

Einwegfunktion unter Quadratwurzelannahme

Definition Einwegfunktion QUADRAT

Definieren *Einwegfunktionsfamilie* QUADRAT = $(Gen, Samp, f)$ als

- ❶ **Gen** (1^n) : $(N, p, q) \leftarrow GenModulus(1^n)$, Ausgabe $I = N$.
Definiert $f : \mathbb{Z}_N^* \rightarrow QR_N$.
- ❷ **Samp** (I) : Wähle $x \in_R \mathbb{Z}_N^*$ zufällig.
- ❸ **f** (I, x) : Berechne $f(x) := x^2 \bmod N$.

Anmerkungen:

- QUADRAT ist Einwegfunktion unter der Quadratwurzelannahme.
- D.h. QUADRAT ist Einwegfunktion unter Faktorisierungsannahme.
- **Ziel:** Konstruktion einer Trapdoor-Einwegpermutation.

Hauptwurzeln

Satz Existenz einer Hauptwurzel

Sei $N = pq$ eine Blumzahl. Dann besitzt jedes $a \in QR_N$ genau ein $b \in QR_N$ mit $b^2 = a \bmod N$. Wir bezeichnen b als *Hauptwurzel*.

Beweis:

- Sei $p = 4k + 3$. Es gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = (-1) \bmod p$.
- D.h. $(-1) \in QNR_p$. Analog folgt $(-1) \in QNR_q$.
- Die vier Quadratwurzeln von a seien

$$(b_p, b_q), (b_p, -b_q), (-b_p, b_q), (-b_p, -b_q).$$

- Angenommen $\left(\frac{b_p}{p}\right) = 1$ und $\left(\frac{b_q}{q}\right) = (-1)$. (andere 3 Fälle analog)
- Dann gilt $\left(\frac{-b_p}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{b_p}{p}\right) = (-1)$ und $\left(\frac{-b_q}{q}\right) = 1$.
- Dann ist nur $b := (b_p, -b_q) \in QR_p \times QR_q$ und damit $b \in QR_N$.

RABIN Trapdoor-Einwegpermutation

Definition RABIN Trapdoor-Einwegpermutation

Trapdoor-Einwegpermutationsfamilie $\text{RABIN} = (\text{Gen}, \text{Samp}, f)$ mit

- ① **Gen**(1^n) : $(N, p, q) \leftarrow \text{GenModulus}(1^n)$ mit Blumzahl N .
Ausgabe $I = N$, $td = (p, q)$. Definiert $f : QR_N \rightarrow QR_N$.
- ② **Samp**(I) : Wähle $r \in_R \mathbb{Z}_N^*$ zufällig. Berechne $x \leftarrow r^2 \bmod N$.
- ③ **f**(I, x) : Berechne $f(x) := x^2 \bmod N$.
- ④ **Inv**(td, y) : Bestimme Hauptwurzel $x \in QR_N$ von $y = x^2$.

Anmerkungen:

- RABIN ist einweg unter der Faktorisierungsannahme. Wir wissen:
Trapdoor-Einwegpermutation + Hardcore-Prädikat
= CPA-sichere Verschlüsselung.
- Benötigen ein Hardcore-Prädikat $hc : QR_N \rightarrow \{0, 1\}$ für f .

Berechnen des niederwertigsten Bits

Satz Hardcore-Prädikat $lsb(x)$

Sei f die RABIN Trapdoor-Einwegpermutation und N eine Blumzahl. Für $x \in QR_N$ bezeichne $lsb(x)$ das niederwertigste Bit von x . Dann ist $hc(x) := lsb(x)$ ein Hardcore-Prädikat für f .

- ohne Beweis (nicht-trivial)
- Für alle ppt $\mathcal{A}$ gilt damit $Ws[\mathcal{A}(N, x^2) = lsb(x)] \leq \frac{1}{2} + \text{negl}(n)$.

RABIN Kryptosystem (1979)

Algorithmus RABIN Verschlüsselung

- ❶ **Gen:** $(N, p, q) \leftarrow \text{GenModulus}(1^n)$, wobei N eine Blumzahl ist.
Ausgabe $pk = N$, $sk = (p, q)$.
- ❷ **Enc:** Für $m \in \{0, 1\}$ wähle $r \in \mathbb{Z}_N^*$, berechne $x \leftarrow r^2 \bmod N$ und
 $c \leftarrow (x^2 \bmod N, \text{lsb}(x) \oplus m)$.
- ❸ **Dec:** Für $c = (c_1, c_2)$ berechne Hauptwurzel x von c_1 und
 $m \leftarrow \text{lsb}(x) \oplus c_2$.

Satz CPA-Sicherheit von RABIN

RABIN Verschlüsselung ist CPA-sicher unter der Faktorisierungsannahme.

Beweis:

- Folgt aus dem Satz zur CPA-Sicherheit von VERSCHLÜSSELUNG_n .

