Mriežky a kryptoanalýza

Martin Stanek

2025

KI FMFI UK Bratislava

Úvod

- minulá prednáška – kryptoanalýza knapsack schémy
  - formulácia kryptoanalýzy ako problému na vhodnej mriežke (SVP)
- **cieľ**: ukázať niektoré kryptoanalytické úlohy, ktoré možno formulovať ako problémy na mriežkach
- náplň:
  - LWE
  - pevná výplň v „učebnicovej“ verzii RSA
  - faktorizácia pri čiastočnej znalosti deliteľa
  - krátky súkromný exponent v RSA
  - problém skrytého čísla (hidden number problem)
  - (EC)DSA a nevhodný parameter pri podpisovaní

LLL ako čierna skrinka

- deterministický polynomiálny algoritmus
  - A. Lenstra, H. Lenstra, L. Lovász
- vstup: báza mriežky L (označme n dimenziu mriežky)
- výstup: LLL-redukovaná báza $\{b_1, \ldots, b_n\}$:
  - $\|b_i\| \leq 2^{(n-1)/2} \cdot \lambda_i$
  - pripomeňme, že λ_i je i-te minimum L
  - vždy, teda aj v najhoršom prípade
- v praxi obvykle lepšie výsledky (menší aproximačný faktor)
  - v priemernom prípade, pre náhodné mriežky (experimentálne) $\|b_1\| \leq 1{,}02^n \cdot \lambda_1$
- existujú aj iné redukčné algoritmy, napr. BKZ a ich varianty
  - BKZ: vyššia zložitosť, lepšia báza (kratšie vektory, „ortogonálnejšia“)

LWE inštancia

- q – prvočíslo pre $\mathbb{Z}_q$
- n – dimenzia, m – počet rovníc
- $\boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$ (m riadkov)
- $s \in_R \mathbb{Z}_q^n$ (častokrát malý vektor)
- e – náhodný malý vektor (vhodná distribúcia)

$$b = \boldsymbol{A} \cdot s^\mathsf{T} + e^\mathsf{T}$$

- LWE: pre dané $\boldsymbol{A}$, b vypočítať s
- poznámka: stĺpcové vektory

Vloženie LWE do mriežky

- budeme chcieť $\mathbb{Z}$ namiesto $\mathbb{Z}_q$:
  - $b = \boldsymbol{A} \cdot s^\mathsf{T} + e^\mathsf{T} - q \cdot k^\mathsf{T}$, pre $k \in \mathbb{Z}^m$
- uvažujme mriežku danú nasledujúcou maticou (báza sú riadky):

$$\boldsymbol{B} = \begin{pmatrix} q\boldsymbol{I}_m & \boldsymbol{0} & \boldsymbol{0} \\ -\boldsymbol{A}^\mathsf{T} & \boldsymbol{I}_n & \boldsymbol{0} \\ b^\mathsf{T} & \boldsymbol{0} & 1 \end{pmatrix}$$

- $\boldsymbol{B}$ je štvorcová matica s $m + n + 1$ riadkami a stĺpcami; plná hodnosť
- počítajme $(k, s, 1) \cdot \boldsymbol{B}$

Krátky vektor v mriežke $\boldsymbol{B}$

$$(k, s, 1) \cdot \boldsymbol{B} = (k, s, 1) \cdot \begin{pmatrix} q\boldsymbol{I}_m & \mathbf{0} & \mathbf{0} \\ -\boldsymbol{A}^\mathsf{T} & \boldsymbol{I}_n & \mathbf{0} \\ b^\mathsf{T} & \mathbf{0} & 1 \end{pmatrix} = (e, s, 1)$$

- prvých m stĺpcov: $q \cdot k - s \cdot \boldsymbol{A}^\mathsf{T} + b^\mathsf{T} = e$, preusporiadané a transponované
- ďalších n stĺpcov: s (triviálne)
- posledný stĺpec: 1 (triviálne)
- $(e, s, 1)$ je krátky vektor v mriežke, skúsme ho nájsť (demo)
  - pre náhodné $s \in \mathbb{Z}_q^n$ s veľkým q a rozumným počtom rovníc m budú existovať aj kratšie vektory $\Rightarrow$ LLL nenájde správne riešenie
  - pre malé s útok funguje lepšie, zvyšujúce sa n ho opäť pokazí

RSA

- $n = p \cdot q$ – súčin dvoch veľkých prvočísel
- e, d – verejný a súkromný exponent
  - $ed \equiv 1 \pmod{(p-1)(q-1)}$
- verejná/súkromná transformácia na $\mathbb{Z}_n$:
  - $m \mapsto m^e \bmod n$
  - $c \mapsto c^d \bmod n$
- optimalizácia e – rýchlosť šifrovania
  - $e = 3$ – najmenšie možné
  - $e = 2^{16} + 1 = 65537$ – najčastejšie využívané v praxi

