

N-te Reste

Definition N-te Reste

Sei N ein RSA-Modul. Wir bezeichnen die Elemente der Menge $\text{Res}(N^2) := \{y \in \mathbb{Z}_{N^2}^* \mid \exists x \in \mathbb{Z}_{N^2}^* \text{ mit } x^N = y\}$ 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 $\text{Res}(N^2) \simeq \{(0, b) \mid b \in \mathbb{Z}_N^*\}$

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
$$x^N \simeq (0, b^{N^{-1} \bmod \phi(N)})^N = (N \cdot 0, b^{N^{-1}N} \bmod N) = (0, b) \simeq y.$$

DCR Annahme

Satz Decisional Composite Residuosity (DCR)

Das *Decisional Composite Residuosity* Problem ist hart bezüglich GenModulus falls für alle ppt \mathcal{A} und $r \in_R \mathbb{Z}_{N^2}^*$ gilt

$$|\text{Ws}[\mathcal{A}(N, r^N \bmod N^2) = 1] - \text{Ws}[\mathcal{A}(N, r) = 1]| \leq \text{negl}(n).$$

DCR Annahme: DCR ist hart bezüglich GenModulus.

- DCR Annahme: Unterscheiden von $(0, r)$ und (r', r) ist schwer.

Idee: zur Konstruktion einer Verschlüsselungsfunktion

- Sei $m \in \mathbb{Z}_N$. Wähle einen zufälligen N -ten Rest $(0, r)$ und setze
$$c \leftarrow (m, 1) \cdot (0, r) = (m, r).$$
- Da $(0, r)$ unterscheidbar von (r', r) , ist c ununterscheidbar von
$$c' \leftarrow (m, 1) \cdot (r', r) = (m + r', r).$$
- $c' = (m + r', r)$ ist für $r' \in_R \mathbb{Z}_N$ ein zufälliges Element in $\mathbb{Z}_N \times \mathbb{Z}_N^*$.
- Insbesondere ist c' unabhängig von m .

Verschlüsselung

Algorithmus Verschlüsselung

EINGABE: $m \in \mathbb{Z}_N$

- 1 Wähle $r \in_R \mathbb{Z}_N^*$.
- 2 Berechne $c \leftarrow f(m, r) = (1 + N)^m \cdot r^N \bmod N^2$.

AUSGABE: $c \in \mathbb{Z}_{N^2}^*$

Anmerkungen:

- Wir berechnen das Bild von (m, r) unter unserem Isomorphismus.
- Faktor der Nachrichtenexpansion beträgt 2.

Entschlüsselung

Algorithmus Entschlüsselung

EINGABE: $c \simeq (m, r) \in \mathbb{Z}_{N^2}^*$

- 1 Berechne $c' \leftarrow c^{\phi(N)} \bmod N^2$.
- 2 Berechne $m' \leftarrow \frac{c'-1}{N}$ über \mathbb{N} .
- 3 Berechne $m \leftarrow m' \cdot \phi(N)^{-1} \bmod N$.

AUSGABE: $m \in \mathbb{Z}_N$

Korrektheit:

- Es gilt $c' \simeq (m, r)^{\phi(N)} = (m\phi(N), r^{\phi(N)}) = (m\phi(N), 1)$.
- Damit gilt
$$c' = (1 + N)^{m\phi(N)} \bmod N^2 = 1 + (m\phi(N) \bmod N) \cdot N \bmod N^2.$$
- Da $1 + (m\phi(N) \bmod N)N < N^2$ gilt die Gleichung über \mathbb{N} .
- Daraus folgt $m' = m\phi(N) \bmod N$. Multiplikation mit $\phi(N)^{-1}$ liefert
$$m = m' \cdot \phi(N)^{-1} \bmod N.$$

Paillier Kryptosystem (1999)

Algorithmus Paillier Verschlüsselung

- 1 **Gen:** $(N, p, q) \leftarrow \text{GenModulus}(1^n)$. Ausgabe $pk = N, sk = \phi(N)$.
- 2 **Enc:** Für eine Nachricht $m \in \mathbb{Z}_N$, wähle ein $r \in_R \mathbb{Z}_N^*$ und berechne
$$c \leftarrow (1 + N)^m \cdot r^N \bmod N^2.$$
- 3 **Dec:** Für einen Chiffretext $c \in \mathbb{Z}_{N^2}^*$ berechne

$$m \leftarrow \frac{(c^{\phi(N)} \bmod N^2) - 1}{N} \cdot \phi(N)^{-1} \bmod N.$$

Sicherheit von Paillier Verschlüsselung

Satz Sicherheit von Paillier Verschlüsselung

Unter der DCR Annahme ist Paillier Verschlüsselung CPA-sicher.

Beweis:

- Sei Π das Paillier Verschlüsselungs-Verfahren.
- Sei \mathcal{A} ein Angreifer mit Erfolgsws $\epsilon(n) = \text{Ws}[PubK_{\mathcal{A},\Pi}^{cpa}(n) = 1]$.
- Konstruieren Algorithmus \mathcal{A}_{dcr} für das DCR Problem.

