



Quantenkryptoanalyse

Marian Margraf

Fraunhofer AISEC, Freie Universität Berlin

Omnisecure 2023

Stand der Wissenschaft

Herausforderungen

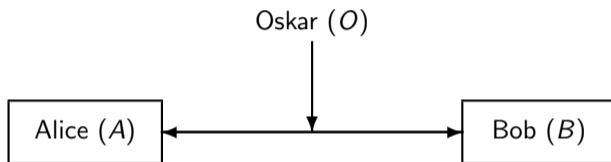
Sicherheit von Post-quantum Crypto

Anzahl benötigter Qubits

Quantenkryptoanalyse

QC: Auswirkungen auf heute eingesetzte Kryptoverfahren

- ▶ Grover-Algorithmus, 1996: Relevant für symmetrische Verfahren wie AES
- ▶ Shor-Algorithmus, 1994: Bricht asymmetrische Verfahren wie RSA, DH, DSA, ElGamal
- ▶ Simon-Algorithmus, 1994: Relevant für symmetrische Verfahren (Even-Mansour-Konstruktion)
- ▶ ?HHL-Algorithmus, 2008: „Löst“ bestimmte exponentiell große lineare GS in Polynomzeit



- ▶ 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

Laufzeit klassisch vs. QC (Shor)

- ▶ 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 $n = 2^{4096}$ ($\log n = 4096 = 2^{12}$, $\log \log n = 12 \approx 2^{3,6}$)

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

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

Laufzeit klassisch vs. QC (Shor)

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 $\approx 2^{34}$ Jahre

Laufzeit klassisch vs. QC (Shor)

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: $\approx (\log n)^2(\log \log n)(\log \log \log n)$

Arbeitshypothese BSI (für Risikoanalyse): Für Kryptoanalyse relevante QC existieren ab ca. 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

- ▶ Sind die neuen Kryptoverfahren wirklich sicher?
- ▶ Lassen sich die bekannten Quantenalgorithmien verbessern (Anzahl benötigter qbits)?
- ▶ Gibt es weitere Quantenalgorithmien für die Kryptoanalyse?
- ▶ Migration hin zu Post-quantum Kryptographie
- ▶ Neues Paradigma: Kryptoagilität

NIST Competition Post-quantum Crypto

- ▶ 2016: Call of Proposals
- ▶ 2022: Gewinner nach drei Runden
 - ▶ KEM: Kyber (gitterbasiert)
 - ▶ Signaturen: Dilithium, FALCON (beide gitterbasiert), SPHINCS+ (hashbasiert)
- ▶ 2022: Start vierte Runde
 - ▶ KEM: BIKE, McEliece, HQC (alle code-basiert), SIKE (EC isogeniebasiert)

Sicherheit von Post-quantum Crypto

Allein 2022 zwei PQC-Verfahren gebrochen

- ▶ Rainbow (multivariate Polynomssystem), Kandidat bis Ende Runde 3 (Beullens¹)
- ▶ SIKE (isogeniebasiert): Kandidat Runde 4 (Castryck, Decru²)

Notwendige Maßnahmen:

- ▶ Hybride Verfahren (z.B. RSA/Kyber)
- ▶ Kryptoagilität

¹Breaking Rainbow Takes a Weekend on a Laptop

²An Efficient Key Recovery Attack on SIDH

Beispiel RSA, wir wollen Modul $N = p \cdot q \approx 2^n$ faktorisieren

- ▶ 1994, Shor : $3n$ Qubits
- ▶ 2000, Seifert³: $\approx 2n$ Qubits
- ▶ 2017, Ekerå, Håstad⁴: $(3/2 + o(1))n$
- ▶ 2019, Gidney, Ekerå⁵: Faktorisieren mit physikalischen an Stelle von logischen Qubits
- ▶ 2021 May, Schlieper⁶: $(1/2 + o(1))n$
- ▶ 2022, Yan et al. Dezember⁷: $n/\log n$???

