O423\
238404152066731350154873684923058959342095561097416509926668052067194395\
159648229493748798615332050052858896009784504620170814783692610398045900\
140167222626905623214902579061673663159365906153364449644240912381048000\
238183883103063286643646262270394166332736638459211300770684353422869195\
996527266327813527690931019987991992600942095272228931181847018205192648\
687960611937525233108111461550726182358572994215168369025892791967296674\
131323898777664515932960356538839891068969078068777021646419769454794321\
74379668988706888694604071755292473340541L
```

Figure: RSA public key

- A quantum computer capable of implementing Shor's algorithms will return the two prime factors.

How large is a 2048 bits integer?

- The current record for factorization RSA modulus with 829 bits and it was factored in Feb. 2020 using CADO-NFS software.

```
RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447
          1401366433455190958046796109928518724709145876873962619215573630474547705208
          0511905649310668769159001975940569345745223058932597669747168173806936489469
          9871578494975937497937
```

```
RSA-250 = 6413528947707158027879019017057738908482501474294344720811685963202453234463
          0238623598752668347708737661925585694639798853367
        × 3337202759497815655622601060535511422794076034476755466678452098702384172921
          0037080257448673296881877565718986258036932062711
```

How large is a 2048 bits integer?

- The current record for factorization RSA modulus with 829 bits and it was factored in Feb. 2020 using CADO-NFS software.

```
RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447
          1401366433455190958046796109928518724709145876873962619215573630474547705208
          0511905649310668769159001975940569345745223058932597669747168173806936489469
          9871578494975937497937
```

```
RSA-250 = 6413528947707158027879019017057738908482501474294344720811685963202453234463
          0238623598752668347708737661925585694639798853367
        × 3337202759497815655622601060535511422794076034476755466678452098702384172921
          0037080257448673296881877565718986258036932062711
```

- They used the General Number Field Sieve (GNFS) algorithm. It is a subexponential algorithm, the best we have for factorization.

How large is a 2048 bits integer?

- The current record for factorization RSA modulus with 829 bits and it was factored in Feb. 2020 using CADO-NFS software.

```
RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447
          1401366433455190958046796109928518724709145876873962619215573630474547705208
          0511905649310668769159001975940569345745223058932597669747168173806936489469
          9871578494975937497937
```

```
RSA-250 = 6413528947707158027879019017057738908482501474294344720811685963202453234463
          0238623598752668347708737661925585694639798853367
        × 3337202759497815655622601060535511422794076034476755466678452098702384172921
          0037080257448673296881877565718986258036932062711
```

- They used the General Number Field Sieve (GNFS) algorithm. It is a subexponential algorithm, the best we have for factorization.
- The computation involved tens of thousands of machines and was finished in a few months.

How large is a 2048 bits integer?

- The current record for factorization RSA modulus with 829 bits and it was factored in Feb. 2020 using CADO-NFS software.

```
RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447
          1401366433455190958046796109928518724709145876873962619215573630474547705208
          0511905649310668769159001975940569345745223058932597669747168173806936489469
          9871578494975937497937
```

```
RSA-250 = 6413528947707158027879019017057738908482501474294344720811685963202453234463
          0238623598752668347708737661925585694639798853367
        × 3337202759497815655622601060535511422794076034476755466678452098702384172921
          0037080257448673296881877565718986258036932062711
```

- They used the General Number Field Sieve (GNFS) algorithm. It is a subexponential algorithm, the best we have for factorization.
- The computation involved tens of thousands of machines and was finished in a few months.
- The (heuristic) time complexity of GNFS is $2^{O(\sqrt[3]{\log_2(N)})}$.

If someone wonders, FACTOR problem is not known to be NP-complete

If someone wonders, FACTOR problem is not known to be NP-complete

- In fact it is in the intersection $NP \cap co-NP$.

If someone wonders, FACTOR problem is not known to be NP-complete

- In fact it is in the intersection $NP \cap co - NP$.
- It is unlikely to be NP-complete.

Is it possible this quantum era to occur?

Is it possible this quantum era to occur?

- Sure!

Is it possible this quantum era to occur?

- Sure!
- In many papers, the authors already assume that Eve has a quantum computers and use it to break the communication between Alice and Bob.

Is it possible this quantum era to occur?

- Sure!
- In many papers, the authors already assume that Eve has a quantum computers and use it to break the communication between Alice and Bob.
- Although, we don't know or predict when a large memory quantum computer has been built. But we have such computers with low memory.

Maybe it's time to panic

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

Maybe it's time to panic

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

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 Problem 2006, (SIDH) Key exchange

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`

So why we do not use them and stop worrying about quantum computers?

- Well, Post quantum cryptographic algorithms are not very efficient...yet

So why we do not use them and stop worrying about quantum computers?

- Well, Post quantum cryptographic algorithms are not very efficient...yet
- We must have good evidences that they are indeed quantum resistant. So, years of research need to be done.

Lattice based PQC

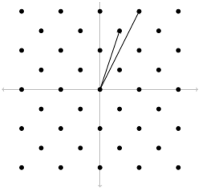
- 

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

Lattice based PQC

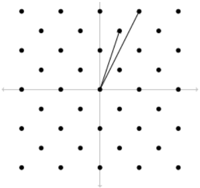
- 

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

- Usually PQC is based on lattice problems.

Lattice based PQC

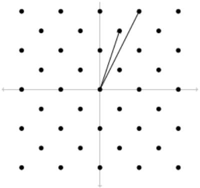
- 

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. 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.

PQC based on Multivariate Quadratic problem (MQ)

- Matsumoto and Imai in 1988 first they presented a cryptosystem based on MQ problem.

PQC based on Multivariate Quadratic problem (MQ)

- Matsumoto and Imai in 1988 first they presented a cryptosystem based on MQ problem.
- Let $p_1(x_1, ..., x_k), ..., p_m(x_1, ..., x_k)$ some quadratic polynomials over a finite field. For simplicity consider that we reduce all the coefficients of p_i modulo a prime number p.

PQC based on Multivariate Quadratic problem (MQ)

- Matsumoto and Imai in 1988 first they presented a cryptosystem based on MQ problem.
- Let $p_1(x_1, ..., x_k), ..., p_m(x_1, ..., x_k)$ some quadratic polynomials over a finite field. For simplicity consider that we reduce all the coefficients of p_i modulo a prime number p.
- The *MQ* problem is the problem of finding the solutions of

$$\{p_1 = p_2 = \cdots = p_m = 0 \pmod{p}\}$$

PQC based on Multivariate Quadratic problem (MQ)

- Matsumoto and Imai in 1988 first they presented a cryptosystem based on MQ problem.
- Let $p_1(x_1, ..., x_k), ..., p_m(x_1, ..., x_k)$ some quadratic polynomials over a finite field. For simplicity consider that we reduce all the coefficients of p_i modulo a prime number p.
- The *MQ* problem is the problem of finding the solutions of

$$\{p_1 = p_2 = \cdots = p_m = 0 \pmod p\}$$

- It seems easy, but it was proved to be NP-hard.

Thank you!