Vorlesung 1

20.4.2021

Literatur:

Neal Koblitz, A course in number theory and cryptography, Springer

Otto Forster, Algorithmische Zahlentheorie, Springer

Wolfgang Scherer, Mathematik der Quanteninformatik, Springer

I. RSA (und ElGamal)

Nachricht oder Klartext ist ein Bitwort endlicher Länge

$$M = (m_1, \dots, m_n), \quad m_i \in \{0,1\}.$$

Verschlüsselung ist Abb., abhängig von einem Schlüssel S,

$$V_S : M \longmapsto V_S(M) = (v_{S,1}(M), \dots, v_{S,r}(M)) \in \{0,1\}^r$$

Entschlüsselung

$$E_S = V_S^{-1} : V_S(M) \longmapsto E_S(V_S(M)) = M$$

RSA (Rivest - Shamir - Adleman 1978)

Wir wollen Nachrichten fester Länge B übertragen, also

$$M = (s_0, s_1, \dots, s_{B-1})$$

M repräsentiert eine Zahl $m \in \mathbb{N}_0$, nämlich

$$m := \sum_{j=0}^{B-1} s_j 2^j$$

mit $0 \le m < 2^B$ und umgekehrt.

Setze: $m_{max} := 2^B - 1$.

Prinzipielles Vorgehen:

1) Der Empfänger
   - sucht zwei große Primzahlen $p \neq q$ (mit $p, q > m_{max}$)
   - wähle $e \in \mathbb{N}$ mit $ggT(e, \underbrace{(p-1)(q-1)}_{=:\varphi(N)}) = 1$.
   - setze $N := pq$

   und gibt den öffentlichen Schlüssel $S = (N, e)$ bekannt.

2) Der Sender
   verschlüsselt eine Nachricht $0 \le m \le m_{max} < N$

durch $V_S(m) := m^e \pmod N$

(Wir rechnen in $\mathbb{Z}/N\mathbb{Z}$)

3) Der Empfänger berechnet $d \in \mathbb{N}$ mit

$$ed \equiv 1 \pmod{\varphi(N)}$$

und entschlüsselt mittels

$$E_S(V_S(m)) := V_S(m)^d \pmod N$$
$$\stackrel{?}{=} m \pmod N$$

(Fast) offensichtlich.

Falls man N faktorisieren kann, so hat man $\varphi(N) = (p-1)(q-1)$ und man kann mit dem erweiterten euklidischen Algorithmus d berechnen.

ANNAHME:
- Faktorisieren ist schwer!
- Außer durch Faktorisieren kann man d nicht berechnen.

ZIEL: Mit QC ist Faktorisieren nicht mehr schwer (Shor 1994)

$\Rightarrow$ PQ - Kryptographie: Suche nach anderen schweren math. Problemen mit denen man Kryptoverfahren bauen kann.

Mathematische Grundlagen von RSA

a) Einheiten in $\mathbb{Z}/N\mathbb{Z}$

Sei $N \in \mathbb{N}$.

Lemma: Sei $a \in \mathbb{Z}$. Dann gilt:

$$\bar{a} \in \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \iff ggT(a, N) = 1.$$

Andernfalls ist $\bar{a}$ ein Nullteiler in $\mathbb{Z}/N\mathbb{Z}$.

Beweis: „$\Rightarrow$" Sei $b \in \mathbb{Z}$ mit

$$ab \equiv 1 \pmod{N}$$

d.h. $\exists\, q \in \mathbb{Z}: \quad ab = 1 + qN$

$$\Rightarrow \quad 1 = ab - qN \quad \Rightarrow \quad ggT(a, N) = 1$$

„$\Leftarrow$" Mit dem <u>erweiterten euklidischen Algorithmus</u> berechnet man $x, y \in \mathbb{Z}$ mit

$$1 = ggT(a, N) = xa + yN$$

$$\Rightarrow \quad \bar{x}\bar{a} = \bar{1} \qquad (xa \equiv 1 \pmod{N})$$

d.h. $\bar{x}$ ist das Inverse von $\bar{a}$.

