The effect of quantum algorithms

Thomas Gregersen

February 28, 2017

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

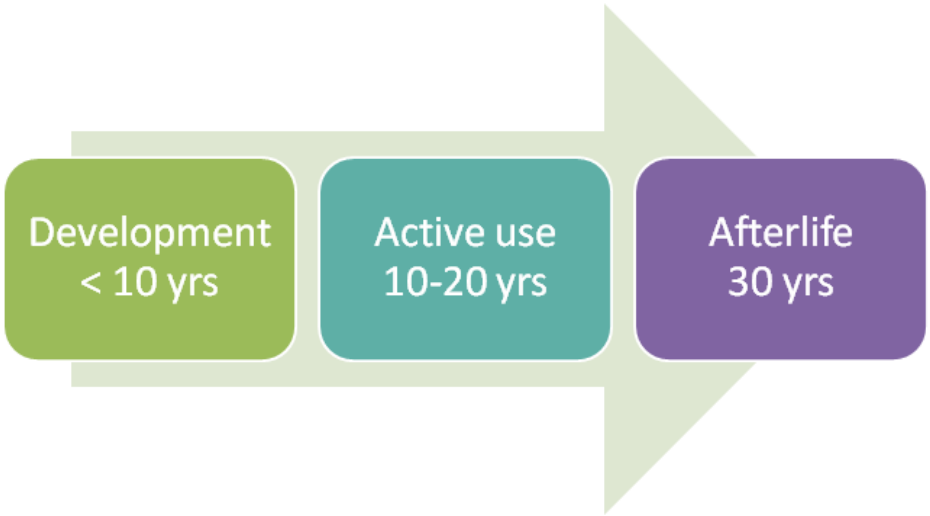
Hash-based signatures

Comparisons

The realities of quantum computers

- We are going to look at the cryptographic consequences of quantum computers.

- We are going to look at the cryptographic consequences of quantum computers.
- Why are we so eager to address this now?
  Long-term consequences:



  - Typically, information needs to be protected for a long time.
  - Implementing new algorithms is time-consuming.
  - If we want longevity, we need to start development early.

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

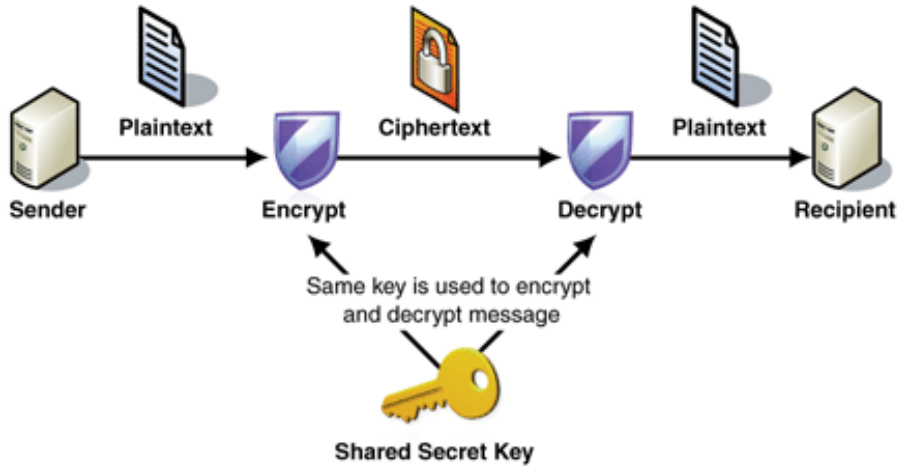
Lattice-based cryptosystems

Hash-based signatures

Comparisons

The realities of quantum computers

- The beginnings: In symmetric cryptography, two parties use a common key for sharing secret information:



Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

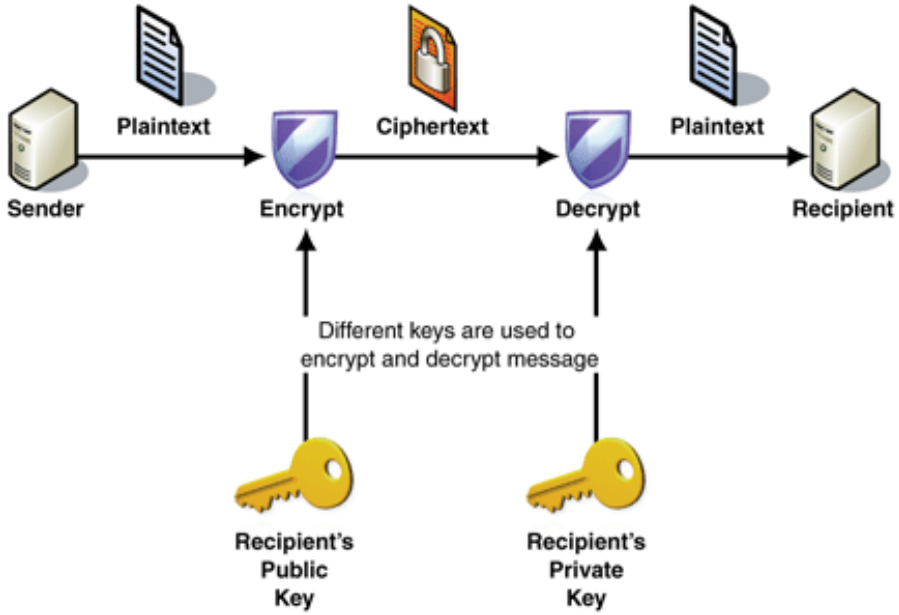
Lattice-based cryptosystems

Hash-based signatures

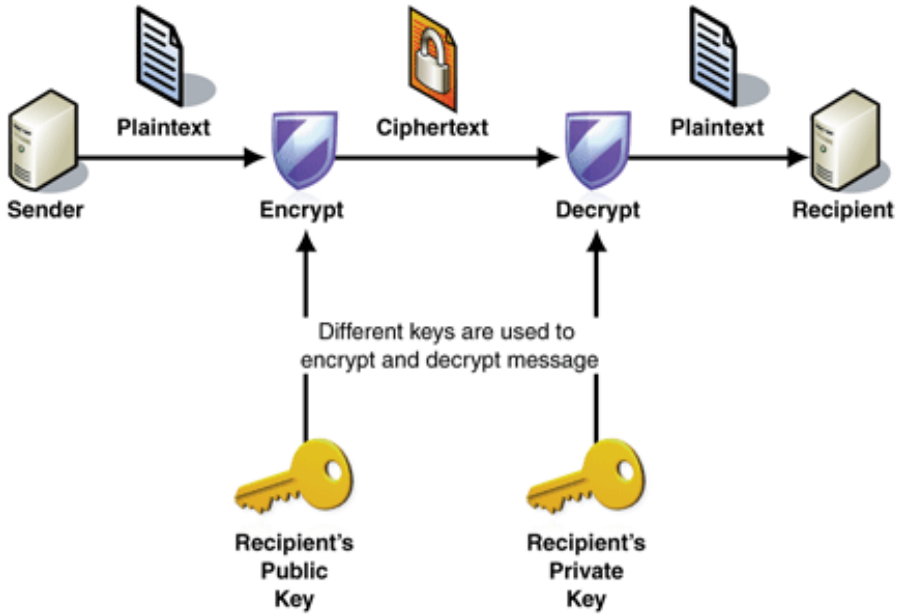
Comparisons

The realities of quantum computers

- To make life easier, we can exchange keys online using asymmetric algorithms:



- To make life easier, we can exchange keys online using asymmetric algorithms:



- This is too time-consuming so there will usually be a key-exchange to establish a symmetric key for bulk transfer.

- There are several algorithms to choose from: RSA, Diffie-Hellman, ElGamal, ECC...

- There are several algorithms to choose from: RSA, Diffie-Hellman, ElGamal, ECC...
- Quantum computers dictates a search for new/other algorithms as these are threatened.

- There are several algorithms to choose from: RSA, Diffie-Hellman, ElGamal, ECC...
- Quantum computers dictates a search for new/other algorithms as these are threatened.
- If all traffic is recorded, an attacker might simply use QC to break the key exchange and find the symmetric key in use.

