Thomas Gregersen

February 28, 2017



The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

computers

New algorithms
Grover's algorithm
Shor's algorithm

The impact on classical cryptogra

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

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 effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

Asymmetric
cryptography
Digital signatures

Quantum computer

> troduction ew algorithms Grover's algorith

The impact on lassical crypto

classical cry

ost-quantur ryptography

ost-quantum ryptography

ryptography Code-based cryptosystems

cryptosystems Lattice-based

cryptosystems Hash-based

signatures Comparisons

Comparisons

uantum compi

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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography odav

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantun

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures
Comparisons
The realities of quantum computs

- ▶ 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.

Thomas Gregersen

Introduction

Overview

Cryptography today

Symmetric cryptography

The effect of quantum algorithms

Thomas Gregersen

Symmetric cryptography

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



The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography Digital signatures Measuring security

Quantum

New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

Overview

Cryptography today

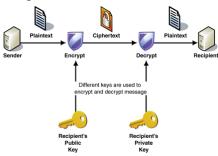
Asymmetric cryptography

The effect of quantum algorithms

Thomas Gregersen

Asymmetric cryptography

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



The effect of quantum algorithms

Thomas Gregersen

troduction

Cryptograp today

Symmetric

Asymmetric cryptography Digital signatures

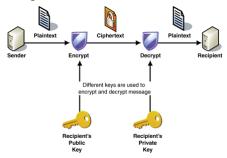
Quantum

Introduction

New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons ➤ 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.

The effect of quantum algorithms

Thomas Gregersen

troduction

Cryptogra_l today

Symmetric

Asymmetric cryptography

Digital signatu Measuring sec

computers

Introduction

New algorithms
Grover's algorithm

The impact on classical cryptograp

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures ► There are several algorithms to choose from: RSA, Diffie-Hellman, ElGamal, ECC...

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

Symmetric cryptography
Asymmetric

cryptography
Digital signatures
Measuring securi

computer

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

► 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.

The effect of quantum algorithms

Thomas Gregersen

Introduction

today
Symmetric
cryptography

Asymmetric cryptography Digital signatures Measuring security

Quantum

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

► 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.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Symmetric cryptography Asymmetric cryptography Digital signatures

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

Fhe path to oost-quantum cryptography Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

Overview

Cryptography today

Digital signatures

The effect of quantum algorithms

Thomas Gregersen

Digital signatures

► A standard technique to check authenticity: They are usually based on asymmetric cryptographic algorithms, e.g:

- RSA
- DSA
- ECDSA

The effect of quantum algorithms

Thomas Gregersen

Digital signatures

Overview

Cryptography today

Measuring security

The effect of quantum algorithms

Thomas Gregersen

Measuring 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).

The effect of quantum algorithms

Thomas Gregersen

troduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

)...ant...m

omputers

roduction w algorithms

Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons The realities of

- 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		crete arithm 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.

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Measuring sec

omputers

Introduction

New algorithms

Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography

Code-based cryptosystems Lattice-based cryptosystems

signatures
Comparisons

The realities of

- 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		crete arithm 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.

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

yptography symmetric yptography igital signature

Measuring security

Quantum

omputers

New algorithms
Grover's algorithm

The impact on classical cryptograph

he path to ost-quantum

Post-quantum cryptography

Code-based cryptosystems Lattice-based cryptosystems

Hash-based signatures

The realities of

Overview

Quantum computers

Introduction

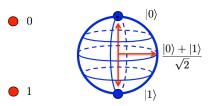
New algorithms

The effect of quantum algorithms

Thomas Gregersen

Introduction

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



The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

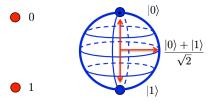
computer

Introduction

Grover's algorithm
Shor's algorithm
The impact on classical cryptography

he path to ost-quantur

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons Quantum computers are based on a different architecture of information, qubits:



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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Introduction

Introduction

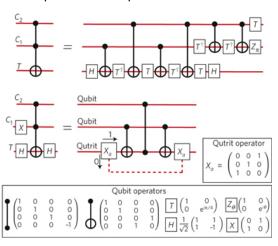
Grover's algorithm
Shor's algorithm
The impact on
classical cryptography

The path to post-quantum ryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems

Comparisons

Circuits do operations on qubits 1:



The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

Introduction

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

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

Thomas Gregersen

Introduction

Cryptography coday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

Introduction

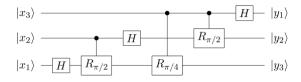
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

► 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.



