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 $(1+N) \bmod N^2$

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

Beweis:

- Es gilt $(1+N)^a = \sum_{i=0}^{a} \binom{a}{i} N^i = 1 + aN \bmod N^2$.
- 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 $y \simeq (0, b)$ ein N-ter Rest ist.
- Falls $y \simeq (0, b)$ ist, so gilt $y = (1 + N)^0 \cdot b^N = b^N \bmod N^2$.
- Damit ist y ein N-ter Rest.

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

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

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 $(0, r)$ ununterscheidbar 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 $c' := c^{\phi(N)} \bmod N^2$.
2. Berechne $m' := \frac{c'-1}{N}$ über $\mathbb{N}$.
3. Berechne $m := m' \cdot \phi(N)^{-1} \bmod N$.

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

Korrektheit:

- Es gilt $c' \simeq (m, r)^{\phi(N)} = \left(m\phi(N), r^{\phi(N)}\right) = (m\phi(N), 1)$.
- Damit gilt

$$c' = (1+N)^{m\phi(N) \bmod N} \; 1^N = 1 + (m\phi(N) \bmod N) \cdot N \bmod N^2.$$

- 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:** $(N, p, q) \leftarrow \mathit{GenModulus}(1^n)$. 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
$$m' := \frac{\left(c^{\phi(N)} \bmod N^2\right) - 1}{N} \text{ über } \mathbb{N} \quad \text{und} \quad m := m' \cdot \phi(N)^{-1} \bmod N.$$

Sicherheit von Paillier Verschlüsselung

Satz Sicherheit von Paillier Verschlüsselung

Unter der DCR Annahme ist Paillier Verschlüsselung Π_P CPA-sicher.

Beweis:

- Sei $\mathcal{A}$ ein Angreifer mit Erfolgsws $\epsilon(n) = \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi_P}(n) = 1]$.
- Konstruieren Algorithmus $\mathcal{A}_{dcr}$ für das DCR Problem.

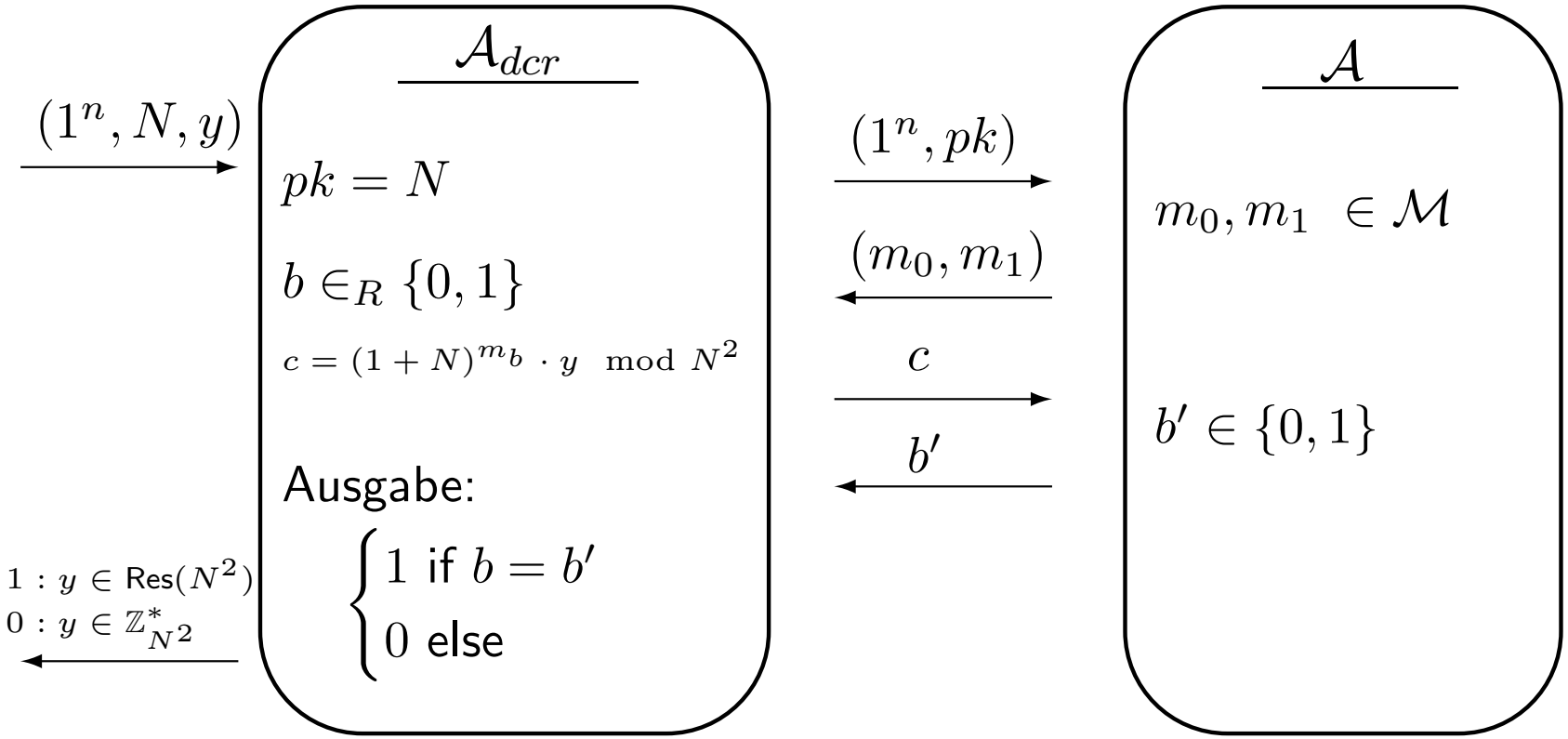
Algorithmus DCR Unterscheider $\mathcal{A}_{dcr}$

EINGABE: $1^n, N, y$

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

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

Algorithmus DRC Unterscheider



Sicherheit von Paillier Verschlüsselung

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

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

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

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

Unter der DCR-Annahme folgt

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

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