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures

Comparisons

The realities of quantum computers

- A standard technique to check authenticity: They are usually based on asymmetric cryptographic algorithms, e.g:
  - RSA
  - DSA
  - ECDSA

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures

Comparisons

The realities of quantum computers

- One way of doing this is comparing the needed effort to a search through the key space of a symmetric cipher (key lengths in number of bits).

- One way of doing this is comparing the needed effort to a search through the key space of a symmetric cipher (key lengths in number of bits).
- Typical levels of security (NIST 2016):

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

All key sizes are provided in bits. These are the minimal sizes for security.

- One way of doing this is comparing the needed effort to a search through the key space of a symmetric cipher (key lengths in number of bits).
- Typical levels of security (NIST 2016):

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

All key sizes are provided in bits. These are the minimal sizes for security.

- These lists are dynamical and change through time. One reason is quantum computing.

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

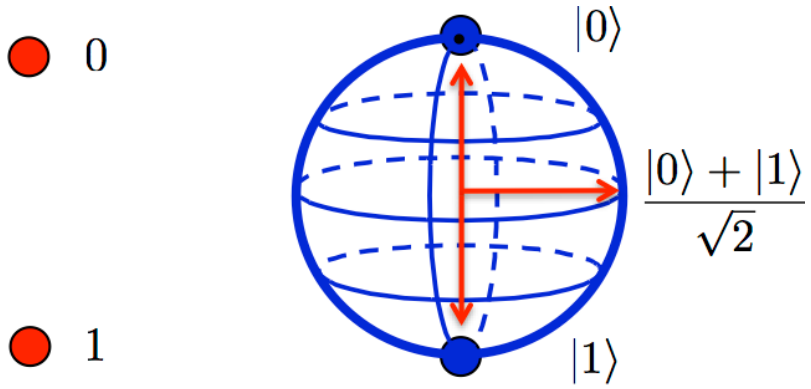
Lattice-based cryptosystems

Hash-based signatures

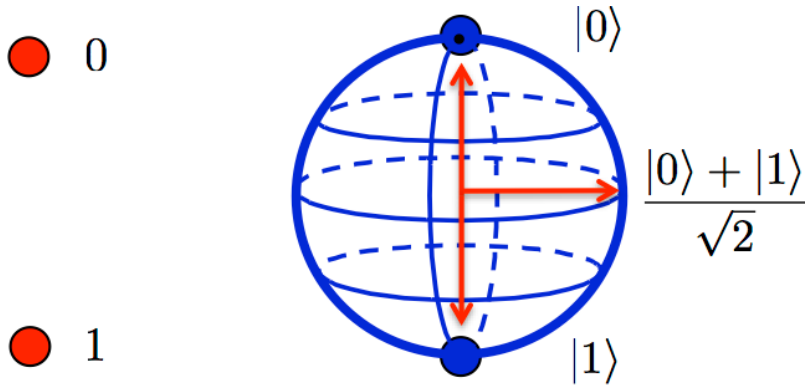
Comparisons

The realities of quantum computers

- Quantum computers are based on a different architecture of information, qubits:

