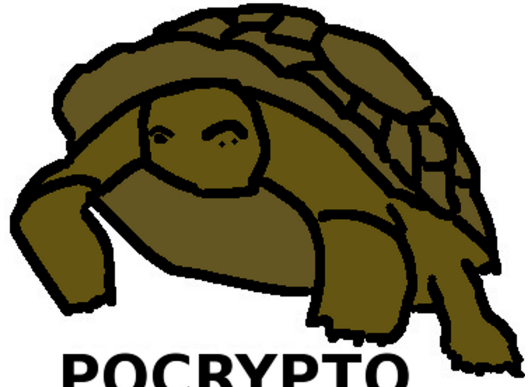
Post-quantum crypto
Summary and recommendations

Tanja Lange

Technische Universiteit Eindhoven



28 September 2018

ENISA summer school
Disclaimer: these are my summaries of the talks

Cryptography

- Motivation #1: Communication channels are spying on our data.
- Motivation #2: Communication channels are modifying our data.

Sender
"Alice"

Untrustworthy network
"Eve"

Receiver
"Bob"

- Literal meaning of cryptography: "secret writing".
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Key size recommendations

	Parameter	Legacy	Future System Use	
			Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size*	m	80	128	256
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(p^{k \cdot n}) \geq$	1024	6144	15360
	$\ell(p), \ell(q) \geq$	160	256	512

- Source: ECRYPT-CSA "Algorithms, Key Size and Protocols Report" (2018).
- These recommendations take into account attacks known today.
- Use extrapolations to larger problem sizes.
- Attacker power typically limited to 2^{128} operations (less for legacy).
- More to come on long-term security ...

Cryptography

- Motivation #1: Communication channels are spying on our data.
- Motivation #2: Communication channels are modifying our data.

Sender
"Alice"

Untrustworthy network
"Eve"

Receiver
"Bob"

- Literal meaning of cryptography: "secret writing".
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Post-quantum cryptography

- Motivation #1: Communication channels are spying on our data.
- Motivation #2: Communication channels are modifying our data.

Sender
"Alice"

"Eve"
with a quantum computer

Receiver
"Bob"

- Literal meaning of cryptography: "secret writing".
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.
- Post-quantum cryptography adds to the model that Eve has a quantum computer.

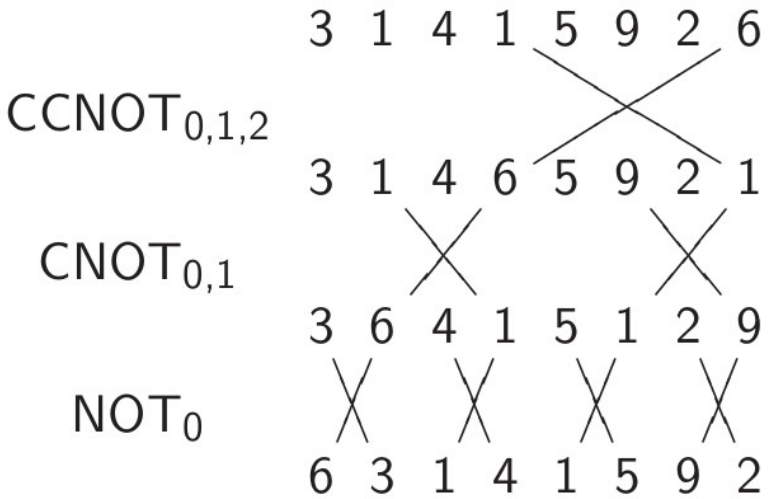
What do quantum computers do?