³Using fewer Qubits in Shor's Factorization Algorithm via Simultaneous Diophantine Approximation

⁴Quantum algorithms for computing short discrete logarithms and factoring RSA integers

⁵How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

⁶Quantum Period Finding is Compression Robust

⁷Factoring integers with sublinear resources on a superconducting quantum processor

Quantenkryptoanalyse

- ▶ Shor (Faktorisierung, Logarithmus)
- ▶ Grover (Schlüsselsuche)
- ▶ Simon (bestimmte Hashfunktionen)
- ▶ HHL (algebraische Attacken)?

Was kommt da noch?

Klassische Kryptoanalyse



Algebraische Kryptoanalyse

Sei $E : \{0, 1\}^n \times \{0, 1\}^t \rightarrow \{0, 1\}^n, (m, k) \mapsto c$ Verschlüsselungsfunktion
 Known Plaintext Attack:
 Wir kennen $m = (m_1, \dots, m_{128})$ und $c = (c_1, \dots, c_{128})$ mit $c = E(m, k)$

Multivariates Polynomsystem
 in der Unbekannten $k = (k_1, \dots, k_{128})$

$$\begin{aligned}
 m_1 m_5 m_{13} c_4 c_{120} k_7 k_{50} \oplus \dots \oplus m_{38} c_{97} c_{100} c_{112} k_7 k_{23} k_{47} k_{101} &= 0 \\
 m_{17} m_{66} c_{13} c_{76} c_{120} k_{15} k_{55} \oplus \dots \oplus m_8 c_{43} c_{100} c_{87} k_{13} k_{67} k_{90} k_{101} &= 0 \\
 m_5 m_{48} m_{53} c_9 c_{16} k_7 k_{50} \oplus \dots \oplus m_{87} c_{97} k_7 k_{23} k_{35} k_{42} k_{47} k_{101} &= 0 \\
 &\vdots \\
 m_{45} m_{72} m_{99} c_{67} c_{120} k_{30} k_{53} \oplus \dots \oplus m_{23} c_{58} c_{127} c_{128} k_{13} k_{67} k_{90} k_{101} &= 0
 \end{aligned}$$

Linearisierung: Lineares GS in den
 Unbekannten $(x_1, x_2, \dots, x_N), N \leq 2^{128}$

$$\begin{aligned}
 m_1 m_5 m_{13} c_4 c_{120} x_1 \oplus \dots \oplus m_{38} c_{97} c_{100} c_{112} x_t &= 0 \\
 m_{17} m_{66} c_{13} c_{76} c_{120} x_s \oplus \dots \oplus m_8 c_{43} c_{100} c_{87} x_u &= 0 \\
 m_5 m_{48} m_{53} c_9 c_{16} x_1 \oplus \dots \oplus m_{87} c_{97} x_v &= 0 \\
 &\vdots \\
 m_{45} m_{72} m_{99} c_{67} c_{120} x_w \oplus \dots \oplus m_{23} c_{58} c_{127} c_{128} x_u &= 0
 \end{aligned}$$

Das linearisierte Gleichungssystem ist exponentiell groß

- ▶ Entwickelt 2008 von Harrow, Hassidim, Lloyd⁸
- ▶ Berechnet Quantenzustand des Lösungsvektors eines linearen GS in Zeit $\mathcal{O}(\log(N)\kappa^2)$
 N Anzahl der Variablen, κ Konditionszahl, GS muss dünn besetzt sein
- ▶ Frage: Lässt sich HHL für algebraische Kryptoanalyse einsetzen?
 - ▶ Gao et al.⁹: Laufzeit für AES-128 $\mathcal{O}(2^{73}\kappa^2)$
- ▶ Wie groß ist κ : Konditionszahl ist ein Maß der Störanfälligkeit des linearen GS
 - ▶ Bei Kryptoverfahren sollte die Störanfälligkeit sehr groß sein
 - ▶ Avalanche-Kriterium: Änderung eines Eingabebits ändert 50% der Ausgabebits
 - ▶ Wir schätzen bei AES-128: $\kappa > 2^{50}$

