Vorlesung 2

27.4.2021

RSA

Öffentlicher Schlüssel: $N = pq$, e

mit $\text{ggT}(e, \varphi(N)) = 1$

Dabei: $\varphi(N) = (p-1)(q-1)$.

Geheimer Schlüssel: d mit $ed \equiv 1 \pmod{\varphi(N)}$

Verschlüsselung: $V(m) = m^e \pmod N$

Entschlüsselung: $E(m) = m^d \pmod N$

Noch zu zeigen: $E(V(m)) = \underline{m^{ed} \equiv m \pmod N}$ $(*)$

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

$N = p_1^{e_1} \cdots p_s^{e_s}$ $\quad \overset{CR}{=} \prod_{i=1}^{s} \varphi(p_i^{e_i})$

$= \prod_{i=1}^{s} (p_i - 1) p_i^{e_i - 1}$

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

Beweis:

$0, \underbrace{1, 2, \ldots, p-1}_{\text{teilerfremd zu } p}, p, \underbrace{p+1, \ldots, 2p-1}_{\text{—"—}}, 2p, \ldots, p^e - 1$

$p^e - 1 = p p^{e-1} - 1$

Es gibt p^{e-1} solche Intervalle

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

Satz von Lagrange: Sei G eine endliche Gruppe. Dann gilt für alle $g \in G$:

$$g^{|G|} = e.$$ ohne Beweis

Spezialfall ("kleiner Satz von Fermat")

Sei $a \in \mathbb{Z}$, $N \in \mathbb{N}$ und $\operatorname{ggT}(a, N) = 1$. Dann gilt:

$$a^{\varphi(N)} \equiv 1 \pmod N.$$

Beweis: Hier ist $G = \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$, $|G| = \varphi(N)$ ∎

Zu (*) (Korrektheit von RSA)

$$E(V(m)) = m^{ed} = m^{1+k\varphi(N)} = m \cdot \underbrace{\left(m^{\varphi(N)}\right)^k}_{\equiv 1}$$

$ed = 1 + k\varphi(N)$, $k \in \mathbb{Z}$ $\equiv m \pmod N$ ∎

- Bester bekannter Faktorisierungsalgorithmus: Zahlkörpersieb

- QC können "schnell" faktorisieren (Shor 1994)
- Andere Kryptoverfahren beruhen auf dem diskreten Logarithmenproblem:

  Sei $G = \langle 5 \rangle$ eine zyklische Gruppe und $g \in G$. Finde e mit $g = 5^e$.

  Bspl: • $G = \mathbb{F}_p^\times = \langle \omega \rangle$
  • G = Untergruppe von $E(\mathbb{F}_p)$ (elliptische Kurve)

  Auch DL-Problem kann ein QC "schnell" lösen.

Hilberträume

Es sei stets $K = \mathbb{R}$ oder $\mathbb{C}$.

Definition: Sei E ein VR über K. Ein Skalarprodukt ist eine Abb.

$$\langle , \rangle = \langle \,|\, \rangle : E \times E \longrightarrow K$$

mit:

a) $\langle , \rangle$ ist sesquilinear, d.h.

$$\langle x, y_1 + y_2 \rangle = \langle x, y_1 \rangle + \langle x, y_2 \rangle$$
$$\langle x, \lambda y \rangle = \lambda \langle x, y \rangle$$

($\langle x_1 + x_2, y \rangle = \langle x_1 + x_2, y \rangle$

$\langle \lambda x, y \rangle = \overline{\lambda} \langle x, y \rangle$.)

b) $\langle \, , \rangle$ ist <u>symmetrisch</u>, $\langle x, y \rangle = \overline{\langle y, x \rangle}$

c) $\langle \, , \rangle$ ist <u>pos. definit</u>, d.h.

$$\langle x, x \rangle \geq 0, \quad \forall x \in E$$

$$\langle x, x \rangle = 0 \iff x = 0$$

<u>Bspl:</u> • $\mathbb{C}^n$ oder $\mathbb{R}^n$ mit

$$\langle x, y \rangle := \sum_{i=1}^{n} \overline{x}_i y_i = \overline{x}^t y$$

• $E = \mathcal{C}([0,1]) =$ stetige Fkt. $[0,1] \to K$

mit $\langle f, g \rangle := \int_0^1 \overline{f(t)}\, g(t)\, dt$

<u>Definition:</u> Ein <u>Prähilbertraum</u> ist ein K-VR E zusammen mit einem Skalarprodukt.