16

More shuffling

Combine NOT, CNOT, Toffoli
to build other permutations.

e.g. series of gates to
rotate 8 positions by distance 1:

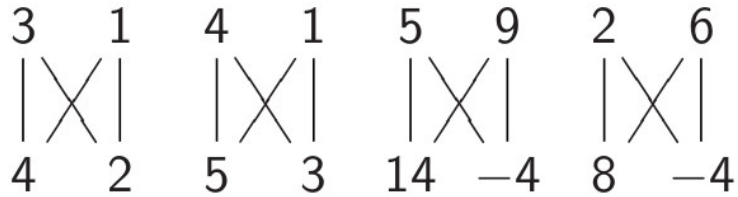


17

Hadamard gates

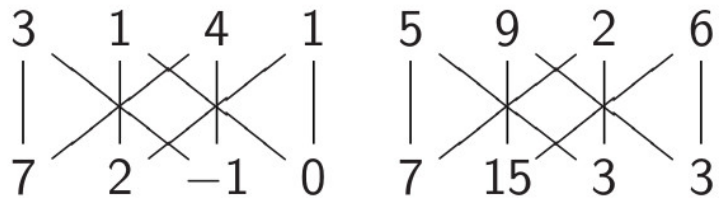
Hadamard$_0$:

$(a, b) \mapsto (a + b, a - b)$.



Hadamard$_1$:

$(a, b, c, d) \mapsto$
$(a + c, b + d, a - c, b - d)$.



Talk by Daniel J. Bernstein.

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of prob-

Attackers exploit physical reality

- 1996 Kocher: Typical crypto is broken by **side channels**.
- Response: Hundreds of papers on side-channel defenses.
- Today's focus: Large universal **quantum computers**.
- Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- Mark Ketchen, IBM Research, 2012, on quantum computing: "We're actually doing things that are making us think like, 'hey this isn't 50 years off, this is maybe just 10 years off, or 15 years off.' It's within reach."
- Fast-forward to 2022, or 2027. Universal quantum computers exist.
- Shor's algorithm solves in polynomial time:
  - Integer factorization. RSA is dead.
  - The discrete-logarithm problem in finite fields. DSA is dead.
  - The discrete-logarithm problem on elliptic curves. ECDHE is dead.
- This breaks all current public-key cryptography on the Internet!

Attackers exploit physical reality

- 1996 Kocher: Typical crypto is broken by **side channels**.
- Response: Hundreds of papers on side-channel defenses.
- Today's focus: Large universal **quantum computers**.
- Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- Mark Ketchen, IBM Research, 2012, on quantum computing: "We're actually doing things that are making us think like, 'hey this isn't 50 years off, this is maybe just 10 years off, or 15 years off.' It's within reach."
- Fast-forward to 2022, or 2027. Universal quantum computers exist.
- Shor's algorithm solves in polynomial time:
  - Integer factorization. RSA is dead.
  - The discrete-logarithm problem in finite fields. DSA is dead.
  - The discrete-logarithm problem on elliptic curves. ECDHE is dead.
- This breaks all current public-key cryptography on the Internet!
- Also, Grover's algorithm speeds up brute-force searches.
- Example: Only 2^{64} quantum operations to break AES-128; 2^{128} quantum operations to break AES-256.

Systems expected to survive

Overview of these systems in talk by Michael Groves.

- Code-based crypto, for details see talk by Daniel Loebenberger.
- Hash-based signatures, for details see talk by Stefan-Lukas Gazdag.
- Isogeny-based crypto: new kid on the block, promising short keys and key exchange without communication (static-static) as possibility; needs more research on security.
- Lattice-based crypto, for details see talks by Vadim Luybashevsky and Maire O'Neill.
- Multivariate crypto.
- Symmetric crypto.

Different recommendations for rollout:

- Vadim Luybashevsky: use most efficient systems with ECC or RSA, to ease usage and gain familiarity.
- Tanja Lange: use most conservative systems (possibly with ECC), to ensure that data really remains secure.

Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Güneysu, Shay Gueron, Andreas Hülsing, Tanja Lange, Mohamed Saied Emam Mohamed, Christian Rechberger, Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, Bo-Yin Yang

Initial recommendations

- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key

  Evaluating: Serpent-256, ...
- **Symmetric authentication** Information-theoretic MACs:
  - GCM using a 96-bit nonce and a 128-bit authenticator
  - Poly1305
- **Public-key encryption** McEliece with binary Goppa codes:
  - length $n = 6960$, dimension $k = 5413$, $t = 119$ errors

  Evaluating: QC-MDPC, Stehlé-Steinfeld NTRU, ...
- **Public-key signatures** Hash-based (minimal assumptions):
  - XMSS with any of the parameters specified in CFRG draft
  - SPHINCS-256

  Evaluating: HFEv-, ...