Thomas Gregersen

Introduction

Cryptography oday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

compute

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

Overview

Quantum computers

New algorithms

The effect of quantum algorithms

Thomas Gregersen

New algorithms

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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum computer:

Introduction

New algorithms Grover's algorithm

Shor's algorithm The impact on Lassical cryptography

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons The realities of quantum compute

▶ 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 effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

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

- ▶ 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:

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

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

Thomas Gregersen

Introduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantun

Introduction

Grover's algorithm Shor's algorithm The impact on

The path to

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures

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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computer

Introduction

Grover's algorithm

Shor's algorithm

Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons The realities of

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

Thomas Gregersen

ntroduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

compute

New algorithms
Grover's algorithm
Shor's algorithm

hor's algorithm he impact on

The path to

ryptography
Post-quantum
cryptography
Code-based
cryptosystems
Lattice-based
cryptosystems
Hash-based
signatures
Comparisons
The realities of
quantum compute

- ▶ 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).

Thomas Gregersen

Shor's algorithm

- ► Shor's algorithm starts with a natural number *N* and finds a nontrivial divisor *a* such that *a* | *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.

Thomas Gregersen

Introduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantu

Introduction
New algorithms
Grover's algorithm
Shor's algorithm

The impact on lassical cryptography

The path to

oost-quantum
cryptography
Post-quantum
cryptography
Post-quantum
cryptography
Code-based
cryptosystems
Lattice-based
cryptosystems
Hash-based
signatures
Comparisons
The realities of

Overview

Quantum computers

The impact on classical cryptography

The effect of quantum algorithms

Thomas Gregersen

The impact on classical cryptography

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

Thomas Gregersen

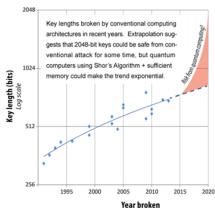
The impact on

classical cryptography

The effect of quantum algorithms

²Quantum 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:



Thomas Gregersen

ntroduction

Cryptography

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

he realities of

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

Thomas Gregersen

Introduction

Cryptography today

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

ntroduction lew algorithms Grover's algorithm

The impact on classical cryptography

The path to post-quantum

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures
Comparisons
The realities of

► 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 effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

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

- For regular asymmetric algorithms it becomes impractical to extend keys, so we need new alternatives.
- ▶ The search for these is ongoing.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

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

- 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:

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Compute

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

- 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

The effect of quantum algorithms

Thomas Gregersen

Introduction

ryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

compute

Introduction
New algorithms
Grover's algorithm
Shor's algorithm

The impact on classical cryptography

The path to post-quantum cryptography
Post-quantum cryptography

cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

- 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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

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

- 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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

compute

Introduction
New algorithms
Grover's algorithm
Shor's algorithm

The impact on classical cryptography

The path to cost-quantum cryptography
Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems

Overview

Introduction

Cryptography today

Symmetric cryptography

Asymmetric cryptography

Digital signatures

Measuring security

Quantum computers

Introduction

New algorithms

Grover'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 computer

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography codav

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum computer

ntroduction

New algorithms
Grover's algorithm
Shor's algorithm

lassical crypto

post-quantum cryptography

Post-quantum cryptography

cryptography Code-based

cryptosystems Lattice-based

cryptosystem Hash-based

signatures

e realities

Thomas Gregersen

Introduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantur

New algorithms
Grover's algorithm
Shor's algorithm

post-quantur cryptography

Post-quantum cryptography

Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

▶ We would like

Thomas Gregersen

Introduction

We would like

Keys and signatures to be "small"

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum

ntroduction

New algorithms
Grover's algorithm
Shor's algorithm
The impact on

post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

> he realities of uantum compi

- Keys and signatures to be "small"
- ► Ciphertext to be as small as possible

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum computers

troduction ew algorithms

Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography

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

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

compute

New algorithms Grover's algorithm Shor's algorithm The impact on

ost-quantum ryptography

Post-quantum cryptography

- 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"

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantur

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

ost-quantum ryptography

Post-quantum cryptography

- 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

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum

omputers

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on
classical cryptograph

ost-quantum ryptography

Post-quantum cryptography

- 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.

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum computers

Introduction New algorithms Grover's algorithm Shor's algorithm The impact on

The path to post-quantum

Post-quantum cryptography

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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

computers

computers

New algorithms Grover's algorithm Shor's algorithm The impact on

The path to post-quantum cryptography

Post-quantum cryptography

Code-based cryptosystems

> Hash-based signatures Comparisons

> > he realities of

► 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

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum computer

New algorithms
Grover's algorithm
Shor's algorithm
The impact on
classical cryptography

post-quantum cryptography

cryptography

Code-based

Code-based cryptosystems

Hash-based signatures

he realities of uantum compu

Thomas Gregersen

Introduction

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

Cryptography today

symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum

omputers

New algorithms Grover's algorithm Shor's algorithm The impact on

The path to post-quantum

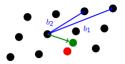
Post-quantum cryptography Code-based cryptosystems

Lattice-based cryptosystems

Hash-based signatures Comparisons The realities of

▶ 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..