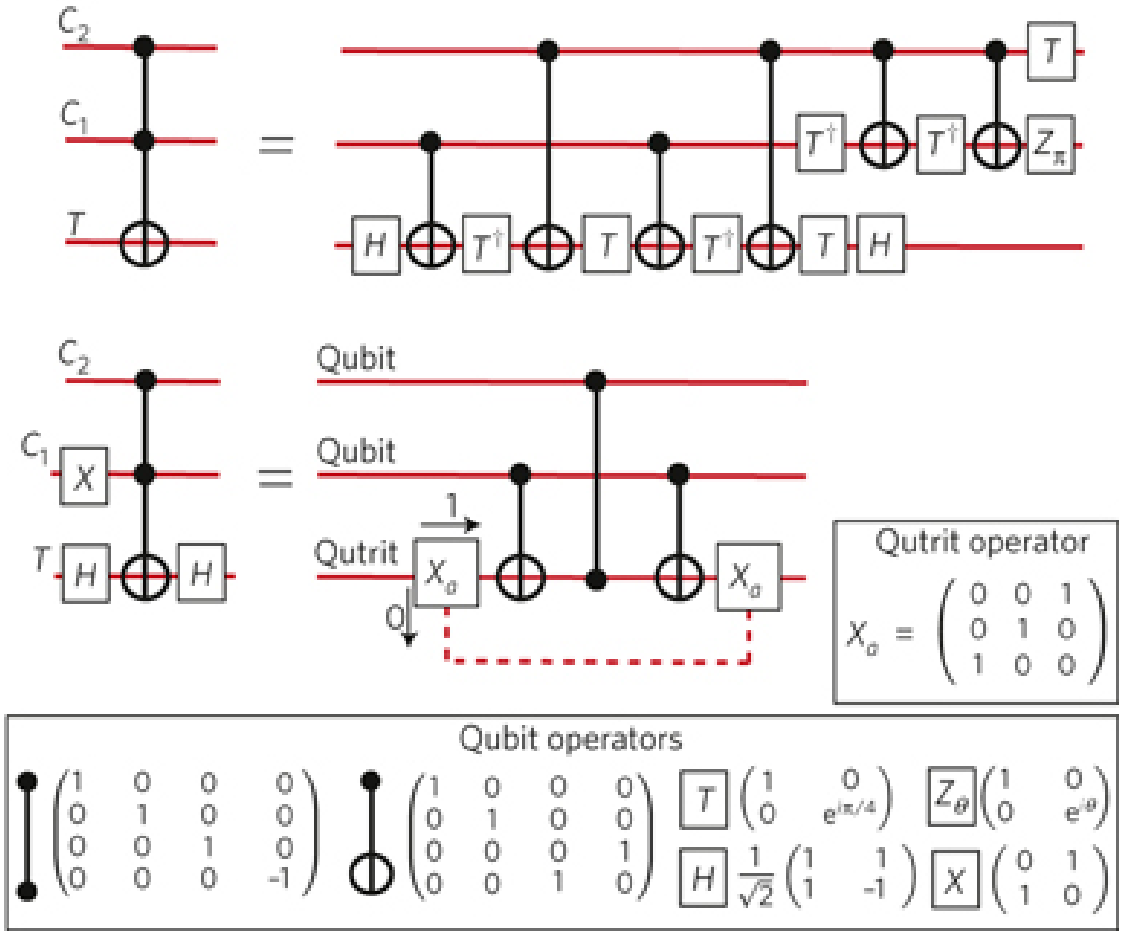


- Quantum computers are based on a different architecture of information, qubits:



- To realize such physical structures, new circuits and technology is needed.

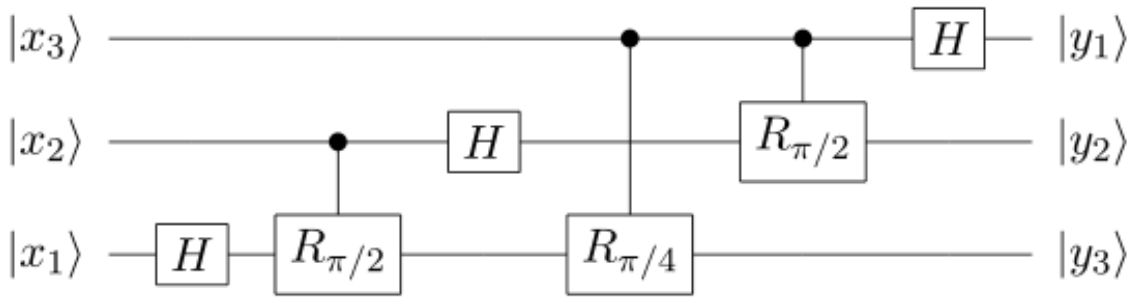
- Circuits do operations on qubits [1]:



[1] Simplifying quantum logic using higher-dimensional Hilbert spaces, *Nature Physics*, 5, 2009

- It turns out that some operations can be performed MUCH faster than before.