Post-quantum secret-key authenticated encryption

- Very easy solutions if secret key k is long uniform random string:
  - "One-time pad" for encryption.
  - "Wegman–Carter MAC" for authentication, e.g., Poly1305.
- AES-256: Standardized method to expand 256-bit k into string indistinguishable from long k.
- AES introduced in 1998 by Daemen and Rijmen. Security analyzed in papers by dozens of cryptanalysts.
- Alternative: ChaCha20 (or Salsa20) well analyzed stream cipher with 256-bit key; in TLS 1.3.
- No credible threat from quantum algorithms. Grover costs 2^{128}.

Policies and alternatives

- Some funding for post-quantum systems in ICT (talk by Nineta Polemi).
- EU investment in quantum computing (talk by Gustav Kalbe). 10^9 EUR for Quantum Flagship but only for quantum technologies.
- Business cases for Quantum Key Distribution (talk by Bart Preneel).

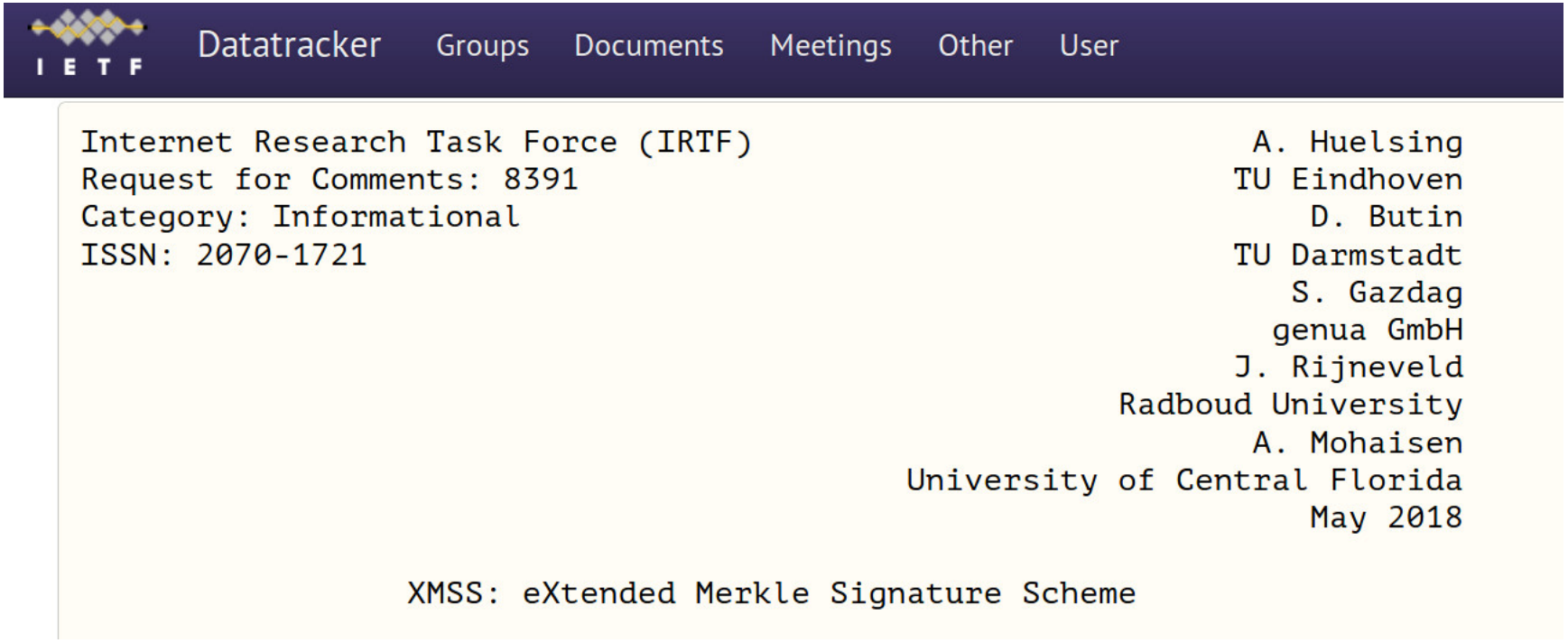
Policies and alternatives

- Some funding for post-quantum systems in ICT (talk by Nineta Polemi).
- EU investment in quantum computing (talk by Gustav Kalbe). 10^9 EUR for Quantum Flagship but only for quantum technologies.
- Business cases for Quantum Key Distribution (talk by Bart Preneel).
  - Commercial QKD implementations encrypt between links, trusted repeaters needed every 200km.
    These repeaters know all secrets.
  - How are these repeaters audited and monitored?