Diskussion RSA versus RABIN

Vergleich: RSA und RABIN

- Quadrieren und Exponentieren mit e erscheinen ähnlich.
- Aber: RABIN ist kein Spezialfall von RSA, da $e = 2 \notin \mathbb{Z}_{\phi(N)}^*$.
- RABIN-Einwegpermutation beruht auf Faktorisierungsannahme.
- Die Faktorisierungsannahme ist möglicherweise schwächer als die RSA-Annahme. Offen: Invertieren von RSA $\Rightarrow$ Faktorisierung?
- RABIN ist nicht ineffizienter als RSA.

- Historische Variante: Textbook RABIN mit $c \leftarrow m^2 \bmod N$.
- Es existiert ein CCA-Angriff auf Textbook RABIN, der p, q liefert. (Wie?)

Die Gruppe $\mathbb{Z}_{N^2}^*$

Lemma Teilerfremdheit von N und $\phi(N)$

Sei $N = pq$ ein RSA-Modulus mit p, q gleicher Bitlänge. Dann gilt $\text{ggT}(N, \phi(N)) = 1$.

Beweis:

- OBdA $p > q$. Dann kann p weder $p - 1$ noch $q - 1$ teilen.
- Annahme: q teilt $p - 1$. Dann ist $\frac{p-1}{q} \geq 2$.
- Widerspruch: $\frac{p}{q} < 2$, da p, q gleiche Bitlänge besitzen.

Lemma Ordnung von $(1 + N)$

Sei N ein RSA-Modul. Dann besitzt $(1 + N)$ in $\mathbb{Z}_{N^2}^*$ Ordnung N .

Beweis:

- Es gilt $(1 + N)^a = \sum_{i=0}^a \binom{a}{i} N^i = 1 + aN \pmod{N^2}$.
- D.h. $(1 + N)^a \neq 1 \pmod{N^2}$ für $1 \leq a < N$ und $(1 + N)^N = 1 \pmod{N^2}$.

Die Struktur von $\mathbb{Z}_{N^2}^*$

Satz Isomorphismus $\mathbb{Z}_N \times \mathbb{Z}_N^* \simeq \mathbb{Z}_{N^2}^*$

Die Abbildung $f : \mathbb{Z}_N \times \mathbb{Z}_N^* \rightarrow \mathbb{Z}_{N^2}^*$ mit $f(a, b) = (1 + N)^a \cdot b^N \bmod N^2$ ist ein Isomorphismus, d.h.

- 1 f ist bijektiv.
- 2 $f(a_1, b_1) \cdot f(a_2, b_2) = f(a_1 + a_2, b_1 b_2) \quad \forall a_1, a_2 \in \mathbb{Z}_N, b_1, b_2 \in \mathbb{Z}_N^*.$

Beweis: Bijektivität

- Zeigen, dass $|\mathbb{Z}_N \times \mathbb{Z}_N^*| = |\mathbb{Z}_{N^2}^*|$ und dass f injektiv ist.
- $|\mathbb{Z}_{N^2}^*| = \phi(N^2) = (p^2 - p)(q^2 - q) = pq(p-1)(q-1) = |\mathbb{Z}_N| \cdot |\mathbb{Z}_N^*|$
- **Annahme:** $\exists (a_1, b_1) \neq (a_2, b_2)$ mit $f(a_1, b_1) = f(a_2, b_2)$.
- Dann folgt $(1 + N)^{a_1} b_1^N = (1 + N)^{a_2} b_2^N \bmod N^2$.
- Wegen $|\mathbb{Z}_{N^2}^*| = N \cdot \phi(N)$ liefert Potenzieren mit $\phi(N)$
$$(1 + N)^{(a_1 - a_2)\phi(N)} = 1 \bmod N^2.$$
- Es gilt $\text{ord}(1 + N) = N$ und daher $N | (a_1 - a_2)\phi(N)$.
- Wegen $\text{ggT}(N, \phi(N)) = 1$ folgt $N | a_1 - a_2$, d.h. $a_1 \equiv a_2 \bmod N$.

Beweis: Fortsetzung Bijektivität

- $a_1 = a_2$ liefert $b_1^N = b_2^N \bmod N^2$ und damit $b_1^N = b_2^N \bmod N$.
- Wegen $\text{ggT}(N, \phi(N))$ ist die Exponentiation mit N bijektiv.
- Daraus folgt $b_1 = b_2 \bmod N$. (Widerspruch: $(a_1, b_1) \neq (a_2, b_2)$)

Beweis: Homomorphismus-Eigenschaft

- Es gilt $f(a_1, b_1) \cdot f(a_2, b_2) = (1 + N)^{a_1+a_2} \cdot (b_1 b_2)^N \bmod N^2$.
- Wegen $\text{ord}(1 + N) = N$ entspricht dies $(1 + N)^{a_1+a_2 \bmod N} \cdot (b_1 b_2)^N$.
- Es gilt
$$f(a_1 + a_2, b_1 b_2) = (1 + N)^{a_1+a_2 \bmod N} \cdot (b_1 b_2 \bmod N)^N \bmod N^2.$$
- Sei $r = b_1 b_2 \bmod N$. D.h. $b_1 b_2 = r + kN$.
- Dann gilt $(b_1 b_2)^N = (r + kN)^N = r^N = (b_1 b_2 \bmod N)^N \bmod N^2$. $\square$