Eigenes „Gesamtbild" CRYPTO1 – Post-Quanten-Algo

27.8.22

(GGH war CVP!)

NTRU (Encrypt) ≙ SVP!

(beide Gitter-basiert:) ≈ GGH/CVP

↳ „rausgeflogen"

↳ =NIST!

(z.B. N=1087) = „n-th truncated polynomial ring"

- Polynomring $R = \mathbb{Z}[x]/\langle x^N - 1\rangle$; $N \in \mathbb{P}$ (groß)
  ↳ d.h. $x^N - 1 = 0 \Rightarrow x^N = 1$, $x^{N+1} = x$, usw.
  (d.h. Grad übersteigt nie N)
- Bruder #1: $R_p = \mathbb{Z}_p[x]/\langle x^N - 1\rangle$; $p \in \mathbb{P}$ (klein)
  (z.B. p=3) ↳ d.h. Koeff. noch mod p, ansonsten dasselbe
- Bruder #2: $R_q = \mathbb{Z}_q[x]/\langle x^N - 1\rangle$; $N \nmid q$, $p \nmid q$
  (z.B. q=2^11) (Wiki: q=2048)
- d_1 sodass $p(6d+1) < q$ (*)
- $T(a,b) := \{ f \in R \mid$ a Koeff. von $f = 1$, b Koeff. von $f = -1$, $N-a-b$ Koeff. v. $f = 0 \}$

de.wiki erst im Abschnitt „Effizienz"!

KeyGen:

π = Projektion

- $f \in_R T(d+1, d)$ ternäres Polynom (geheim)
- $g \in_R T(d, d)$ ternäres Polynom (Ephemeral: geh.+vergessen)
- Dabei muss $\pi_p(f)$ in R_p und $\pi_q(f)$ in R_q invertierbar sein, sonst generiere f neu!
  ⇒ $f_p := \pi_p(f)^{-1} \in R_p$, d.h. $f \cdot f_p \equiv 1 \pmod p$
  ⇒ $f_q := \pi_q(f)^{-1} \in R_q$, d.h. $f \cdot f_q \equiv 1 \pmod q$
- Öffentl. Schlüssel: $h = f_q \cdot \pi_q(g) \in R_q$ („verschleiern")
- Privaten Schlüssel: (f, f_p) (f_p nur damit schneller) ↳ Wiki: $h \equiv f_q \cdot g \pmod q$

Encrypt:

- Nachricht $m \in \lambda_p(R_p) \subseteq R$ Polynom
  ↳ $\lambda_p : \mathbb{Z}_p \to \mathbb{Z}$, $\{\dots, a-2p, a-p, a, a+p, a+2p, \dots\} \mapsto \xi \in [-\frac{p}{2}, \frac{p}{2})$ „symmetr. Vertreter" ($\in [0,p)$)
  ↳ $\lambda_p : R_p \to R$ koeffizientenweise
- Ternäres Polynom $r \in_R T(d,d) \subseteq R$
- Ciphertext: $c = p \cdot \pi_q(r) \cdot h + \pi_q(m) \pmod q$

Decrypt:

- $a = \pi_q(f) \cdot c \in R_q \pmod q$
- $m' = \pi_p(\lambda_q(a)) \cdot f_p \in R_p \pmod p$
- $m = \lambda_p(m') \in \lambda_p(R_p) \subseteq R$

Korrektheit:

- $a = \pi_q(f) \cdot c$
  $= \pi_q(f) \cdot [p \cdot \pi_q(r) \cdot h + \pi_q(m)]$
  $= p \cdot \pi_q(r) \cdot \pi_q(f) \cdot f_q \cdot \pi_q(g) + \pi_q(f) \cdot \pi_q(m)$
  $= p \cdot \pi_q(r) \cdot 1 \cdot \pi_q(g) + \pi_q(f) \cdot \pi_q(m)$
  $= \pi_q(p \cdot r \cdot g + f \cdot m)$
  ↳ da π_q eine strukturerhaltende Abb.
  ⇒ $\lambda_q(a) = p \cdot r \cdot g + f \cdot m$ (wegen (*))
- $m' = \pi_p(\lambda_q(a)) \cdot f_p$
  $= \pi_p(p \cdot r \cdot g + f \cdot m) \cdot f_p$
  $= \pi_p(f \cdot m) \cdot f_p$ (da mod p)
  $= \pi_p(f) \cdot \pi_p(m) \cdot f_p$
  $= \pi_p(m)$ (da $f_p := \pi_p(f)^{-1}$)
  ⇒ $\lambda_p(m') = \lambda_p(\pi_p(m)) = m$, $m \in \lambda_p(R_p)$