- It turns out that some operations can be performed MUCH faster than before.
- One important example:
  The discrete Fourier transform on 2^n amplitudes can be implemented on $\mathcal{O}(n^2)$ quantum gates vs $\mathcal{O}(n2^n)$ regular gates.



Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures

Comparisons

The realities of quantum computers

- Basically, a general algorithm that finds elements that map to a given answer given some function f.

- Basically, a general algorithm that finds elements that map to a given answer given some function f.
- This is interesting since f can be a cipher and we can search for the key used for encryption.

- Basically, a general algorithm that finds elements that map to a given answer given some function f.
- This is interesting since f can be a cipher and we can search for the key used for encryption.
- The complexity with which we can search is an improvement over what todays best algorithms can do:

$$\mathcal{O}(\sqrt{N}) \text{ versus } \mathcal{O}(N),$$

$(N = |dom(f)|)$.

- Shor's algorithm starts with a natural number N and finds a nontrivial divisor a such that $a \mid N$.

- Shor's algorithm starts with a natural number N and finds a nontrivial divisor a such that $a \mid N$.
- This is interesting to cryptographers because we may factor the modulus used in RSA, finding the private key as a result.

- Shor's algorithm starts with a natural number N and finds a nontrivial divisor a such that $a \mid N$.
- This is interesting to cryptographers because we may factor the modulus used in RSA, finding the private key as a result.
- The algorithm may also be used to find the discrete logarithm of group elements in certain classes of groups. This breaks many other asymmetric algorithms (including ECC).

- Shor's algorithm starts with a natural number N and finds a nontrivial divisor a such that $a \mid N$.
- This is interesting to cryptographers because we may factor the modulus used in RSA, finding the private key as a result.
- The algorithm may also be used to find the discrete logarithm of group elements in certain classes of groups. This breaks many other asymmetric algorithms (including ECC).
- The complexity of the algorithm is a *massive* improvement over the best factoring algorithms of today.

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures

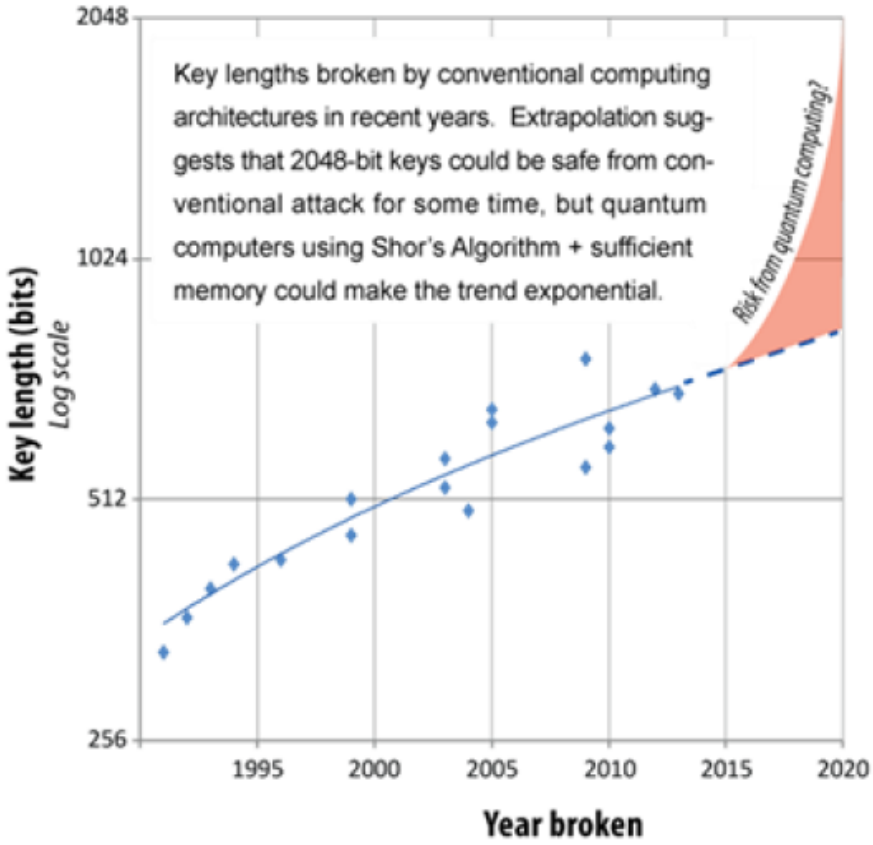
Comparisons

The realities of quantum computers

- For symmetric algorithms: The security is reduced by a square root.