Auf E hat man eine Norm

$$\| \, \| : E \longrightarrow \mathbb{R}, \quad \|x\| := \sqrt{\langle x, x \rangle}$$

Es gilt die Cauchy-Schwarz'sche Ungleichung:

$$|\langle x, x \rangle| \leq \|x\| \cdot \|y\|, \quad \forall x, y \in E$$

ohne Beweis

Sprechweisen:

- $x, y \in E$ heißen <u>orthogonal</u>, falls $\langle x, y \rangle = 0$.
  Es gilt dann: $\|x+y\|^2 = \|x\|^2 + \|y\|^2$

- Eine Familie $(e_i)_{i \in I}$ heißt <u>orthonormal</u>, falls

$$\|e_i\| = 1, \ \forall i \in I \quad \text{und} \quad \langle e_i, e_j \rangle = 0, \ \forall i \neq j.$$

Für $x = \sum_{i \in I} x_i e_i$, $y = \sum_{i \in I} y_i e_i$ gilt:

$$\langle x, y \rangle = \sum_{i \in I} \overline{x_i} y_i, \quad \|x\| = \sum_{i \in I} |x_i|^2$$

<u>Satz:</u> Sei E ein Prähilbertraum und $F \subseteq E$ ein Unterraum.

a) Dann gibt es zu $x \in E$ höchstens ein $p_F(x) \in F$, so daß

$$\langle x - p_F(x), y \rangle = 0, \ \forall y \in F$$

b) Falls $\dim(F) < \infty$, so ist p_F überall definiert.

<u>Def.:</u> p_F nennt man die <u>orthogonale Projektion</u> auf F.

Beweis:

a) Es gelte $\langle x - y_1, y \rangle = 0 = \langle x - y_2, y \rangle$ für alle $y \in F$. Z.z. $y_1 = y_2$

Dann: $y_1 - y_2 = (x - y_2) - (x - y_1)$

$\Rightarrow \langle y_1 - y_2, y \rangle = 0, \forall y \in F$

$\Rightarrow \langle y_1 - y_2, y_1 - y_2 \rangle = 0 \Rightarrow y_1 = y_2$

b) Sei $e_1, \dots, e_d$ eine ON-Basis von F (berechenbar mit Orthogonalisierungsverfahren von Schmidt) Dann definieren wir:

$$p_F(x) := \sum_{i=1}^{d} \langle e_i, x \rangle e_i$$

Z.z. $\langle x - p_F(x), y \rangle = 0, \forall y \in F$.

Sei $y = \sum_{i=1}^{d} \lambda_i e_i \Rightarrow \langle e_j, y \rangle = \lambda_j$

Also ist jedes $y \in F$ von der Form

$$y = \sum_{j=1}^{d} \langle e_j, y \rangle e_j \qquad (*)$$

Es folgt:

$$\langle e_j, x - p_F(x) \rangle = \langle e_j, x \rangle - \sum_{i=1}^{d} \langle e_i, x \rangle \langle e_j, e_i \rangle$$

$$= 0$$

$\overset{(*)}{\Longrightarrow} \langle y, x - p_F(x) \rangle = 0, \quad \forall y \in F$

Bemerkungen: $p_F : E \to F$ ist linear

$p_F(x) = x, \quad \forall x \in F$

$p_F^2 = p_F$

Satz: Sei $(f_i)_{i \in I}$ eine linear unabhängige Familie von Vektoren in E und I abzählbar. Dann kann man mit dem Schmidt'schen ON-Verfahren eine ON-Basis von $F = \mathrm{Lin}(f_i)_{i \in I}$ konstruieren.

Satz: Sei $\dim(E) = n < \infty$ und $e_1, \dots, e_n$ eine ON-Basis. Dann gilt für alle $x, y \in E$:

$$x = \sum_{i=1}^{n} \langle e_i, x \rangle e_i$$

und $$\langle x, y \rangle = \sum_{i=1}^{n} \overline{\langle e_i, x \rangle} \langle e_i, y \rangle.$$

Mit anderen Worten

$$K^n \xrightarrow{\sim} E, \quad z \longmapsto \sum_{i=1}^{n} z_i e_i$$

ist kompatibel mit dem Skalarprodukt.