The effect of quantum algorithms

Thomas Gregersen

Introduction

ryptography oday

cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum

New algorithms
Grover's algorithm
Shor's algorithm
The impact on
classical cryptography

The path to post-quantum cryptography

cryptography Code-based cryptosystems

Lattice-based cryptosystems Hash-based signatures Comparisons Merkle signatures.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

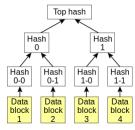
The path to post-quantum

Post-quantum cryptography Code-based cryptosystems Lattice-based

Hash-based signatures

The realities of

- 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

Thomas Gregersen

ntroduction

Cryptography coday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

ntroduction

Grover's algorithm Shor's algorithm The impact on

The path to post-quantum

cryptography

cryptography Code-based cryptosystems Lattice-based

Hash-based signatures

he realities of

► Encryption³:

	J C. O							
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	<i>k</i> 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

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptography

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum compute

New algorithms Grover's algorithm Shor's algorithm

The impact on classical cryptogra

oost-quantun cryptography -

Post-quantum rryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

Comparisons The realities of

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

► Signatures⁴:

0		-							
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)	220	100000	2	0.2	7296	152	19608	k²	k²
BLISS (lattice- based)		0.005	0.02	0.01	7000	2000	5600	k²	k
Rainbow signature (multivariate)		20	0.02	0.02	842400	561352	264	k³	k³
RSA		50	1	0.01	3072	24,576	3072	k ⁶	k³
DSA		0.2	0.2	0.2	3072	3328	3072	k ⁴	k³
ECDSA		0.05	0.05	0.05	512	768	512	k²	k

The effect of quantum algorithms

Thomas Gregersen

ntroduction

Cryptograph

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computer

New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path t

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

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

Comparisons
The realities of

Thomas Gregersen

Introduction

Cryptography today

Key observations:

► Keys/signatures are BIG

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantun

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

Thomas Gregersen

Introduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantun

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantur

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

The realities of quantum computers

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)

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography today

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

The realities of

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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum computers

New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

Comparisons The realities of

Overview

The path to post-quantum cryptography

The realities of quantum computers

The effect of quantum algorithms

Thomas Gregersen

The realities of quantum computers ► Research into the implementation of quantum circuits is highly active.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

ntroduction Iew algorithms Grover's algorithm

Shor's algorithm
The impact on

The path to post-quantum

ryptography
Post-quantum
ryptography
Code-based
cryptosystems
Lattice-based
cryptosystems
Hash-based
signatures
Comparisons

The realities of

quantum computers

⁵https://www.dwavesys.com

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



Thomas Gregersen

ntroduction

Cryptography oday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum computers

New algorithms
Grover's algorithm
Shor's algorithm
The impact on
classical cryptography

The path to post-quantu cryptograph

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based

The realities of quantum computers

Thomas Gregersen

The realities of

quantum computers

▶ There are several different computing models to try:

Quantum Gate Array

▶ Measurement Based Quantum Computer

Adiabatic Quantum Computer

► Topological Quantum Computer

Thomas Gregersen

Introduction

Cryptography oday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantur

Introduction New algorithms Grover's algorithm

Shor's algorithm The impact on

The path to

ost-quantur ryptography

rost-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures

Comparisons
The realities of guantum computers

▶ 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

Thomas Gregersen

Introduction

Cryptography coday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures Comparisons

quantum computers

▶ 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).

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum computer

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures

The realities of guantum computers

► 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.

The effect of quantum algorithms

Thomas Gregersen

ntroduction

ryptography oday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

computers

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

ryptography
Post-quantum
cryptography
Code-based
cryptosystems
Lattice-based
cryptosystems
Hash-based
signatures

The realities of guantum computers

Thomas Gregersen

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

The path to post-quantum

Post-quantum
Post-quantum
Code-based
cryptosystems
Lattice-based
cryptosystems
Hash-based
signatures
Comparisons
The realities of

quantum computers

▶ 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.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

Symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures
Comparisons
The realities of quantum computers

▶ 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.

The effect of quantum algorithms

Thomas Gregersen

Introduction

ryptography oday

symmetric cryptography Asymmetric cryptography Digital signatures Measuring security

Quantum computer

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum cryptography

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures
Comparisons
The realities of

quantum computers

Summary

Quantum computers force new algorithms upon us.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum computers

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to post-quantum

Post-quantum cryptography
Code-based cryptosystems
Lattice-based cryptosystems
Hash-based signatures
Comparisons
The realities of

Summary

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

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantum

Introduction
New algorithms
Grover's algorithm
Shor's algorithm
The impact on
classical cryptography

he path to ost-quantum

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.

The effect of quantum algorithms

Thomas Gregersen

Introduction

Cryptography coday

cryptography
Asymmetric
cryptography
Digital signatures
Measuring security

Quantur

New algorithms
Grover's algorithm
Shor's algorithm
The impact on

The path to

Post-quantum cryptography Code-based cryptosystems Lattice-based cryptosystems Hash-based signatures