genua.

Der lange Weg zur quantenresis-tenten Kryptografie

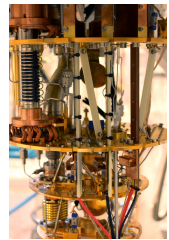
Stefan-Lukas_Gazdag@genua.de

02. Juni 2022

genua.

Die wunderbare Welt der Quanten

- **Quantum Computing**
  - Quantum Computers
  - Quantum Supremacy
  - Quantum Advantage
- **Quantum Cryptography**
  - Quantum Key Distribution (QKD)
- **Post-Quantum Cryptography (PQC)**
  - aka Quantum-Safe Cryptography (QSC)
  - aka Quantum-Resistant Cryptography (QRC)



genua.

Das Quantum-Trauma

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.

https://arxiv.org/abs/quant-ph/9508027

genua.

Der Quantum-Schock

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.

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired item.

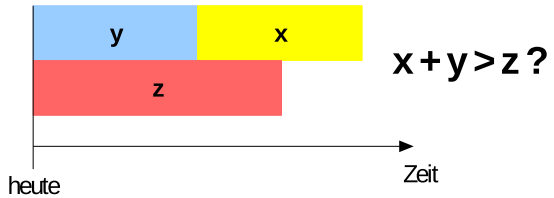
https://arxiv.org/abs/quant-ph/9605043

genua.

Tempus fugit

Wann muss man sich sorgen machen?
(nach Michele Mosca, University of Waterloo)

- Wie lange muss die Kryptographie standhalten? (*x* Jahre)
- Wie lange benötigen wir, um post-quantum sicher zu werden? (*y* J.)
- Wie lange wird es dauern, einen großen Quantencomputer oder bessere Angriffe zu entwickeln? (*z* Jahre)



genua.

Die Migration zur Post-Quanten-Kryptografie

Wie es begann:

Wie es läuft:

Quelle: Sisyphus by Titian, Wikimedia, User Escarlati, Public Domain

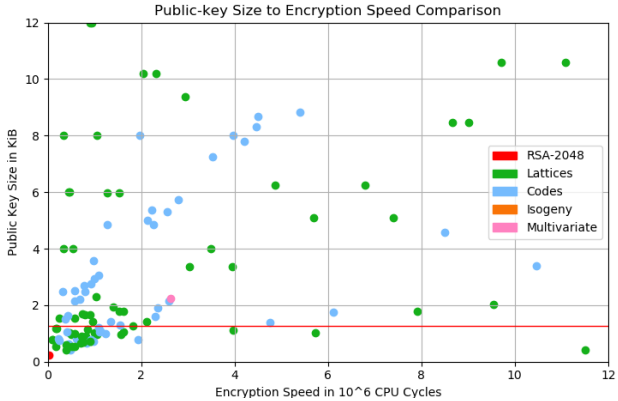
genua.

Post-Quantum Cryptography

Die Suche nach quantenresistenten Verfahren:

- Gitter-basierte Kryptographie
- Multivariate Kryptographie
- Code-basierte Kryptographie
- Isogenien in supersingularen elliptischen Kurven
- Hash-basierte Signaturen
- ...

Alles wird immer schneller und kleiner - nicht



by Tobias Heider, `https://github.com/tobhe/pq-plot`

genua.

squareUP

- *Quantencomputer-resistente Signaturverfahren für die Praxis*
- Mai 2014 - Juni 2017
- Förderung:
  - *IuK-Bayern* des bayerischen StMWi für genua
  - *Erkenntnistransfer* der DFG für die TU Darmstadt
  - Bundesamt für Sicherheit in der Informationstechnik (assoziiert)
- `https://square-up.org`