⁸Quantum algorithm for solving linear systems of equations

⁹Quantum Security of AES-128 under HHL Algorithmen

Sei $E : \{0, 1\}^n \times \{0, 1\}^t \rightarrow \{0, 1\}^n, (m, k) \mapsto c$ Verschlüsselungsfunktion

- ▶ Finde $\alpha, \beta, \gamma \in \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^t$ mit

$$\Pr_{m,k}[\alpha \bullet m \oplus \beta \bullet E(m, k) = \gamma \bullet k] \geq 1/2 + \varepsilon \quad (x \bullet y = \sum_{i=1}^n x_i y_i \bmod 2)$$

- ▶ Known Plaintext Attack: N bekannte Paare $(m^i, c^i = E(m^i, k)), i \leq N$
 - ▶ Berechne $\alpha \bullet m^i \oplus \beta \bullet c^i \in \{0, 1\}$ für alle $i \leq N$, sei s Anzahl der Einsen
 - ▶ Setze $\gamma \bullet k = 1$, wenn $s > N/2$, sonst 0 (Majoritätsentscheidung)
 - ▶ Damit erhalten wir 1 Bit Information über k

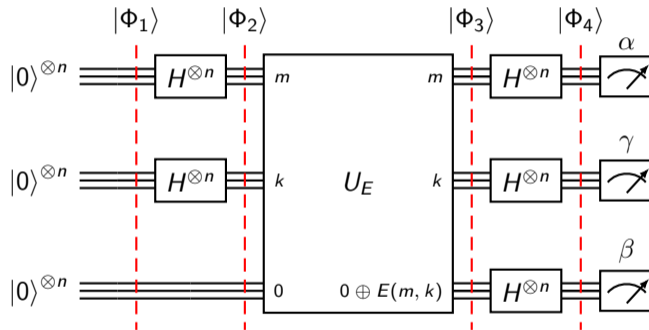
Offensichtlich: Je größer ε , desto weniger Plain-/Ciphertextpaare werden benötigt

Sei $E : \{0, 1\}^n \times \{0, 1\}^t \rightarrow \{0, 1\}^n, (m, k) \mapsto c$ Verschlüsselungsfunktion

- ▶ Finde $\alpha, \beta, \gamma \in \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^t$ mit

$$\Pr_{m,k}[\alpha \bullet m \oplus \beta \bullet E(m, k) = \gamma \bullet k] \geq 1/2 + \varepsilon \quad (x \bullet y = \sum_{i=1}^n x_i y_i \bmod 2)$$

- ▶ Betrachte $\chi_E(\alpha, \beta, \gamma) := \sum_{m,k} (-1)^{\alpha \bullet m \oplus \beta \bullet E(m,k) \oplus \gamma \bullet k}$
- ▶ Es gilt $-2^{n+t} \leq \chi_E(\alpha, \beta, \gamma) \leq 2^{n+t}$
- ▶ Wie finden wir (α, β, γ) so, dass $|\chi_E(\alpha, \beta, \gamma)|$ groß ist? Es gibt $2^n 2^n 2^t$ Kandidaten.