Wo Gitter?:

- Ring R = Polynome mit Grad $\le N-1$ $\leftrightarrow \mathbb{Z}^N$ (Gitter)
- NTRU-Angriff: aus $h \equiv f_q \cdot g$ f und g berechnen
- SVP-Angriff:

$$(f, u) \cdot \begin{bmatrix} I_N & C_h \\ 0 & q \cdot I_N \end{bmatrix} = (f, g) \in L^{NTRU}$$

Das L^{NTRU}-Gitter. — klein! ⇒ finde durch Lösen von SVP in L^{NTRU}

C_h = die zyklische Rotation von h
I_N = $N \times N$ – Einheitsmatrix

BRUNNEN

Kyber / VL auch: „CRYSTAL-KYBER"

- rechnet im Ring $R = \mathbb{Z}_q[x]/\langle x^d + 1\rangle$
  ↳ $q = 7681 \in \mathbb{P}$, $d = 256$
  ⇒ rechne mod q, d.h. im Kreis: $0 \to [\frac{q}{2}]$
- Rundungsfunktion round: $0 \to [\frac{q}{2}]$
- Lernen (im Sinne von „in Erfahrung bringen") with Errors: Geg.: $b = sA + err$; $b \approx s \cdot A \pmod q$
  Aufgabe: Finde s.

KeyGen:

- Wähle zufällige Matrix $A \in_R R^{n \times n}$
- Wähle $s, e \leftarrow \chi^n$ mit χ einen um 0 zentr. Verteilung
- $t = As + e$
- Öffentl. Schlüssel: (A, t)
  Privater Schlüssel: s

Encrypt:

- Nachricht $m \in R$ Ringelement
- $r, e \leftarrow \chi^n$ Zufallsvektoren
- $f \leftarrow \chi$ Zufallselement
- $u = r \cdot A + e$
- $v = r \cdot t + f + \lfloor \frac{q}{2} \rfloor \cdot m$
- Ciphertext: $c = (u, v)$

Decrypt:

- $w = v - u \cdot s$
- $m = \frac{\text{round}(w)}{\lfloor q/2 \rfloor}$

Korrektheit:

- $w = v - u \cdot s$
  $= (r \cdot t + f + \lfloor \frac{q}{2} \rfloor \cdot m) - (r \cdot A + e) \cdot s$
  $= r \cdot t + f + \lfloor \frac{q}{2} \rfloor \cdot m - r \cdot A \cdot s - e \cdot s$
  $\approx f + \lfloor \frac{q}{2} \rfloor \cdot m - e \cdot s$
  $\approx$ klein $+ \lfloor q/2 \rfloor \cdot m$ (klein)

round → bekomme genau $\lfloor q/2 \rfloor \cdot m$
$\div \lfloor q/2 \rfloor$ → m. ∎

NTRU „kurz & knackig" (de.wiki):

KeyGen: 1. Wahl N, p, q mit $q > p$, $ggT(p,q) = 1$
2. zuf. inv. Polyn. f mit Koeff. in $\{0, \pm 1\}$ (f_q = das Inverse von f modulo q)
3. zuf. Polyn. g mit Koeff. in $\{0, \pm 1\}$
4. $h \equiv f_q \cdot g \pmod q$ öff.; f geheim

Enc: 1. Umwandlung Klartext in Polynom m
2. zuf. Polyn. r mit kleinen Koeff.
3. $e \equiv pr \cdot h + m \pmod q$ Geheimtext

Dec: 1. $a \equiv f \cdot e \pmod q$ (Koeff. v. a in $(-\frac{q}{2}, \frac{q}{2})$ wählen)
2. $c \equiv f_p \cdot a \pmod p$ ⇒ Klartext

Korr.: $a \equiv f \cdot e \equiv f \cdot pr \cdot h + f \cdot m \equiv f \cdot pr \cdot f_q \cdot g + f \cdot m$
$\equiv pr \cdot g + f \cdot m \pmod q$; $c \equiv f_p \cdot pr \cdot g + f_p \cdot f \cdot m \equiv m \pmod p$