Freie Universität Berlin

Kryptoagilität

Marian Margraf

Freie Universität Berlin

TeleTrusT Konferenz 2021

Agenda

Motivation

Quantencomputer

Kryptoagilität, Definition

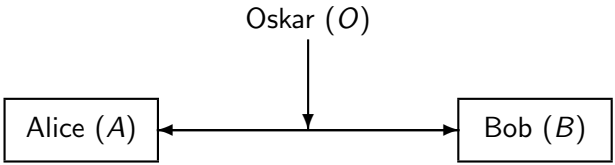
Kryptoagilität, Leitlinien

Handlungsempfehlungen hinsichtlich QC

- Fortschritte in der Kryptoanalyse führen zur Anpassungen am Kryptokonzept
  - Evolutionär: Anpassung der Schlüssellängen
  - Disruptiv: Nutzung neuer Kryptoalgorithmen
- Ein Beispiel: Quantencomputer

QC: Auswirkungen auf heute eingesetzte Kryptoverfahren

- Grover-Algorithmus, 1996: Relevant für symmetrische Verfahren wie AES
- Shor-Algorithmus, 1997: Relevant für asymmetrische Verfahren wie RSA, DH



- Authentischer Schlüsselaustausch mit asymmetrischen Verfahren (RSA, DH, ...)
- Sichere Kommunikation mit symmetrischen Verfahren (AES, H-MAC, ...)

- Suche in unsortierter Datenbank mit N Einträgen in $\approx \sqrt{N}$ Schritten
- Anwendung: Suche Schlüssel der Länge n (also 2^n verschiedene Schlüssel)
- Mit Grover in $\approx \sqrt{2^n} = 2^{n/2}$ Schritten
- Gegenmaßnahme: Verdoppelung der Schlüssellänge (128 auf 256 Bit)
- AES-256 einsetzen!

- Faktorisierung von $n = p \cdot q$ in $\approx (\log n)^2 (\log \log n)(\log \log \log n)$ Schritten
- Gegenmaßnahme: Einsatz neuer Kryptoalgorithmen

- Klassische Computer (Number Field Sieve): $\approx 2^{2(\log n)^{1/3}(\log\log n)^{2/3}}$
- Quantencomputer (Shors Algorithmus): $\approx (\log n)^2(\log\log n)(\log\log\log n)$
- Für $n = 2^{4096}$ ($\log n = 4096 = 2^{12}$, $\log\log n = 12 \approx 2^{3,6}$)

$$\text{klassisch: } \approx 2^{2(4.096)^{1/3}(12)^{2/3}} \approx 2^{2\cdot 16\cdot 5} \approx 2^{160}$$

$$\text{QC: } \approx (2^{12})^2 \cdot 2^{3,6} \cdot 2^2 = 2^{2\cdot 12+3,6+2} \approx 2^{30}$$

Computer berechnet $2.000.000.000 \approx 2^{31}$ Operationen pro Sekunde

- Klassisch: $2^{160}/2^{31} = 2^{129}$ Sekunden $= 2^{104}$ Jahre
- QC: $2^{30}/2^{31} = 1/2$ Sekunden
- Alter Universum: $13,8$ Mrd Jahre $\approx 2^{34}$

Naheliegende Idee: Erhöhung der Schlüssellänge, aber

- Schlüssel, Ver- und Entschlüsselung müssen effizient berechenbar sein
- Insb. muss aus e der geheime Schlüssel d berechnet werden können
- Laufzeit (Erweiterter Euklidischer Algorithmus): $\approx (\log n)^2$
- Laufzeit Shor-Algorithmus: $\approx (\log n)^2 (\log \log n)(\log \log \log n)$

$$(\log n)^2 \quad \text{versus} \quad (\log n)^2(\log\log n)(\log\log\log n)$$

- Faktorisieren $(\log\log n)(\log\log\log n)$-mal langsamer als Schlüsselberechnung
  - $(\log\log n)(\log\log\log n)$ ist sehr kleine Zahl (selbst für große n)
  - Beispiel: $n = 2^{4096}$: $\log n = 4096 = 2^{12}, \log\log n = 12, \log\log\log n = 3,6$

Voraussichtlich ab 2030:

- QC brechen Verfahren, die auf Faktorisierung setzen, vollständig
- Gleiches gilt für Diskreten Logarithmus (DH, DSA, ECDSA)
- Symmetrische Verfahren sind nicht so stark betroffen

Für langlebige Sicherheit besteht akuter Handlungsbedarf

- Snowden Leaks (2013): NSA forscht an QC
- Store now, decrypt later

Bei Neu- und Weiterentwicklung

- Flexible Gestaltung der eingesetzten kryptographischen Verfahren
- Ziel: Es muss einfach möglich sein
  - Schlüssellängen und sonstige Parameter zu vergrößern
  - kryptographischen Verfahren, die nicht mehr sicher sind, auszutauschen

- Implementierung mehrerer Kryptoalgorithmen
- Implementierung mehrerer Schlüssellängen
- Variable Größe der Kommunikationsschnittstellen

  (Nachrichten sind bei verschiedenen Algorithmen unterschiedlich)
- Protokolle müssen Name des Kryptoalgorithmus enthalten

- Erarbeitung eines Mikrationskonzepts
- Etablierung eines Incident Management Systems

Umsetzung von Kryptoagilität erfordert häufig Neuentwicklung

- Dann könnte gleich PQC eingesetzt (und auf Agilität verzichtet) werden
- Aber:
  - PQC-Verfahren sind noch nicht standardisiert
  - Kryptoagilität ist nicht nur für Bedrohungen durch Quantencompter relevant
  - Kryptoanalyse kann sich für alle eingesetzten Verfahren sprunghaft verbessern

- Signaturverfahren: LMS, XMSS (z.B. für Software-Updates)
  - Standardisiert und resistent gegen QC
  - Nachteil: zustandsbehaftet
- Schlüsseleinigung: Hybride Verfahren
  - Kombination von klassischen mit quantencomputerresistenten Verfahren
  - BSI Empfehlung für PQC-Anteil: Classic McEliece, FrodoKEM