[2] Quantum safe cryptography and security, *ETSI White paper no.8*

- For symmetric algorithms: The security is reduced by a square root.
- For popular asymmetric algorithms [2]:



[2] Quantum safe cryptography and security, *ETSI White paper no.8*

- For symmetric algorithms doubling the number of bits in keys will suffice.

- For symmetric algorithms doubling the number of bits in keys will suffice.
- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.

- For symmetric algorithms doubling the number of bits in keys will suffice.
- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.
- The search for these is ongoing.

- For symmetric algorithms doubling the number of bits in keys will suffice.
- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.
- The search for these is ongoing.
- There are several initiatives to pave the way for acceptable algorithms:

- For symmetric algorithms doubling the number of bits in keys will suffice.
- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.
- The search for these is ongoing.
- There are several initiatives to pave the way for acceptable algorithms:
  - NIST call for proposals is open until november 2017

- For symmetric algorithms doubling the number of bits in keys will suffice.
- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.
- The search for these is ongoing.
- There are several initiatives to pave the way for acceptable algorithms:
  - NIST call for proposals is open until november 2017
  - ETSI quantum safe cryptography group seeking standardization

- For symmetric algorithms doubling the number of bits in keys will suffice.
- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.
- The search for these is ongoing.
- There are several initiatives to pave the way for acceptable algorithms:
  - NIST call for proposals is open until november 2017
  - ETSI quantum safe cryptography group seeking standardization
  - PQCRYPTO project researching options and primitives

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures

Comparisons

The realities of quantum computers

- We would like

- We would like
  - Keys and signatures to be "small"

- We would like
  - Keys and signatures to be "small"
  - Ciphertext to be as small as possible

- We would like
  - Keys and signatures to be "small"
  - Ciphertext to be as small as possible
  - Encryption/decryption + signing/authenticating to be "fast"

- We would like
  - Keys and signatures to be "small"
  - Ciphertext to be as small as possible
  - Encryption/decryption + signing/authenticating to be "fast"
  - Key/signature generation to be "fast"

- We would like
  - Keys and signatures to be "small"
  - Ciphertext to be as small as possible
  - Encryption/decryption + signing/authenticating to be "fast"
  - Key/signature generation to be "fast"
  - Security to be founded on problems that we trust to be hard

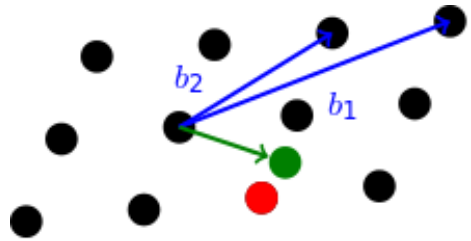
- We would like
  - Keys and signatures to be "small"
  - Ciphertext to be as small as possible
  - Encryption/decryption + signing/authenticating to be "fast"
  - Key/signature generation to be "fast"
  - Security to be founded on problems that we trust to be hard
- This is not straightforward but alternatives are being researched, as we will see.

- There are choices: McEliece- and Niederreiter-algorithms.

- There are choices: McEliece- and Niederreiter-algorithms.
- Quick facts:
  - Private key: Matrices G, P, S (G a linear code)
  - Public key: $(G' = S \circ G \circ P, t)$ where t is a parameter
  - Security based on the hardness of decoding random linear codes (an old problem)
  - Possibility of choosing between different codes, but this might be questionable with respect to security
  - The matrices are very large

- There are several choices: Ring-LWE, GGH, NTRU.

