# Quantum Leap Cryptography

Ruediger Weis

Physikalische Kolloquium der Universität Bonn, 31. Januar 2020

# A Mathematician's Apology

- Hardy, G. H. (1940)
- A Mathematician's Apology

"The imputation is usually based on an incautious saying attributed to Gauss, to the effect that,

> *if mathematics is the queen of the sciences, then the theory of numbers is, because of its supreme uselessness, the queen of mathematics-*

– I have never been able to find an exact quotation."

# The beginning of Public Key Cryptography

- Ralph Merkle (* 1952)
- http://www.merkle.com/

  *My first paper (and, in fact, the first paper) on public key cryptography was submitted in 1974 and initially rejected by an unknown "cryptography expert" because it was "...not in the main stream of present cryptography thinking...."*

- http://www.merkle.com/1974/PuzzlesAsPublished.pdf

# Math is Your friend

"Trust the math. Encryption is your friend."

- Bruce Schneier, Guardian, 6. September 2013.

# RSA

- Rivest, R.; Shamir, A.; Adleman, L. (February 1978).
  - "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"
- Communications of the ACM. 21 (2): 120–126.

1. Choose two distinct prime numbers $p$ and $q$.
2. $n = p \cdot q$
3. $\varphi(n) = (p-1) \cdot (q-1)$
4. Choose $e$ with $1 < e < \varphi(n)$ and $\gcd(e, \varphi) = 1$
5. $d = e^{-1} \bmod \varphi(n)$ with the Extended Euclidean Algorithm

## Implementation

```
rsaencrypt = lambda x : x ** e % n
rsadecrypt = lambda x : x ** d % n
```

# GNU-Rrivacy Guard: Prime-Number-Generator Subsystem

The primality test works in three steps:

- The standard sieve algorithm using the primes up to 4999 is used as a quick first check.
- A Fermat test filters out almost all non-primes.
- A 5 round Rabin-Miller test is finally used. The first round uses a witness of 2, whereas the next rounds use a random witness.
- `https://www.gnupg.org/documentation/manuals/gcrypt/Prime_002dNumber_002dGenerator-Subsystem-Architecture.html`

# Fermat Test (Wikipedia)

Repeat k times:

- Pick a randomly in the range [2, n - 2]
- If $a^{n-1} \neq 1 \bmod n$
  - then return composite

If composite is never returned: return probably prime

# Rabin Miller Test

- Source based on Wikipedia article

```
#include <stdint.h>
bool mrt (const uint32_t n, const uint32_t a) {
   const uint32_t n1 = n - 1;
   uint32_t d = n1 >> 1;
   int j = 1;
   while ((d & 1) == 0) d >>= 1, ++j;
   uint64_t t = a, p = a;
   while (d >>= 1) {
      p = p*p % n;
      if (d & 1) t = t*p % n;
   }
   if (t == 1 || t == n1) return true;
   for (int k=1 ; k<j ; ++k) {
      t = t*t % n;
      if (t == n1) return true;
      if (t <= 1) break;
   }
   return false;
}
```

# What can possibly go wrong?

## Fast Prime Generation

- Bad idea.

## Old Attack

- Coppersmith (1996)
- Matus Nemec, Marek Sys, Petr Svenda (2017)
  - "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli"

## Costs

- 512 bit: $0,002
- 1024 bit: $1,78
- 2048 bit: $944
- 3072 bit: $1,90 * 10^{26}$
- 4096 bit: $8,48 * 10^{9}$

# Discrete Logarithm Problem

The positive integer $x$ which solves the equation

$$g^x = a$$

is the discrerte logarithm of $a$ to the base $g$.

## Diffie Hellman: New Directions

- Diffie, W.; Hellman, M.E. (November 1976).
  - "New directions in cryptography".
- IEEE Transactions on Information Theory. 22 (6): 644–654.
- Cooperation with Ralph Merkle

## Diffie Hellman Keyexchange

$$(g^a)^b = (g^b)^a$$

# Daniel J. Bernstein: Quantum Computers are coming!

# NIST (2016): How soon do we need to worry?

- When will a quantum computer be built that breaks current crypto?
  - 15 years, $1 billion USD, nuclear power plant (to break RSA-2048)
- (PQCrypto 2014, Matteo Mariantoni)

# The sky is falling?

- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
  - Symmetric key crypto:
    - AES — Need larger keys
    - Triple DES — Need larger keys
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3 — Use longer output

# Longer Keys for DES based encryption

- 2000
- Stefan Lucks, Rüdiger Weis:
  - "How to Make DES-based Smartcards fit for the 21-st Century"
- CARDIS 2000

## Techniques

- Whitening: Frugal DESX
- Feistel Networks: $\mathrm{DEAL}^{\mathrm{KX}}$-128

## Ongoing Research

- Double Encryption with Whitening

# Algorithms for Quantum Computers

- "How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today"

## Shor Algorithm

- 1994
- Peter W. Shor
  - "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"
- In: SIAM Journal on Computing, 26/1997, S. 1484–1509.