$$\begin{aligned}
 & |0\rangle |0\rangle |0\rangle \xrightarrow{H^{\otimes n} \otimes H^{\otimes t} \otimes \text{Id}} \frac{1}{\sqrt{2^n}} \sum_{m=0}^{2^n-1} |m\rangle \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |0\rangle = \frac{1}{\sqrt{2^n}} \frac{1}{\sqrt{2^t}} \sum_{m=0}^{2^n-1} \sum_{k=0}^{2^t-1} |m\rangle |k\rangle |0\rangle \\
 & \xrightarrow{U_E} \frac{1}{\sqrt{2^{n+t}}} \sum_{m=0}^{2^n-1} \sum_{k=0}^{2^t-1} |m\rangle |k\rangle |0 \oplus \underbrace{E(m,k)}_c\rangle = \frac{1}{\sqrt{2^{n+t}}} \sum_{m=0}^{2^n-1} \sum_{k=0}^{2^t-1} |m\rangle |k\rangle |c\rangle \\
 & \xrightarrow{H^{\otimes n} \otimes H^{\otimes t} \otimes H^{\otimes n}} \frac{1}{\sqrt{2^{n+t}}} \sum_{m=0}^{2^n-1} \sum_{k=0}^{2^t-1} \left(\frac{1}{\sqrt{2^n}} \sum_{\alpha=0}^{2^n-1} (-1)^{m \bullet \alpha} |\alpha\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_{\gamma=0}^{2^t-1} (-1)^{k \bullet \gamma} |\gamma\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_{\beta=0}^{2^n-1} (-1)^{E(m,k) \bullet \beta} |\beta\rangle \right) \\
 & = \frac{1}{\sqrt{2^{n+t}}} \frac{1}{\sqrt{2^{3n}}} \sum_{m=0}^{2^n-1} \sum_{k=0}^{2^t-1} \sum_{\alpha=0}^{2^n-1} \sum_{\gamma=0}^{2^t-1} \sum_{\beta=0}^{2^n-1} (-1)^{m \bullet \alpha} |\alpha\rangle (-1)^{k \bullet \gamma} |\gamma\rangle (-1)^{E(m,k) \bullet \beta} |\beta\rangle \\
 & = \frac{1}{\sqrt{2^{n+t}}} \frac{1}{\sqrt{2^{3n}}} \sum_{\alpha, \beta, \gamma} \sum_{m, k} (-1)^{\alpha \bullet m \oplus \beta \bullet E(m,k) \oplus \gamma \bullet k} |\alpha \beta \gamma\rangle
 \end{aligned}$$

Zusammenfassung:

- ▶ Wir suchen α, β, γ mit $|\chi_E(\alpha, \beta, \gamma)| = \left| \sum_{m,k} (-1)^{\alpha \bullet m \oplus \beta \bullet E(m,k) \oplus \gamma \bullet k} \right|$ groß
- ▶ Berechne effizient Quantenzustand $\frac{1}{\sqrt{2^{n+t}}} \frac{1}{\sqrt{2^{3n}}} \sum_{\alpha, \beta, \gamma} \sum_{m,k} (-1)^{\alpha \bullet m \oplus \beta \bullet E(m,k) \oplus \gamma \bullet k} |\alpha\beta\gamma\rangle$
- ▶ Messen eines Zustands $\sum_{i=0}^{2^n} a_i |i\rangle$: Wir erhalten $|i\rangle$ mit Wahrscheinlichkeit $|a_i|^2$
- ▶ Also: $|\alpha\beta\gamma\rangle$ wird mit Wahrscheinlichkeit $\frac{1}{2^{n+t}} \frac{1}{2^{3n}} |\chi_E(\alpha, \beta, \gamma)|^2$ gemessen

Hidden Subgroup Problem (HSP)

Sei G eine Gruppe, $H \leq G$ eine Untergruppe, X eine Menge.

- ▶ $f : G \rightarrow X$ versteckt die Gruppe H , wenn f.a. $g_1, g_2 \in G$ gilt

$$f(g_1) = f(g_2) \iff g_1H = g_2H$$

- ▶ Faktorisierung, Logarithmus lassen sich auf das HSP für **abelsche** Gruppen reduzieren
- ▶ Für abelsche Gruppen existiert ein QA für das Hidden Subgroup Problem
- ▶ Wir kennen für einige nichtabelsche Gruppen ebenfalls effiziente Quantenalgorithmen
- ▶ Auch Gitterprobleme lassen sich auf das HSP reduzieren
 - ▶ Allerdings für Gruppen, für die noch kein eff. Quantenalgorithmus bekannt ist

Sind wir nahe dran, Gitterprobleme zu brechen?