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

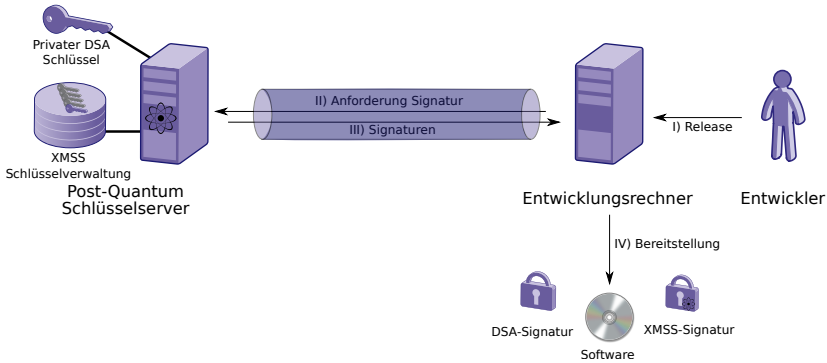
May 2018

XMSS: eXtended Merkle Signature Scheme

Abstract

This note describes the eXtended Merkle Signature Scheme (XMSS), a hash-based digital signature system that is based on existing descriptions in scientific literature. This note specifies Winternitz One-Time Signature Plus (WOTS+), a one-time signature scheme; XMSS, a single-tree scheme; and XMSS^MT, a multi-tree variant of XMSS. Both XMSS and XMSS^MT use WOTS+ as a main building block. XMSS provides cryptographic digital signatures without relying on the conjectured hardness of mathematical problems. Instead, it is proven that it only relies on the properties of cryptographic hash functions. XMSS provides strong security guarantees and is even secure when the collision resistance of the underlying hash function is broken. It is suitable for compact implementations, is relatively simple to implement, and naturally resists side-channel attacks. Unlike most other signature systems, hash-based signatures can so far withstand known attacks using quantum computers.

squareUP


Privater DSA Schlüssel
XMSS Schlüsselverwaltung
Post-Quantum Schlüsselserver
II) Anforderung Signatur
III) Signaturen
I) Release
Entwicklungsrechner
Entwickler
IV) Bereitstellung
DSA-Signatur
Software
XMSS-Signatur

genua.

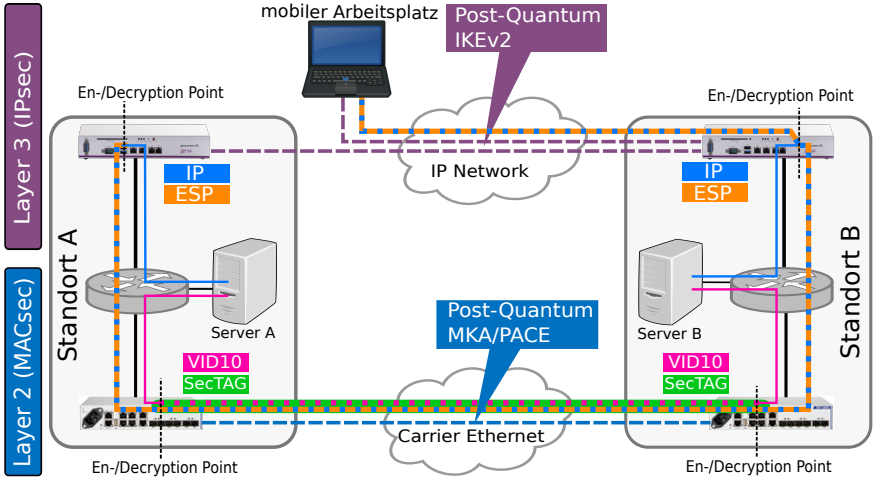
QuaSiModO

- *Quanten-Sichere VPN-Module und -Operationsmodi*
- September 2019 - August 2022
- Förderung durch das BMBF
- Partner:
  - ADVA Optical Networking SE
  - Fraunhofer AISEC
  - genua GmbH
  - Ludwig-Maximilians-Universität München

  Assoziierter Partner:
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Hessen 3C
- `https://pq-vpn.de/`

genua.

