Kryptografie und -analyse, Zusammenfassung Vorlesung 11

Henry Haustein

Welche passiven/aktiven Angriffe sind bei der unsicheren Variante von RSA möglich?

passive Angriffe: RSA arbeitet deterministisch, man kann also verschlüsseln und vergleichen

aktive Angriffe: RSA ist ein Homomorphismus bezüglich Multiplikation: Angreifer beobachtet Signaturen s_1, s_2 für Nachrichten m_1, m_2. Dann ist $s_3 = s_1 \cdot s_2$ eine Signatur für $m_3 = m_1 \cdot m_2$

Wie sind diese Angriffe zu verhindern?

Zufallszahl r hinzufügen: $c = (r, m, h(r, m))^{k_e}$

Was ist ein quadratischer Rest?

Quadratische Reste modulo p:

$$\mathcal{QR}_p = \{x \in \mathbb{Z}_p^* \mid \exists y \in \mathbb{Z}_p^* : y^2 \equiv x \mod p\}$$

Wie kann ermittelt werden, ob eine Zahl quadratischer Rest mod p bzw. mod n ist?

Euler-Kriterium:

$$z \in \mathcal{QR} \quad \Leftrightarrow \quad z^{\frac{p-1}{2}} \equiv 1 \mod p$$

Wie können Wurzeln mod p ($p \equiv 3 \mod 4$) bzw. mod n bestimmt werden?

Es gilt:

$$y = \pm z^{\frac{p+1}{4}} \mod p$$

Wie funktioniert das Rabin-System?

Schlüsselgenerierung: Jeder Teilnehmer

- wählt zufällig und unabhängig 2 verschiedene Primzahlen p und q mit $p \equiv q \equiv 3 \mod 4$
- berechnet $n = p \cdot q$

$\Rightarrow$ öffentlicher Schlüssel: n

$\Rightarrow$ privater Schlüssel: (p, q)

Verschlüsselung:

$$c = m^2 \mod n$$

Entschlüsselung:

- Empfänger bestimmt 4 Quadratwurzeln aus c
- unklar, welche Wurzel die Nachricht ist

Wie kann seine Sicherheit gezeigt werden?

Der große Vorteil des Rabin-Kryptosystems ist, dass man es nur dann brechen kann, wenn man das beschriebene Faktorisierungsproblem effizient lösen kann.

Anders als etwa bei RSA lässt sich zeigen, dass das Rabin-Kryptosystem genauso schwer zu brechen ist wie das Faktorisierungsproblem, auf dem es beruht. Es ist somit sicherer. Wer also das Rabin-Verfahren brechen kann, der kann auch das Faktorisierungsproblem lösen und umgekehrt. Es gilt daher als sicheres Verfahren, solange das Faktorisierungsproblem ungelöst ist. Vorausgesetzt ist dabei wie bereits beschrieben aber, dass die Klartexte keine bestimmte Struktur aufweisen.

Da man auch außerhalb der Kryptologie bemüht ist Faktorisierungsprobleme zu lösen, würde sich eine Lösung rasch in der Fachwelt verbreiten. Doch das ist bislang nicht geschehen. Man kann also davon ausgehen, dass das zugrundeliegende Faktorisierungsproblem derzeit unlösbar ist. Ein Angreifer, der nur belauscht, wird daher derzeit nicht in der Lage sein, das System zu brechen.

Ein aktiver Angreifer aber kann das System mit einem Angriff mit frei wählbarem Geheimtext (englisch *chosen-ciphertext attack*) brechen, wie sich mathematisch zeigen lässt. Aus diesem Grund findet das Rabin-Kryptosystem in der Praxis kaum Anwendung.

Durch Hinzufügen von Redundanz, z. B. Wiederholen der letzten 64 Bit, wird die Wurzel eindeutig. Dadurch ist der Angriff vereitelt (weil der Entschlüssler nur noch die Wurzel zurückliefert, die der Angreifer schon kennt). Dadurch ist die Äquivalenz der Sicherheit zum Rabin-Kryptosystem nicht mehr beweisbar. Allerdings, laut dem *Handbook of Applied Cryptography* von Menezes, Oorschot und Vanstone, hält die Äquivalenz unter der Annahme, dass das Wurzelziehen ein zweigeteilter Prozess ist (1. Wurzel $\mod p$ und Wurzel $\mod q$ ziehen und 2. Chinesischen Restsatzalgorithmus anwenden).

Da bei der Kodierung nur die quadratischen Reste verwendet werden (im Beispiel $n = 77$ sind das nur 23 der 76 möglichen Zustände), ist das Verfahren zusätzlich angreifbar.

siehe: https://de.wikipedia.org/wiki/Rabin-Kryptosystem

Welche Angriffsmöglichkeit ergibt sich?

aktiver Angriff, gewählter-Schlüsseltext-Angriff

Was ist eine elliptische Kurve?

Alle Punkte (x, y), die

$$y^2 = x^3 + ax + b$$

erfüllen + Punkt im Unendlichen $\mathcal{O}$.

Wie wird auf elliptischen Kurven gerechnet?

Addition geometrisch:

- Gerade durch P und Q
- diese Gerade schneidet Kurve in R'
- $R = P + Q$ entsteht durch Spiegelung von R' an der x-Achse

Addition analytisch:

$$\begin{aligned} s &= \frac{y_Q - y_P}{x_Q - x_P} \\ x_R &= s^2 - x_P - x_Q \\ y_R &= -y_P + s(x_P - x_R) \end{aligned}$$