  - QKD implementations use AES for bulk encryption, so continue to rely on algorithmic crypto.
  - QKD needs preshared key for authentication or digital signatures.
    No way to avoid post-quantum cryptography unless we preshare keys

Policies and alternatives

- Some funding for post-quantum systems in ICT (talk by Nineta Polemi).
- EU investment in quantum computing (talk by Gustav Kalbe). 10^9 EUR for Quantum Flagship but only for quantum technologies.
- Business cases for Quantum Key Distribution (talk by Bart Preneel).
  - Commercial QKD implementations encrypt between links, trusted repeaters needed every 200km.
    These repeaters know all secrets.
  - How are these repeaters audited and monitored?
  - QKD implementations use AES for bulk encryption, so continue to rely on algorithmic crypto.
  - QKD needs preshared key for authentication or digital signatures.
    No way to avoid post-quantum cryptography unless we preshare keys (then we might as well use symmetric cryptography).
  - Side-channel attacks need to be avoided *all along the connection*; no way to fully shield devices because they need to interact.

Standardization efforts



IETF Datatracker Groups Documents Meetings Other User

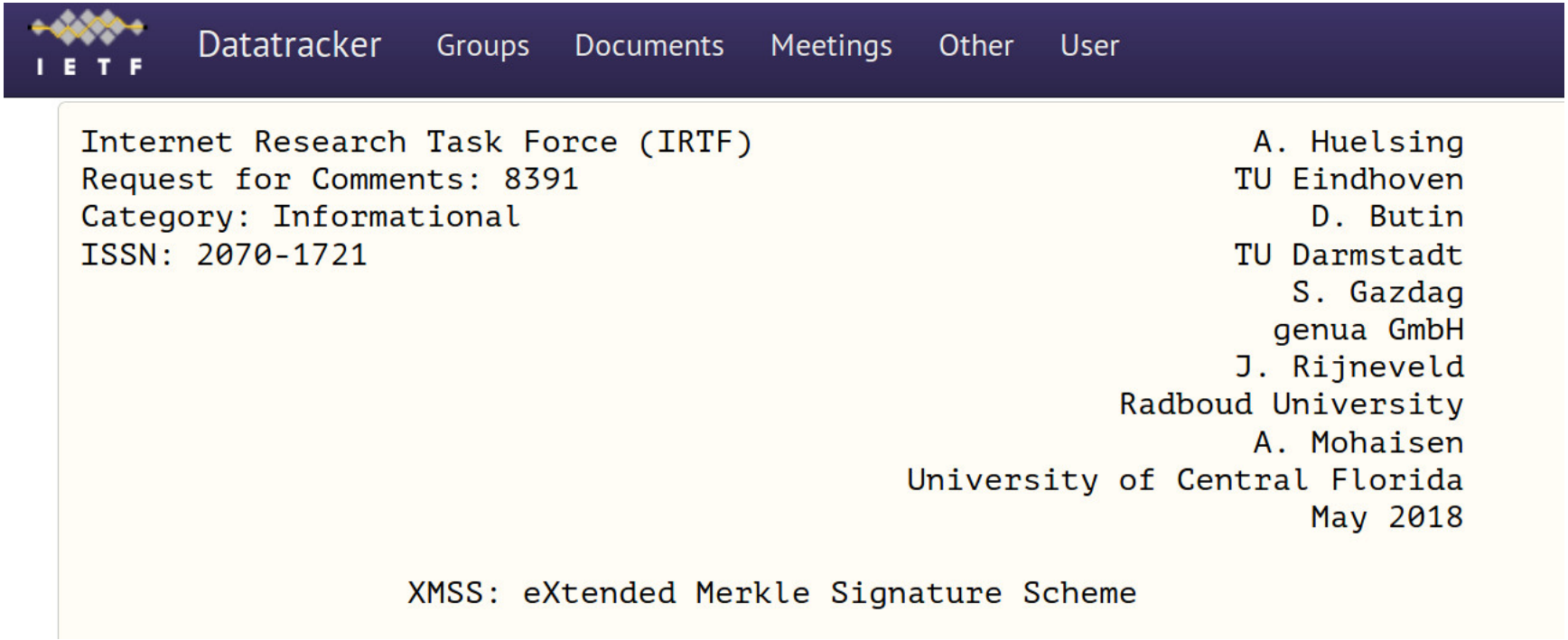
Internet Research Task Force (IRTF)
Request for Comments: 8391
Category: Informational
ISSN: 2070-1721