QuaSiModO



genua.

Einige Aspekte

- PQ-Schlüsselaustausch mit IKEv2
- experimentell: Verwendung großer Schlüssel
- Abstimmung mit Regulatoren (BSI, NIST)
- Beteiligung an Standardisierungsverfahren
- Formale Verifikation
- Alternative Schemata für Key Agreement
- Authentifizierung per PQ-Zertifikat

genua.

Fragen?

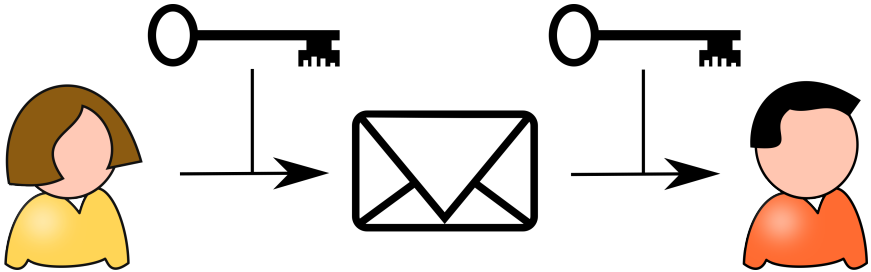
Stefan-Lukas_Gazdag@genua.de

www.square-up.org

www.pq-vpn.de

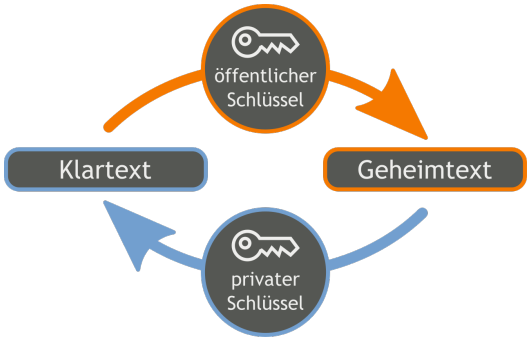
www.genua.de

Kryptographie: symmetrisch



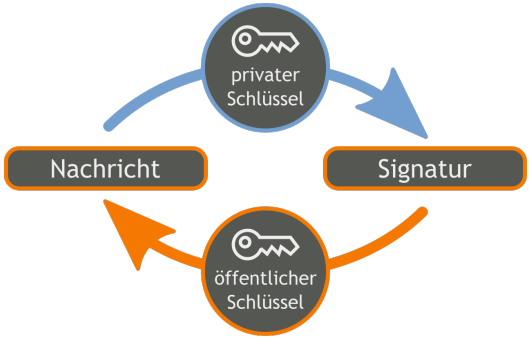
openclipart.org: dimitri, milovanderlinden, SavanaPrice

Kryptographie: asymmetrisch



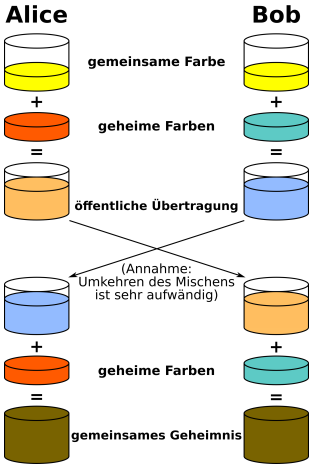
by Bananenfalter, CC0 1.0

Kryptographie: asymmetrisch



by Bananenfalter, CC0 1.0

Schlüsselaustausch / -vereinbarung



by A. J. Han Vinck, Public Domain

Sicherheit der Verfahren?

Kurzfassung:
Alle sind sich einig, dass alle nicht wissen, wie man ein Verfahren bricht.

genua.

Sicherheit der Verfahren?

Kurzfassung:
Alle sind sich einig, dass alle nicht wissen, wie man ein Verfahren bricht.