Beweis:

$$\left\langle \sum_i z_i e_i, \sum_i \tilde{z}_i e_i \right\rangle = \sum_{i,j} \overline{z_i} \tilde{z}_j \langle e_i, e_j \rangle$$

$$= \sum_{i=1}^{n} \overline{z_i}\, \tilde{z}_i$$

Unitäre Endomorphismen

Motivation:

Quantenmechanische Systeme $\longleftrightarrow$ H Hilbertraum

zeitliche Entwicklung $\longleftrightarrow$ unitäre Operatoren

Observable (= physikalische Meßgrößen) $\longleftrightarrow$ selbstadjungierte Operatoren

Zustand des Systems $\longleftrightarrow$ Dichteoperatoren

$\varrho : H \to H$

$\varrho^* = \varrho,\ \varrho \geq 0$

$\mathrm{Tr}(\varrho) = 1$

Definition: $u \in \mathrm{End}(E)$ heißt *unitär*, falls

$$\langle u(x), u(y) \rangle = \langle x, y \rangle, \quad \forall x, y \in E$$

Lemma: u unitär $\iff \|u(x)\| = \|x\|, \ \forall x \in E$

Beweis: $\Rightarrow$ $\|u(x)\|^2 = \langle u(x), u(x) \rangle = \langle x, x \rangle = \|x\|^2$

$\Leftarrow$ $\|u(x) + u(y)\|^2 - \|u(x)\| - \|u(y)\|$

$$= \|x + y\|^2 - \|x\| - \|y\|$$

Beweise ebenfalls:

$$\|x+y\|^2 = \langle x+y, x+y\rangle$$
$$= \|x\|^2 + \|y\|^2 + 2\,\mathrm{Re}\left(\langle x, y\rangle\right)$$

Also folgt: $\mathrm{Re}\left(\langle u(x), u(y)\right) = \mathrm{Re}\left(\langle x, y\rangle\right)$.

Ersetze das Paar x, y durch ix, y. Dann folgt:

$$\mathrm{Re}\left(\langle u(ix), u(y)\rangle\right) = \mathrm{Re}\left(\langle ix, y\rangle\right)$$

$$\mathrm{Re}\left(\tfrac{1}{i}\langle u(x), u(y)\rangle\right) \qquad \| \qquad \mathrm{Im}\left(\langle x, y\rangle\right).$$

$$\| \qquad\qquad\qquad\qquad$$

$$\mathrm{Im}\left(\langle u(x), u(y)\rangle\right)$$

∎

Satz: Sei $E / \mathbb{C}$ von endlicher Dimension und $u \in \mathrm{End}(E)$ unitär. Dann gibt es eine ON-Basis von E bez. der u Diagonalgestalt hat. Die EW (= Diagonalelemente) haben Betrag 1.

Beweisskizze: Sei $u(x) = \lambda x$ mit $x \neq 0$.

$$\Longrightarrow \quad \|\lambda x\| = \|u(x)\| = \|x\|$$

$$\| \qquad\qquad \Longrightarrow |\lambda| = 1.$$

$$|\lambda|\,\|x\|$$

Die Diagonalisierbarkeit folgt mittels Induktion $n = \dim(E)$.

$n=1$: ✓

$n \geq 2$: u hat EW λ_1, da $\dim(E) < \infty$ und $E/\mathbb{C}$ algebraisch abgeschlossen

Sei $e_1 \in E$ ein EV zu λ_1 und

$$F := (\mathbb{C}e_1)^\perp$$

Dann zeigt man leicht: $u_F = u|_F : F \to F$

$u_F : F \to F$ unitär.

Wende Induktion an ▨

Def.: Eine Matrix $P = (a_{ij}) \in M_n(K)$ heißt unitär, falls $\overline{P}^t P = E_n$. Falls $P \in M_n(\mathbb{R})$ nennt man P auch orthogonal.

Satz: FASÄ:

a) P ist unitär

b) Die Spalten von P sind eine ON-Basis des K^n

c) $-"-$ Zeilen $-"-$ $-"-$

Satz: a) P unitär $\Rightarrow$ $\mu_P : K^n \to K^n$
$x \mapsto Px$
ist unitär

b) Sei $\dim(E) = n < \infty$, $\mu : E \to E$ unitär
$\Rightarrow$ die darstellende Matrix bez. einer ON-Basis ist unitär.