## Grover Algorithm

- 1996
- "A fast quantum mechanical algorithm for database search"
- $O(\sqrt{n})$

# Wikipedia: Grover Publications

- `https://en.wikipedia.org/wiki/Lov_Grover`
- Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212
- Grover L.K.: From Schrödinger's equation to quantum search algorithm, American Journal of Physics, 69(7): 769-777, 2001. Pedagogical review of the algorithm and its history.
- Grover L.Ki.: QUANTUM COMPUTING: How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today, The Sciences, July/August 1999, pp. 24–30.
- What's a Quantum Phone Book?, Lov Grover, Lucent Technologies

# Grover in Praktice

## Symmetrical Encryption

- Problem:
  AES-128 $2^{64}$ quantum operations
- Solution:
  AES-256 $2^{128}$ quantum operations

## Hash

- Problem:
  SHA-1, SHA-256 hash length to short
- Solution:
  SHA-512, SHA-3 512 bit hash length

# Shor Algorithm

- Polynomial-time quantum computer algorithm for integer factorization and solving the DLP.
- Quantum Fourier transform
- Quantum gates $O((\log(n))^2 \cdot \log\log(n) \cdot \log\log\log(n))$

# Shor Algoritm Classical Part

1. Pick a random number $a$.
2. Compute $\gcd(a, n)$ with the Euclidean algorithm.
3. If $\gcd(a, n) \neq 1$ then we have found an nontrivial factor of $n$.
4. $r = \text{QuantumPeriodFinding}(a^x \bmod n)$.
5. If $r$ is odd, then go to step 1.
6. If $a^{r/2} \bmod n = -1$, then go to step 1.
7. $\gcd(a^{r/2} + 1, n)$ or $\gcd(a^{r/2} - 1, n)$ is a nontrivial factor of n.

# Quantum period-finding subroutine

- Quantum magic happens here.

# Fatoring 15

## 7 qbits

## Nuclear magnetic resonance quantum computer

- 2001
- Vandersypen, Lieven M. K.; Steffen, Matthias; Breyta, Gregory; Yannoni, Costantino S.; Sherwood, Mark H. & Chuang, Isaac L. (2001),
  - "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance"
- Nature, 414 (6866): 883–887, 2001.

# Josephson phase qubit quantum processor

## Faktoring with a Josephson phase qubit quantum processor

- 2012
- Lucero, Erik; Barends, Rami; Chen, Yu; Kelly, Julian; Mariantoni, Matteo; Megrant, Anthony; O'Malley, Peter; Sank, Daniel; Vainsencher, Amit; Wenner, James; White, Ted; Yin, Yi; Cleland, Andrew N.; Martinis, John M. (2012).
  - "Computing prime factors with a Josephson phase qubit quantum processor".
- Nature Physics. 8 (10): 719.

# Factoring 21

- Markov, Igor L.; Saeedi, Mehdi (2013).
  - "Faster Quantum Number Factoring via Circuit Synthesis".
- Phys. Rev. A. 87 (1): 012310.

# DLP: Hidden Subgroup Problem

- Kernel of $f(a, b) = g^a \cdot (g^r)^{-b}$
- Real World Problem: ECC keylength

# A RIDDLE WRAPPED IN AN ENIGMA

NEAL KOBLITZ AND ALFRED J. MENEZES

- https://eprint.iacr.org/2015/1018.pdf

Theories about the NSA's Motives

> *The NSA believes that RSA-3072 is much more quantum-resistant than ECC-256 and even ECC-384. The quantum complexity of integer factorization or discrete logarithm essentially depends only on the bit length of the group order. Thus, there could be a big lag between the time when quantum computers can solve the ECDLP on P-256 and even P-384 and the time when they can factor a 3072-bit integer. However, it will require major advances in physics and engineering before quantum computing can scale significantly. When that happens, of course P-256 and P-384 will fall first.*

# Hash is still fine

# Lamport 1979

## One Time Signatures

- Leslie Lamport
  - "Constructing digital signatures from a one-way function"
- Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, Okt. 1979.
- Cooperation with Witfield Diffie.

# Merkle Trees

- Ralph Merkle
  - "Secrecy, authentication and public key systems / A certified digital signature"
- Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979

# Hash Trees

## NIST: Stateful Hash-based signatures

- NIST plans to approve stateful hash-based signatures
- 1) XMSS, specified in RFC 8391
- 2) LMS, specified in RFC 8554
- Will include their multi-tree variants, $XMSS^{MT}$ and HSS

## Rethinking PKI

- Do not mention the blockchain;-)

## Stateless hash-based Signature Sphincs

- `https://sphincs.org/`

# Research

- Understanding old an new math
- Real World Algorithms
  - Trees for statlefull hash based signatures
  - Reducing public key size
  - Reducing signature size
  - ...
- NIST Candidates Round 2 (2019)
  - Lattice-based (12)
  - Code-based (7)
  - Symmetric-bases (2)
  - Other (1)
- Beyond Error correction
- ...

# Side Effects of Theoretical Physics

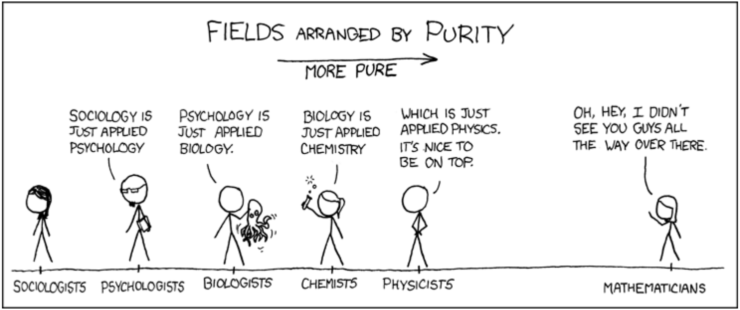
## CERN

- WWW
- Cloud Computing
- . . .

## Quantum Computers

- New math
- New computer hardware
- New computer software

# Thank you!




https://xkcd.com/435/