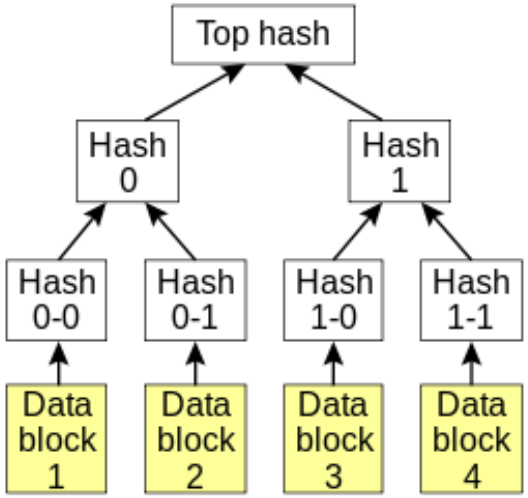
- There are several choices: Ring-LWE, GGH, NTRU.
- Quick facts:
  - Encryption/decryption involves manipulating points in a lattice:



  - Security based on the hardness of problems in lattices (SVP,CVP,LWE, SIS or approximate versions)
  - More efficient versions using lattices from polynomial rings, but security in question..

- Merkle signatures.

- Merkle signatures.
- Quick facts:
  - We build a Merkle-tree from one-time signatures (Lamport, Winternitz..):



  - We obtain but a finite number of signatures for a given public key
  - Large signature if the tree grows big
  - Security based on the strength of cryptographic hash functions

- Encryption[3]:

Algorithm	KeyGen (time compared to RSA decrypt)	Decryption (time compared to RSA decrypt)	Encryption (time compared to RSA decrypt)	PubKey (key size in bits to achieve 128 bits of security)	PrivateKey (key size in bits to achieve 128 bits of security	Cipher text (size of resulting cipher text)	Time Scaling	Key Scaling
NTRU	5	0.05	0.05	4939	1398	4939	k^2	k
McEliece	2	0.5	0.01	1537536	64861	2860	k^2	k^2
Quasi-Cyclic MDPC McEliece	5	0.5	0.1	9857	19714	19714	k^2	k
RSA	50	1	0.01	3072	24,576	3072	k^6	k^3
DH	0.2	0.2	0.2	3072	3238	3072	k^4	k^3
ECDH	0.05	0.05	0.05	256	256	512	k^2	k

[3]Quantum safe cryptography and security, *ETSI White paper no.8*

- Signatures[4]:

Algorithm	Num of sign	Key Gen (time compared to RSA sign)	Signing (time compared to RSA sign)	Verifying (time compared to RSA sign)	PubKey (size in bits to achieve 128 bits of security)	PrivateKey (size in bits to achieve 128 bits of security	Signature (size in bits of resulting digital signature)	Time Scaling	Key Scaling
XMSS signatures (hash based)	2^{20}	100000	2	0.2	7296	152	19608	k^2	k^2
BLISS (lattice-based)		0.005	0.02	0.01	7000	2000	5600	k^2	k
Rainbow signature (multivariate)		20	0.02	0.02	842400	561352	264	k^3	k^3
RSA		50	1	0.01	3072	24,576	3072	k^6	k^3
DSA		0.2	0.2	0.2	3072	3328	3072	k^4	k^3
ECDSA		0.05	0.05	0.05	512	768	512	k^2	k

[4] Quantum safe cryptography and security, *ETSI White paper no.8*

- Key observations:
  - Keys/signatures are BIG

- Key observations:
  - Keys/signatures are BIG
  - Ciphertext is BIG

- Key observations:
  - Keys/signatures are BIG
  - Ciphertext is BIG
  - Time consumption is not a big issue (in some cases faster than classical algorithms)

- Key observations:
  - Keys/signatures are BIG
  - Ciphertext is BIG
  - Time consumption is not a big issue (in some cases faster than classical algorithms)
  - Security based on problems that MAY be quantum resistant