Langfassung:

- Bester bekannter Angriff
- Math. Beweise / Modelle
- spezifisch vs. generisch
- Theorie vs. Praxis (Implementierung, z. B. schlechter Zufall)

genua.

Sicherheit der Verfahren?

Kurzfassung:
Alle sind sich einig, dass alle nicht wissen, wie man ein Verfahren bricht.

Langfassung:

- Bester bekannter Angriff
- Math. Beweise / Modelle
- spezifisch vs. generisch
- Theorie vs. Praxis (Implementierung, z. B. schlechter Zufall)

Aber: Manch ein Mensch weiß nicht, dass das schwer ist und löst es.

genua.

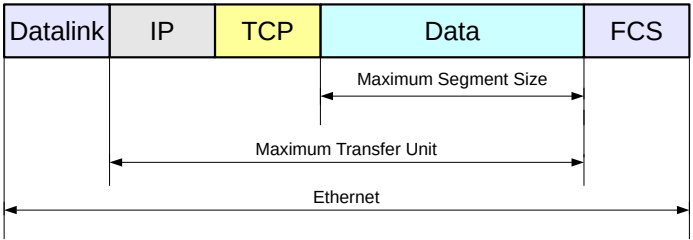
Maximum Transmission Unit

Maximale Datenmenge (Frame), die von Maschine zu Maschine zum Empfänger geschickt werden kann.

Beispiel: auf dem Weg steht alte Maschine mit begrenztem Speicher und es gibt keine alternative Route.

- IPv4: 68 Bytes (Minimale MTU)
- IPv6: 1280 Bytes (Minimale MTU)
- Classic McEliece Public Key: 1 MB
- Durchschnittliche Website: > 2 MB

Fragmentierung



genua.

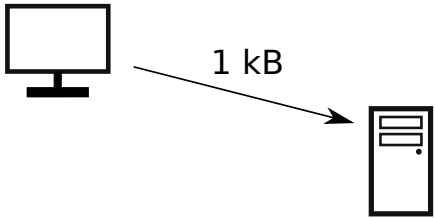
Fragmentierung

Wichtiges Feature, um große Daten in kleine Pakete zu zerlegen

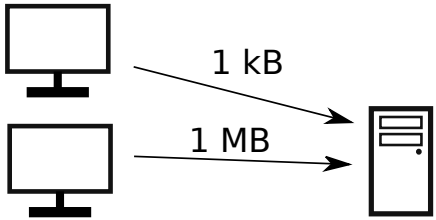
- IP-Fragmentierung wird in der Praxis vermieden
- Maschinen (Middleware / Firewalls) leiten Pakete nicht weiter

  ⇒ Fragmentierung auf höheren Schichten behandelt
- (Initiale) Pakete müssen / sollen in MTU passen

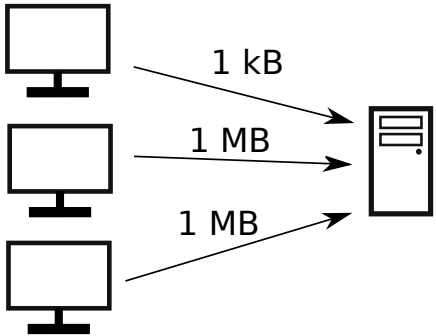
Denial of Service



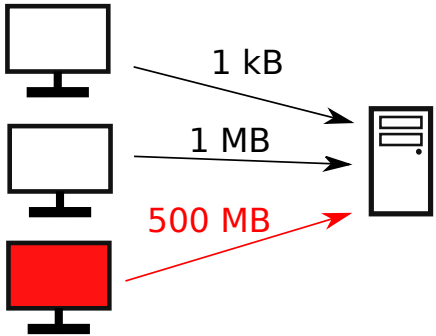
Denial of Service



Denial of Service



Denial of Service



genua.

Fragen?

Stefan-Lukas_Gazdag@genua.de

www.square-up.org

www.pq-vpn.de

www.genua.de