Towards new security standards

Jean-Christophe Deneuville

<jean-christophe.deneuville@enac.fr>

September the 19th, 2019

Les communautés d'experts

Outline

1 Overview of the main security aspects

2 Quantum computers and their impact over current security

3 Counter-measures and work in progress

Outline

1 Overview of the main security aspects

2 Quantum computers and their impact over current security

3 Counter-measures and work in progress

Security goals

Computer security has for main objectives :

- Confidentiality
- Authentication
- Integrity
- Non-repudiation / Traceability / Accountability

Security goals

Computer security has for main objectives :

- Confidentiality
- Authentication
- Integrity
- Non-repudiation / Traceability / Accountability

Cryptographic mecanisms involved

Security goals

Computer security has for main objectives :

- **Confidentiality**
- **Authentication**
- Integrity
- Non-repudiation / Traceability / Accountability

Cryptographic mecanisms involved

(Modern) encryption (see below)

Security goals

Computer security has for main objectives :

- Confidentiality
- **Authentication**
- **Integrity**
- **Non-repudiation / Traceability / Accountability**

Cryptographic mecanisms involved

Digital signature (see below)

Security goals

Computer security has for main objectives :

- Confidentiality
- **Authentication**
- **Integrity**
- **Non-repudiation / Traceability / Accountability**

Cryptographic mecanisms involved

(Collision-resistant) hash functions

Modern cryptographic schemes

1975	**D**ata **E**ncryption **S**tandard (DES)
1976	**D**iffie-**H**elmann (DH) key exchange protocol
1978	**R**ivest **S**hamir **A**dleman (RSA)
1991	**I**nternational **D**ata **E**ncryption **A**lgorithm (IDEA)
1991	**D**igital **S**ignature **A**lgorithm (DSA)
1992	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm (ECDSA)
1993	Blowfish
1999	Triple-DES

Legend :
- symmetric scheme
- asymmetric scheme

Current security

Current security vs. computing power (2019)

Current security vs. computing power (2019)

1 standard machine : 64 bits architecture

2^6

Current security vs. computing power (2019)

1 standard machine : 8 cores

$2^6 \times 2^4$

Current security vs. computing power (2019)

1 standard machine : 4 GHz

$2^6 \times 2^4 \times 2^2 \times 10^9$

Current security vs. computing power (2019)

1 standard machine : running 1 month

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30$

Current security vs. computing power (2019)

NSA $\geq$ 10 000 standard machines ?

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30 \times 10^5$

Current security vs. computing power (2019)

NSA $\geq$ 10 000 standard machines ?

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30 \times 10^5 \approx 2^{80}$ elementary operations

Current security vs. computing power (2019)

NSA $\geq$ 10 000 standard machines ? (without possible GPU, ASICS, ...)

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30 \times 10^5 \approx 2^{80}$ elementary operations

Current security vs. computing power (2019)

NSA $\geq$ 10 000 standard machines ? (without possible GPU, ASICS, ...)

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30 \times 10^5 \approx 2^{80}$ elementary operations

A concrete example

During 2018, there were 2^{89} SHA-256 hashes computed on the blockchain BitCoin...

Current security vs. computing power (2019)

NSA $\geq$ 10 000 standard machines ? (without possible GPU, ASICS, ...)

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30 \times 10^5 \approx 2^{80}$ elementary operations

A concrete example

During 2018, there were 2^{89} SHA-256 hashes computed on the blockchain BitCoin...

Security in 2019

Setting parameters so that best known attacks have complexity (at least) 2^{128}.

Current security vs. computing power (2019)

NSA $\geq$ 10 000 standard machines ? (without possible GPU, ASICS, ...)

$2^6 \times 2^4 \times 2^2 \times 10^9 \times 60 \times 60 \times 24 \times 30 \times 10^5 \approx 2^{80}$ elementary operations

A concrete example

During 2018, there were 2^{89} SHA-256 hashes computed on the blockchain BitCoin...

Security in 2019

Setting parameters so that best known attacks have complexity (at least) 2^{128}.

Classical best known attacks :

- Symmetric primitives : brute-force
- Asymmetric primitives : GNFS, sub-exponential complexity

Outline

1 Overview of the main security aspects

2 Quantum computers and their impact over current security

3 Counter-measures and work in progress

Better quantum algorithms

Better quantum algorithms

- 1975 **D**ata **E**ncryption **S**tandard (DES)
- 1976 **D**iffie-**H**elmann (DH) key exchange protocol
- 1978 **R**ivest **S**hamir **A**dleman (RSA)
- 1991 **I**nternational **D**ata **E**ncryption **A**lgorithm (IDEA)
- 1991 **D**igital **S**ignature **A**lgorithm (DSA)
- 1992 **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm (ECDSA)
- 1993 Blowfish
- 1999 Triple-DES