A. Huelsing
TU Eindhoven
D. Butin
TU Darmstadt
S. Gazdag
genua GmbH
J. Rijneveld
Radboud University
A. Mohaisen
University of Central Florida

May 2018

XMSS: eXtended Merkle Signature Scheme

Standardization efforts



IETF Datatracker Groups Documents Meetings Other User

Internet Research Task Force (IRTF)
Request for Comments: 8391
Category: Informational
ISSN: 2070-1721

A. Huelsing
TU Eindhoven
D. Butin
TU Darmstadt
S. Gazdag
genua GmbH
J. Rijneveld
Radboud University
A. Mohaisen
University of Central Florida

May 2018

XMSS: eXtended Merkle Signature Scheme

- NIST (National Institute for Standards and Technology) asked for submissions to post-quantum project. Ongoing efforts to analyze, implement, select; final results expected in 4-6 years.
- ETSI QSC: several whitepapers.
- ISO: working on whitepaper.
- OASIS: KMIP (key management) standard with PQC.
- ANSI and IEEE have standardized NTRU (not for PQC parameters).

Deployment issues & solutions

- Some of the cryptosystems have interesting other features, see Michael Groves talk on identity-based cryptography.
- Protocol integration and implementation problems (talk by Stefan-Lukas Gazdag)
  - Key sizes or message sizes are larger for post-quantum systems, but IPv6 guarantees only delivery of $\leq$ 1280-byte packets.
  - Google experimented with larger keys and noticed delays and dropped connections.
  - Long-term keys require extra care (reaction attacks).
- Maire O'Neill presented SAFEcrypto results on small devices.
- Daniel J. Bernstein presented libpqcrypto: library based on 22 NIST submissions from PQCRYPTO. Not production quality, but ready for experiments.

Stay tuned for more

- 2019: Executive summer school in Eindhoven.
  Dates TBD.
- https://pqcrypto.org: Survey site by Daniel J. Bernstein & me.
  - Many pointers: e.g., PQCrypto conference series.
  - Bibliography for 4 major PQC systems.
- PQCrypto 2016 with slides and videos from lectures
  (incl. winter school)
- https://www.safecrypto.eu: SAFEcrypto EU project.
- https://pqcrypto.eu.org: PQCRYPTO EU project.
  - Expert recommendations.
  - Free software libraries (libpqcrypto, pqm4, pqhw).
  - Lots of reports, scientific papers, (overview) presentations.
- https://2017.pqcrypto.org/school: PQCRYPTO summer school with 21 lectures on video + slides + exercises.
- https://2017.pqcrypto.org/exec: Executive school (12 lectures), less math, more overview. So far slides, soon videos.
- https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions:
  NIST PQC competition.