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover's algorithm

Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures

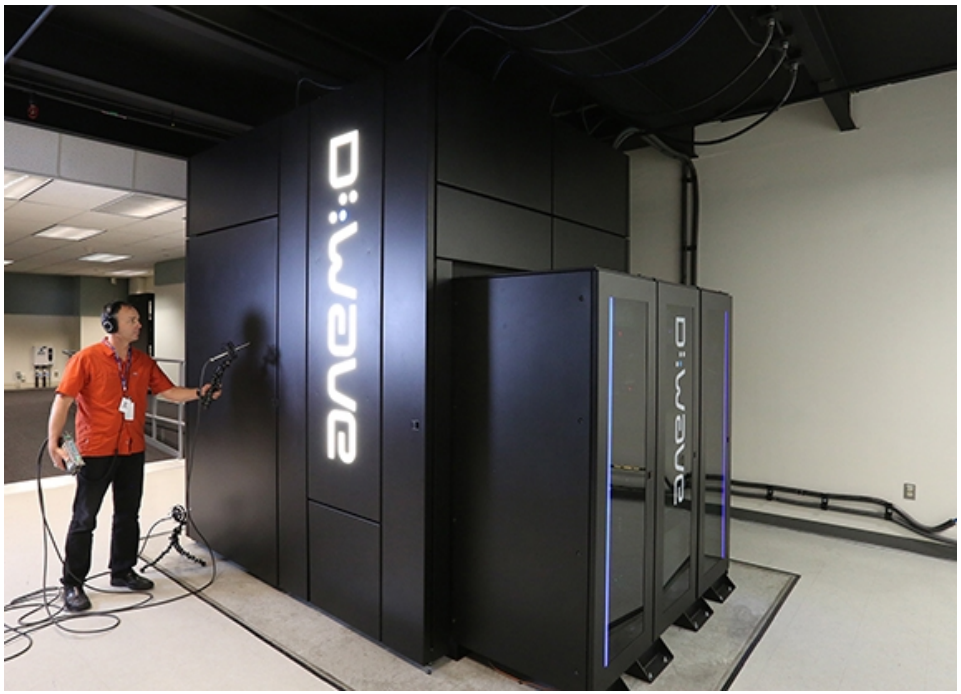
Comparisons

The realities of quantum computers

- Research into the implementation of quantum circuits is highly active.

[5] https://www.dwavesys.com

- Research into the implementation of quantum circuits is highly active.
- An immature example [5]:



[5] https://www.dwavesys.com

- There are several different computing models to try:
  - Quantum Gate Array
  - Measurement Based Quantum Computer
  - Adiabatic Quantum Computer
  - Topological Quantum Computer

- There are several different computing models to try:
  - Quantum Gate Array
  - Measurement Based Quantum Computer
  - Adiabatic Quantum Computer
  - Topological Quantum Computer
- And, several possible physical implementations:
  - Superconductor-based quantum computer
  - Trapped ion quantum computer
  - Optical lattices
  - Quantum dot computer
  - Many more..

- All alternatives run into problems, e.g:
  - Quantum decoherence, stability of qubits
  - Scalability

- All alternatives run into problems, e.g:
  - Quantum decoherence, stability of qubits
  - Scalability
- Despite of difficulties, there is heavy investment in the field (Google, IBM, Lockheed Martin, governments).

- All alternatives run into problems, e.g:
  - Quantum decoherence, stability of qubits
  - Scalability
- Despite of difficulties, there is heavy investment in the field (Google, IBM, Lockheed Martin, governments).
- Consensus points to the strong possibility of overcoming the problem barrier.

- It is not easy to determine *when* a practical and relevant quantum computer is ready.

- It is not easy to determine *when* a practical and relevant quantum computer is ready.
- There is a certain consensus pointing to 2030 as a realistic time frame.

- It is not easy to determine *when* a practical and relevant quantum computer is ready.
- There is a certain consensus pointing to 2030 as a realistic time frame.
- More important to us: We need flexibility so that we may choose different algorithms when needed.

Summary

- Quantum computers force new algorithms upon us.

Summary

- Quantum computers force new algorithms upon us.
- We do not know exactly *when* they are here, but we need to be ready.

Summary

- Quantum computers force new algorithms upon us.
- We do not know exactly *when* they are here, but we need to be ready.
- We should pay close attention to standards in the making.