genua Ein Unternehmen der Bundesdruckerei

Post-Quanten-Kryptographie

Bedrohung, aktueller Stand, Lösungen

Alexander von Gernler, Stefan-Lukas Gazdag

UniBW CODE 2018, 11. Juli 2018 | v1

genua Ein Unternehmen der Bundesdruckerei

Inhalt

Vorstellung

Post-Quanten-Kryptographie

Fazit

genua Ein Unternehmen der Bundesdruckerei

Inhalt

genua Ein Unternehmen der Bundesdruckerei

Was ist genua?

- Spezialist für IT-Sicherheit
  - gegründet 1992, Kirchheim bei München
  - 230 Mitarbeiter (April 2018)
  - Unternehmen der Bundesdruckerei-Gruppe
- Hochsicherheits-Firewalls
  - ein- oder zweistufig
  - OpenBSD-basiert
  - BSI-zertifiziert: Common Criteria, EAL4+
- Stehen bei...
  - Konzernen (MAN, RTL II, Hypo-Vereinsbank, Klüber, …)
  - Behörden, Verwaltungen, BOS (Bundestag, BSI, Generalbundesanwalt, Stadt München, Bundeswehr, …)

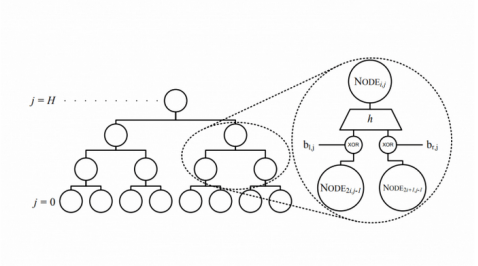
genua Ein Unternehmen der Bundesdruckerei

Inhalt

genua Ein Unternehmen der Bundesdruckerei

Digitale Signaturen: Erster Standard für Post-Quantum-Signaturen

20.06.2018 07:00 Uhr – Jürgen Schmidt



(Bild: Buchmann, Dahmen, Hulsing)

Das neue Signaturverfahren namens XMSS soll auch der Rechenpower von Quantencomputern standhalten.

Forscher der Technischen Universität Darmstadt und des deutschen Sicherheitsunternehmens Genua haben ein Verfahren zur Erstellung digitaler Signaturen entwickelt, das auch den Angriffen mit Quanten-Computern standhalten soll. Das eXtended Merkle Signature

genua Ein Unternehmen der Bundesdruckerei

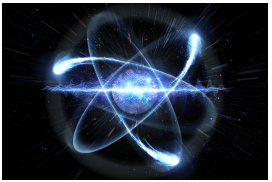
Konventionelle Kryptographie -- was ist das?

- Mathematisch harte Probleme
- Angreifer muss langwierige Berechnungen durchführen
- Besitzer des Schlüssels brauchen nur vertretbaren Aufwand
- Bekannteste Probleme:
  - Faktorisierung großer Zahlen (RSA)
  - diskreter Logarithmus in endlichen Gruppen (Diffie-Hellman)

genua Ein Unternehmen der Bundesdruckerei

Quantencomputer

- Nutzen physikalische Effekte aus
- Quantenzustände, vgl. *Schrödingers Katze*
- Wahrscheinlichkeitswolken
- Ergebnis durch Beobachtung
- Dadurch substanzielle Beschleunigungen möglich: Alle Zustände auf einmal
- Anwendung zum Brechen konventioneller Krypto:
  - Shor's Algorithmus (Faktorisierung)
  - Grover's Algorithmus (Suche in unsortierten Daten)



genua Ein Unternehmen der Bundesdruckerei

Angriffsvektoren durch Quantencomputer

Was geht kaputt, wenn Quantencomputer existieren?

1. Angriff auf Signaturen
   - Fälschen von Dokumenten
   - Fälschen von E-Mails
   - Fälschen von Software-Updates
2. Angriff auf Schlüsselaustausch
   - Vertraulichkeit verschlüsselter Kommunikation (VPN)
3. Angriff auf Verschlüsselung
   - Bedrohung für verschlüsselte Langzeit-Archivierung
   - Vertraulichkeit verschlüsselter Kommunikation (VPN)

genua Ein Unternehmen der Bundesdruckerei

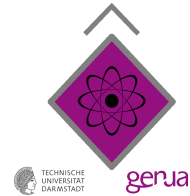
Gegengift: Post-Quanten-Kryptographie

- Neue Krypto-Algorithmen werden benötigt
- Verwundbare Primitive vermeiden: Faktorisierungsproblem, diskreter Logarithmus in endlichen Gruppen
- Aktuelles Forschungsthema: Post-Quanten-Kryptographie (PQC)
  - Erfahrung mit RSA und anderer konventioneller Krypto über 20 Jahre
  - Sehr intensive öffentliche Aufmerksamkeit
  - PQC-Forschung dagegen noch jung

genua Ein Unternehmen der Bundesdruckerei

✓ Gegenmaßnahmen: 1. Sichere Signaturen

- ✓ Erfolgreiches Forschungsprojekt squareUP
  - Mit Prof. Dr. Johannes Buchmann, TU Darmstadt
- ✓ Software-Updates genua ab jetzt zusätzlich mit PQC-Signatur
  - Verfahren: XMSS-MT (hash-basierte PQC-Signaturen)
- ✓ Kein proprietäres Eigenwerk, sondern jetzt RFC 8391
- ✓ Referenzimplementation als OpenSource freigegeben
  - Weitere Anwendungen denkbar und in Prüfung



Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie

genua Ein Unternehmen der Bundesdruckerei

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

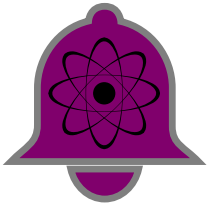
This note describes the eXtended Merkle Signature Scheme (XMSS), a hash-based digital signature system that is based on existing descriptions in scientific literature. This note specifies Winternitz One-Time Signature Plus (WOTS+), a one-time signature scheme; XMSS, a single-tree scheme; and XMSS^MT, 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.

genua Ein Unternehmen der Bundesdruckerei

Gegenmaßnahmen: 2. und 3. Sicheres VPN

QuasIModO: Quantensichere IPsec Module und Operationsmodi

- Laufende Forschung bei genua
  - Auch hier offener Standard angestrebt
  - Ziele
    1. KnowHow zu PQ-Crypto aufbauen
    2. Quantensicherheit unserer VPNs sicherstellen
    3. Standardisierung / Referenzimplementation herausgeben
    4. Ergebnisse auf andere Produktfeatures übertragen
    5. Bei BSI, Behördenkunden, BOS einsetzen



genua Ein Unternehmen der Bundesdruckerei

Inhalt

genua Ein Unternehmen der Bundesdruckerei

Zusammenfassung

1. Konventionelle Krypto sicher gegen konventionelle Rechner
2. Quantencomputer ist Game Changer
3. Sicherheit gegen Quantencomputer: Post-Quanten-Krypto
4. Neues Feld, Forschung noch im Gange
5. Einige Erkenntnisse bereits sicher, z. B. Hash-basierte Signaturen

genua Ein Unternehmen der Bundesdruckerei

Fragen?

<forschung@genua.de>

Danksagung an unseren Kollegen Kryptologen für wertvolle Beiträge zu diesem Vortrag:

- Dr. Daniel Loebenberger