Better quantum algorithms

1976 **D**iffie-**H**elmann (DH) key exchange protocol

1978 **R**ivest **S**hamir **A**dleman (RSA)

1991 **D**igital **S**ignature **A**lgorithm (DSA)

1992 **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm (ECDSA)

Better quantum algorithms

1976	**D**iffie-**H**elmann (DH) key exchange protocol
1978	**R**ivest **S**hamir **A**dleman (RSA)
1991	**D**igital **S**ignature **A**lgorithm (DSA)
1992	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm (ECDSA)
1994	**Shor's algorithm** [Sho97]
1996	**Grover's algorithm** [Gro96]

Shor's algorithm

SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1484–1509, October 1997

© 1997 Society for Industrial and Applied Mathematics
009

POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER*

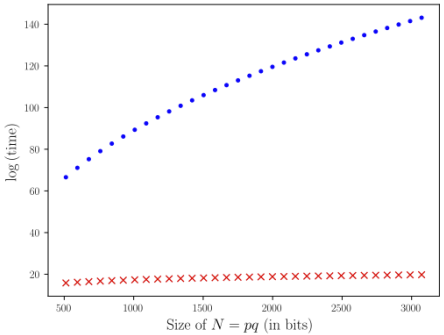
PETER W. SHOR†

Abstract. A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Consequences of Shor's algorithm on PKC

- Factoring becomes polynomial-time
- Discrete logarithm becomes almost polynomial-time

In other words, **security as we know it becomes down**...



Grover's algorithm

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Summary

Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

Consequences of Grover's algorithm

(n-entries) Database search takes $\mathcal{O}(\sqrt{n})$ queries instead of $\mathcal{O}(n)$.

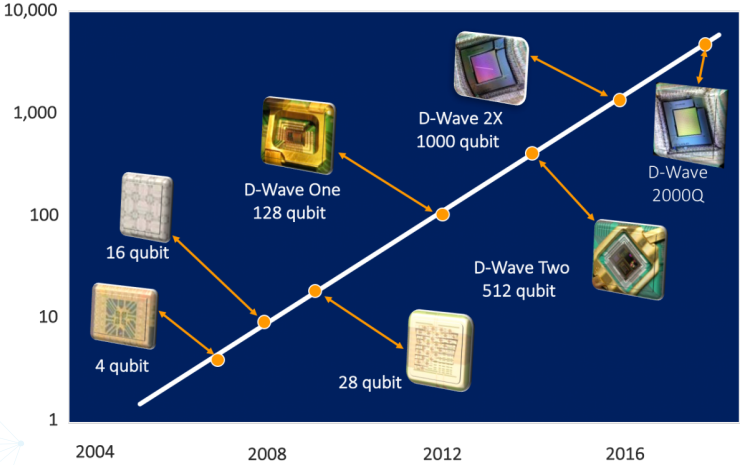
Consequence over symmetric crypto :

→ The length of the secret key must be **doubled** to preserve the same level of security

Consequence over hash functions :

→ More tricky (depending on the model, the size of the quantum computer, ...), at least +33% to preserve the security level

How far are we from a large-scale quantum computer ?



Analog to Moore's law for quantum computing : the number of qubits (y-axe, logarithmic scale) approximately doubles every year (x-axe). (Source : D-Wave)

Large-scale quantum computing : a caveat

This analog to Moore's law has several drawbacks :

- essentially corresponds to multiple 32 qubits architectures mounted in parallel
- fault-tolerance remains an open problem
- still far from what is required to factor 2048 bits moduli

In 2019, the largest quantum computer features 72 qubits (Google).

Open challenges towards quantum computing

More work in required to embrace a large scale quantum computer :

- the developing error-correcting codes for error-free quantum computing
- building architectures and interfaces between quantum computers and communication systems
- developing reliable quantum memories
- developing quantum programming languages, compilers and middle-ware stack

Open challenges towards quantum computing

More work in required to embrace a large scale quantum computer :

- the developing error-correcting codes for error-free quantum computing
- building architectures and interfaces between quantum computers and communication systems
- developing reliable quantum memories
- developing quantum programming languages, compilers and middle-ware stack

Still, a Sword of Damocles hanging over our heads

Open challenges towards quantum computing

More work in required to embrace a large scale quantum computer :

- the developing error-correcting codes for error-free quantum computing
- building architectures and interfaces between quantum computers and communication systems
- developing reliable quantum memories
- developing quantum programming languages, compilers and middle-ware stack

Still, a Sword of Damocles hanging over our heads, and **now** is the time for designing **quantum-safe** alternatives.

Outline

1 Overview of the main security aspects

2 Quantum computers and their impact over current security

3 Counter-measures and work in progress

In the meantime, other algorithms...

1978 — **R**ivest **S**hamir **A**dleman (RSA) [RSA78]

1991 — **I**nternational **D**ata **E**ncryption **A**lgorithm (IDEA)

In the meantime, other algorithms...