Zu „Andernfalls": Sei $d := ggT(a, N) > 1$

$$\Rightarrow \quad N = dd_1 \text{ mit } 1 < d, d_1 < N. \text{ Es gilt:}$$

$$\underbrace{\bar{d}}_{\neq \bar{0}} \cdot \underbrace{\bar{d}_1}_{\neq \bar{0}} = \bar{N} = \bar{0}$$

$a d_1 = \frac{a}{d} \cdot d d_1 = \underbrace{\frac{a}{d}}_{\in \mathbb{Z}} \cdot N \Rightarrow \bar{a}\,\bar{d_1} = \bar{0}$ ∎

Definition: $\varphi(N) := \left| \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \right|$

heißt Eulersche Funktion.

b) **Der Chinesische Restsatz**

R sei ein kommutativer Ring mit 1

Bspl: $\mathbb{Z}$, $K[X]$, K (K kp.), $\mathbb{Z}/N\mathbb{Z}$

Für $a \in R$ sei

$$(a) = aR = \{ ra \mid r \in R \}$$

das von a erzeugte Hauptideal.

Schreibweisen: $a \mid b$, falls es ein $c \in R$ gibt mit $b = ac$.

$a \sim b \iff a \mid b \;\&\; b \mid a$

Lemma: Sei R nullteilerfrei. Dann gilt für $a, b \in R$, $a \neq 0 \neq b$:

1) $a \sim b \overset{(*)}{\iff} \exists e \in R^\times : b = ae \iff (a) = (b)$

2) $a \mid b \iff (b) \subseteq (a)$

3) $(a) = R \iff a \in R^\times$

Beweis: Nur (*)

„$\Rightarrow$" $\left.\begin{aligned} a &= bc \\ b &= da \end{aligned}\right\} \Rightarrow a = dac$

$\Rightarrow a\underbrace{(1-dc)}_{\neq 0} = 0$

$\Rightarrow dc = 1 \Rightarrow d, c \in R^\times$

(R nullteilerfrei)

„$\Leftarrow$" klar. ∎

Definition: $\mathfrak{I} \subseteq R$ heißt **Ideal**, falls

- $0 \in \mathfrak{I}$
- $a, b \in \mathfrak{I} \Rightarrow a + b \in \mathfrak{I}$
- $a \in \mathfrak{I}, r \in R \Rightarrow ra \in \mathfrak{I}$

Beobachtung: $I, \mathfrak{I}$ Ideale in R $\Rightarrow$

$$I + \mathfrak{I} = \{ a + b \mid a \in I, b \in \mathfrak{I} \}$$

$$I \cap \mathfrak{I}$$

$$I\mathfrak{I} = \left\{ \sum_{\text{endl.}} a_i b_i \mid a_i \in I, \; b_i \in \mathfrak{I} \right\}$$

sind ebenfalls Ideale

Satz: $\mathbb{Z}$ ist ein HIR (d.h. nullteilerfrei und jedes Ideal ist ein Hauptideal).

Beweis: In $\mathbb{Z}$ kann man Teilen mit Rest, d.h. zu $a, b \in \mathbb{Z}$, $b \neq 0$, gibt es $q, r \in \mathbb{Z}$

mit $a = qb + r$ mit $0 \leq r < |b|$.

Sei $I \neq (0)$ ein Ideal in $\mathbb{Z}$. Sei:

$$a := \min(\underbrace{I \cap \mathbb{N}}_{\neq \emptyset}) = \text{kleinste pos. ganze Zahl in } I$$

Wir zeigen: $(a) = I$

„$\subseteq$" klar, da $a \in I$

„$\supseteq$" Sei $b \in I$. Schreibe $b = qa + r$, $0 \leq r < a$.

$$\Rightarrow r = \underbrace{b}_{\in I} - q\underbrace{a}_{\in I} \in I \Rightarrow r = 0$$

$$\Rightarrow b \in (a)$$

∎

Bemerkung: Alle euklidischen Ringe (z.B. auch $K[x]$) sind HIR.

