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 RABIN$= (Gen, Samp, f)$ mit

1. $\boldsymbol{Gen(1^n)}$: $(N, p, q) \leftarrow GenModulus(1^n)$ mit Blumzahl N.
   Ausgabe $I = N$, $td = (p, q)$. Definiert $f : QR_N \rightarrow QR_N$.
2. $\boldsymbol{Samp(I)}$: Wähle $r \in_R \mathbb{Z}_N^*$ zufällig. Berechne $x \leftarrow r^2 \bmod N$.
3. $\boldsymbol{f(I, x)}$: Berechne $f(x) := x^2 \bmod N$.
4. $\boldsymbol{Inv(td, y)}$: 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 $\mathrm{Ws}[\mathcal{A}(N, x^2) = lsb(x)] \leq \frac{1}{2} + \mathrm{negl}(n)$.

RABIN Kryptosystem (1979)

Algorithmus RABIN Verschlüsselung

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

Satz CPA-Sicherheit von RABIN

RABIN Verschlüsselung ist CPA-sicher unter der Faktorisierungsannahme.

Beweis:

- Folgt aus dem Satz zur CPA-Sicherheit von VERSCHLÜSSELUNG$_\Pi$.

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 $\mathrm{ggT}(N, \phi(N)) = 1$.

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

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

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

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

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

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 $\mathrm{ord}(1+N) = N$ und daher $N \mid (a_1-a_2)\phi(N)$.
- Wegen $\mathrm{ggT}(N, \phi(N)) = 1$ folgt $N \mid a_1 - a_2$, d.h. $a_1 = a_2 \bmod N$.

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 $\mathrm{ggT}(N, \phi(N))$ 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 $\mathrm{ord}(1+N) = N$ 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 $(b_1 b_2)^N = (r+kN)^N = r^N = (b_1 b_2 \bmod N)^N \bmod N^2$. $\square$

N-te Reste

Definition N-te Reste

Sei N ein RSA-Modul. Wir bezeichnen die Elemente der Menge $Res(N^2) := \{y \in \mathbb{Z}^*_{N^2} \mid \exists x \in \mathbb{Z}^*_{N^2} \text{ mit } x^N = y\}$ als *N-te Reste* in $\mathbb{Z}^*_{N^2}$.

Lemma Eigenschaften N-ter Reste

1. Exponentiation mit N ist eine $(N:1)$-Abbildung in $\mathbb{Z}^*_{N^2}$.
2. $Res(N^2) \simeq \{(0,b) \mid b \in \mathbb{Z}^*_N\}$

Beweis:

- Sei $x \in \mathbb{Z}^*_{N^2}$ mit $x \simeq (a,b)$. Dann gilt
$$x^N \bmod N^2 \simeq (a,b)^N = (N \cdot a \bmod N, b^N \bmod N) = (0, b^N).$$
- Für die N Elemente (a,b), $a \in \mathbb{Z}_N$, gilt $(a,b)^N = (0,b^N)$.
- Damit ist jeder N-te Rest von der Form $(0,b^N)$.
- Bleibt zu zeigen, dass jedes Element $y = (0,b)$ ein N-ter Rest ist.
- Wir definieren $x = (0, b^{N^{-1} \bmod \phi(N)})$. Damit gilt
$$x^N \simeq (0, b^{N^{-1} \bmod \phi(N)})^N = (N \cdot 0, b^{N^{-1}N} \bmod N) = (0,b) \simeq y.$$