Algorithmus DCR Unterscheider \mathcal{A}_{dcr}

EINGABE: N, y

- 1 Setze $pk = N$ und berechne $(m_0, m_1) \leftarrow \mathcal{A}(pk)$.
- 2 Wähle $b \in \{0, 1\}$ und berechne $c \leftarrow (1 + N)^{m_b} \cdot y \bmod N^2$.
- 3 $b' \leftarrow \mathcal{A}(c)$.

AUSGABE: $= \begin{cases} 1 & \text{falls } b = b', \\ 0 & \text{sonst,} \end{cases}$ Interpretation $y \in \text{Res}(N^2)$
Interpretation $y \in \mathbb{Z}_{N^2}^*$

Sicherheit von Paillier Verschlüsselung

Fall 1: $y \in_R \text{Res}(N^2)$, d.h. $y = r^N$ für $r \in_R \mathbb{Z}_N^2$.

- Verteilung von c identisch zum Paillier Verfahren.
- D.h. $\text{Ws}[\mathcal{A}_{dcr}(N, r^N) = 1] = \epsilon(n)$.

Fall 2: $y \in_R \mathbb{Z}_{N^2}^*$, d.h. $y = r \in_R \mathbb{Z}_{N^2}^*$.

- Dann ist $c = (1 + N)^{mb} \cdot y \bmod N^2$ zufällig in $\mathbb{Z}_{N^2}^*$.
- Insbesondere ist die Verteilung von c unabhängig von b .
- Daraus folgt $\text{Ws}[\mathcal{A}_{dcr}(N, r) = 1] = \frac{1}{2}$.

- Unter der DCR-Annahme folgt

$$\begin{aligned} \text{negl}(n) &\geq \left| \text{Ws}[\mathcal{A}_{dcr}(N, r^N \bmod N^2) = 1] - \text{Ws}[\mathcal{A}_{dcr}(N, r) = 1] \right| \\ &= \left| \epsilon(n) - \frac{1}{2} \right|. \end{aligned}$$

- Daraus folgt $\epsilon(n) \leq \frac{1}{2} + \text{negl}(n)$.

Homomorphe Verschlüsselung

Definition Homomorphe Verschlüsselung

Sei Π ein Verschlüsselungsverfahren mit $Enc : G \rightarrow G'$ für Gruppen G, G' . Π heißt *homomorph*, falls $Enc(m_1) \circ Enc(m_2)$ eine gültige Verschlüsselung von $m_1 \circ m_2$ für alle $m_1, m_2 \in G$ ist.

Bsp:

- **Textbook-RSA** mit $Enc : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ und

$$m_1^e \cdot m_2^e = (m_1 \cdot m_2)^e \text{ mod } N.$$

Eigenschaft: Textbook-RSA ist nicht CPA-sicher.

- **ElGamal** mit $Enc : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ und

$$(g^{y_1}, h^{y_1} m_1) \cdot (g^{y_2}, h^{y_2} m_2) = (g^{y_1+y_2}, h^{y_1+y_2} m_1 m_2).$$

Eigenschaft: $G_1 = (\mathbb{Z}_p^*, \cdot)$ ist eine multiplikative Gruppe.

- **Goldwasser-Micali** mit $Enc : \{0, 1\} \rightarrow \mathbb{Z}_N^*$ und

$$z^{m_1} x_1^2 \cdot z^{m_2} x_2^2 = z^{m_1+m_2} (x_1 x_2)^2 \text{ mod } N.$$

Eigenschaft: $G_1 = (\mathbb{F}_2, +)$ ist eine additive Gruppe.

E-voting mit Paillier

- **Paillier** mit $Enc : \mathbb{Z}_N \rightarrow \mathbb{Z}_{N^2}^*$ und

$$(1 + N)^{m_1} r_1^N \cdot (1 + N)^{m_2} r_2^N = (1 + N)^{m_1+m_2} (r_1 r_2)^N \pmod{N^2}.$$

Eigenschaft: $G_1 = (\mathbb{Z}_N, +)$ ist additiv und groß.

Algorithmus E-voting mit Paillier

- Wahlleiter generiert öffentlichen RSA-Modul $N = pq$.
- Wähler $i \in [n]$ mit $n < N$ wählt $v_i = 0$ für NEIN, $v_i = 1$ für JA und sendet an alle anderen Wähler $c_i = (1 + N)^{v_i} r_i^N \pmod{N^2}$, $r_i \in_R \mathbb{Z}_N$.
- Wähler aggregieren $c := \prod_{i=1}^n c_i \pmod{N^2}$.
- Wahlleiter erhält c und veröffentlicht $Dec(c) = \sum_{i=1}^n v_i$.

Eigenschaften: (falls alle Parteien sich an das Protokoll halten)

- Wahlleiter erhält c , ohne die einzelnen c_i kennenzulernen.
- Kein Wähler erhält Informationen über die v_i anderer Wähler.
- Berechnung von c ist öffentlich verifizierbar.