Übung: Es gilt in $\mathbb{Z}$

$$(a) + (b) = (d) \text{ mit}$$

$$d = ggT(a, b).$$

Chinesischer Restsatz: Seien $I_1, \dots, I_n$ Ideale in R mit $I_k + I_\ell = R$ für $k \neq \ell$. Seien $a_1, \dots, a_n \in R$. Dann gibt es $x \in R$ mit

$$x \equiv a_i \pmod{I_i}, \quad i = 1, \dots, n.$$

Falls $y \in R$ eine weitere Lsg. der simultanen Kongruenzen ist, so gilt

$$x \equiv y \pmod{J}, \quad J := I_1 \cap \dots \cap I_n.$$

Beweis: Induktion über n.

$n = 2$: $I_1 + I_2 = R \Rightarrow \tilde{z}_1 + \tilde{z}_2 = 1$, $\tilde{z}_1 \in I_1$, $\tilde{z}_2 \in I_2$

$\Rightarrow a_2 - a_1 = z_1 + z_2$, $z_i \in I_i$, $i = 1, 2$

$\Rightarrow \underbrace{z_1}_{\in I_1} + a_1 = a_2 \underbrace{- z_2}_{\in I_2} =: x$ leistet das Verlangte

$n \to n+1$: Löse

$$\begin{aligned} y &\equiv a_1 \pmod{I_1} \\ &\vdots \\ y &\equiv a_n \pmod{I_n} \end{aligned}$$

nach Induktion. Löse nun

$$\begin{aligned} x &\equiv y \pmod{I_1 \cap \dots \cap I_n} \\ x &\equiv a_{n+1} \pmod{I_{n+1}} \end{aligned}$$

Dann leistet x das Verlangte, denn:

$$x \equiv y \pmod{I_1 \cap \dots \cap I_n}$$

$$\Rightarrow \quad x \equiv y \pmod{I_j}, \qquad j = 1, \dots, n.$$

$$\Rightarrow \quad x \equiv a_j \pmod{I_j}, \qquad j = 1, \dots, n.$$

Nach z.z.: • $I_1 \cap \dots \cap I_n + I_{n+1} = R$

Übung • $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$

Die Eindeutigkeit folgt aus

$$x \equiv y \pmod{I_j} \qquad j = 1, \dots, n$$

$$\Leftrightarrow \quad x - y \in I_j \qquad \text{—"—}$$

$$\Leftrightarrow \quad x - y \in J \quad \Leftrightarrow \quad x \equiv y \pmod{J}$$

∎

Folgerung: Voraussetzungen wie im CR. Dann ist

$$\varphi : R/J \longrightarrow R/I_1 \oplus \dots \oplus R/I_n$$

$$x + J \longmapsto (x + I_1, \dots, x + I_n)$$

ein Ringisomorphismus.

Beweis: Surjektivität folgt aus der Existenzaussage.
Injektivität —"— Eindeutigkeit.

∎

Folgerung: Sei $N = p_1^{e_1} \cdots p_n^{e_n}$ die Primzahlzerlegung von N. Dann gilt:

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{e_n}\mathbb{Z}.$$

Beweis: CR für $R = \mathbb{Z}$, $I_j = (p_j^{e_j})$. ∎

Folgerung: $\varphi(N) = \prod_{i=1}^{n} \varphi(p_i^{e_i})$

Satz: Sei p eine Primzahl, $e \in \mathbb{N}$. Dann gilt:

$$\varphi(p^e) = (p-1)\,p^{e-1}$$

Beweis: Abzählen. ∎

Zurück zu RSA: $N = pq$

$\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$ ist Ordnung der abelschen Gruppe $\left(\mathbb{Z}/N\mathbb{Z}\right)^\times$