- 1978 — **R**ivest **S**hamir **A**dleman (RSA) [RSA78]
- 1978 — McEliece cryptosystem (error-correcting codes) [McE78]
- 1979 — Lamport (one-time) signature scheme (hash based) [Lam79]
- 1988 — C^* cryptosystem (multivariate) [MI88]
- 1991 — **I**nternational **D**ata **E**ncryption **A**lgorithm (IDEA)
- 1996 — NTRU cryptosystem (lattices) [HPS98]
- 2006 — Isogeny based encryption [RS06]

Using different primitives

The aforementioned schemes are based upon :

- euclidean lattices,
- error-correcting codes,
- security of hash functions,
- multivariate polynomials,
- supersingular isogenies.

Until now, **none** of these primitives are known to allow **quantum speedups**.

Standardization ongoing...

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

`https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm`

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round

Standardization ongoing...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)

Main candidates' features

Hard to make general statements about post-quantum crypto standards as each primitive has its pros and cons.

Main candidates' features

Hard to make general statements about post-quantum crypto standards as each primitive has its pros and cons.

But, generally speaking :

Main candidates' features

Hard to make general statements about post-quantum crypto standards as each primitive has its pros and cons.

But, generally speaking :

→ Expect larger public keys ⇒ increase storage capacity

Main candidates' features

Hard to make general statements about post-quantum crypto standards as each primitive has its pros and cons.

But, generally speaking :

→ Expect larger public keys ⇒ increase storage capacity

→ Expect larger ciphertexts ⇒ increase bandwidth

Main candidates' features

Hard to make general statements about post-quantum crypto standards as each primitive has its pros and cons.

But, generally speaking :

→ Expect larger public keys ⇒ increase storage capacity

→ Expect larger ciphertexts ⇒ increase bandwidth

→ Expect smaller moduli ⇒ room for faster algorithms

A team of experts next to you

Carlos Aguilar Melchor (ISAE-Supaéro) and myself (ÉNAC) are involved (together with a lot of people) in NIST's standardization process :

- 4 submissions still in race for standardization (2^{nd} round)
- Provide either encryption or key-exchange
- Some of our candidates feature best properties among all candidates

A team of experts next to you

Carlos Aguilar Melchor (ISAE-Supaéro) and myself (ÉNAC) are involved (together with a lot of people) in NIST's standardization process :

- 4 submissions still in race for standardization (2nd round)
- Provide either encryption or key-exchange
- Some of our candidates feature best properties among all candidates

Together with Jérôme Lacan (ISAE-Supaéro), we are announcing the creation of a **workgroup around post-quantum cryptography**.

Stay tuned, or reach out directly to us if interested :
pqcrypto@recherche.enac.fr

Conclusion

To sum up :

Conclusion

To sum up :

- Current standards' security is well-studied/understood

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers
- We have time to widely deploy quantum-safe security

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers
- We have time to widely deploy quantum-safe security
- But not enough time to waste it : we must act now

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers
- We have time to widely deploy quantum-safe security
- But not enough time to waste it : we must act now
- Infrastructure will require some upgrades, we must anticipate them

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers
- We have time to widely deploy quantum-safe security
- But not enough time to waste it : we must act now
- Infrastructure will require some upgrades, we must anticipate them
- Quantum-safe primitives are undergoing a thorough standardization process

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers
- We have time to widely deploy quantum-safe security
- But not enough time to waste it : we must act now
- Infrastructure will require some upgrades, we must anticipate them
- Quantum-safe primitives are undergoing a thorough standardization process
- Local experts next to you are willing to help :)

Conclusion

To sum up :

- Current standards' security is well-studied/understood
- There is a growing threat with quantum computers
- We have time to widely deploy quantum-safe security
- But not enough time to waste it : we must act now
- Infrastructure will require some upgrades, we must anticipate them
- Quantum-safe primitives are undergoing a thorough standardization process
- Local experts next to you are willing to help :)

Thanks !

Références I

Lov K. Grover.
A fast quantum mechanical algorithm for database search.
In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman.
Ntru : A ring-based public key cryptosystem.
In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer, 1998.

Leslie Lamport.
Constructing digital signatures from a one-way function.
Technical report, 1979.

Robert J. McEliece.
A public key cryptosystem based on algebraic coding theory.
In *Jet Propulsion Laboratory DSN Progress Report*, pages 42–44, 1978.

Tsutomu Matsumoto and Hideki Imai.
Public quadratic polynomial-tuples for efficient signature-verification and message-encryption.
In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.

Alexander Rostovtsev and Anton Stolbunov.
Public-key cryptosystem based on isogenies.
Cryptology ePrint Archive, Report 2006/145, 2006.
https://eprint.iacr.org/2006/145.

Ronald L Rivest, Adi Shamir, and Leonard Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Communications of the ACM, 21(2) :120–126, 1978.

Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5) :1484–1509, 1997.