Malé e a krátka správa

- učebnicová verzia s malým $e = 3$ (napr.)
- známy problém pre správu $m < n^{1/3}$
  - povedzme m ako symetrický kľúč
  - $m^3 < n \;\Rightarrow\; c = m^3$ (bez mod n)
  - m je možné ľahko vypočítať $m = c^{1/3}$
- možné riešenie – pridať výplň
  - správa m dĺžky l bitov, teda $m < 2^l$
  - statická výplň $a = v \cdot 2^l$ (fixne zvolené a pre všetky m)
  - $c = (a + m)^3 \bmod n$

Útok na fixnú výplň

- uvažujme polynóm $f(x) = (a + x)^3 - c$
  - $f(x) = (a + x)^3 - c = x^3 + 3ax^2 + 3a^2x + \left(a^3 - c\right)$ (poznáme koeficienty f)
- m je *malý* ($m < 2^l = R$) koreň polynómu $f(x)$, počítajúc mod n
- budeme konštruovať polynóm $g(x) \in \mathbb{Z}[x]$, ktorý má tiež koreň m, teraz však nad $\mathbb{Z}$
  - hľadať korene v $\mathbb{Z}$ vieme efektívne

Hľadanie polynómu g

1. zabezpečíme, že $g(m) \equiv 0 \pmod{n}$ nasledovným tvarom polynómu:

$$g(x) = c_3 f(x) + c_2 n x^2 + c_1 n x + c_0 n$$

2. nájdeme g: $|g(m)| < n$, aby nebolo potrebné pre $g(m)$ počítať mod n

$$\begin{aligned} |g(m)| &= |g_3 m^3 + g_2 m^2 + g_1 m + g_0| \\ &< |g_3| R^3 + |g_2| R^2 + |g_1| R + |g_0| < n \qquad (\star) \end{aligned}$$

... teda potrebujeme nájsť malé koeficienty g_i

(1), (2) $\Rightarrow g(m) = 0$, lebo mod n sa neuplatní

Hľadanie koeficientov

$$\left.\begin{aligned} & c_3 \cdot \left(x^3 + 3ax^2 + 3a^2x + \left(a^3 - c\right)\right) \\ + & c_2 \cdot \left(\quad nx^2 \quad \right) \\ + & c_1 \cdot \left(\quad nx \quad \right) \\ + & c_0 \cdot \left(\quad n \right) \end{aligned}\right\} \; g_3x^3 + g_2x^2 + g_1x + g_0$$

- nezáleží nám na hodnotách $c_0, \ldots, c_3$, avšak chceme platnosť $(\star)$
- l_1 norma vs. l_2 norma:
  - $\|v\|_1 = |v_1| + |v_2| + \ldots + |v_n|$
  - $\|v\|_2 = \left(v_1^2 + v_2^2 + \ldots + v_n^2\right)^{1/2}$
  - použijeme Cauchyho-Schwarzovu nerovnosť: $|\langle v, u\rangle| \leq \|v\|_2 \cdot \|u\|_2$
  - dostaneme: $\|v\|_1 = \langle(|v_1|, \ldots, |v_n|), \mathbf{1}\rangle \leq \|v\|_2 \cdot \|\mathbf{1}\|_2 \leq \sqrt{n} \cdot \|v\|_2$

Mriežka pre nájdenie koreňa v $\mathbb{Z}$

– hľadáme krátky vektor v celočíselnej mriežke, pričom vektory bázy škálujeme tak, aby najkratší vektor minimalizoval ($\star$)

$$(c_3, c_2, c_1, c_0) \cdot \begin{pmatrix} R^3 & 3aR^2 & 3a^2R & a^3 - c \\ 0 & nR^2 & 0 & 0 \\ 0 & 0 & nR & 0 \\ 0 & 0 & 0 & n \end{pmatrix} = \begin{pmatrix} c_3R^3 \\ c_3aR^2 + c_2nR^2 \\ c_3a^2R + c_1nR \\ c_3(a^3 - c) + c_0n \end{pmatrix}^{\mathsf{T}}$$

– použijeme LLL a následne pre nájdený najkratší vektor po odstránení R faktorov hľadáme koreň v $\mathbb{Z}$ (demo)

– m nemôže byť veľmi dlhé

Poznámky

- zovšeobecnený tvar $g(x)$
  - $g(x) = s(x)f(x) + nt(x)$, pre nejaké $s, t \in \mathbb{Z}[x]$
  - m je stále koreň g počítajúc mod n
  - potenciál pre krátky vektor na dosiahnutie $|g(m)| < n$ (iná mriežka)
- hranica pre m je $n^{1/e}$ (Coppersmith)
  - využitie vyšších mocnín $f^2(x)$, … a n^2, …
  - výber vhodných polynómov do bázy mriežky
  - pripustenie polynómov vyšších stupňov
- potrebná analýza – dĺžka správy, aproximácia SVP pomocou LLL, …

Faktorizácia pri čiastočnej znalosti deliteľa

- RSA: $n = p \cdot q$ a nech $p > q$, teda $p > n^{1/2}$
- predpokladajme, že poznáme väčšiu časť prvočísla p
  - znalosť najvýznamnejších bitov, označme a
  - špeciálna konštrukcia p, chybný RNG a pod.
- nepoznáme posledných l bitov p, teda $p = a + m$, kde neznáme $m < 2^l = R$
- m je koreň polynómu $f(x) = x + a$, počítajúc mod p
  - m je koreň (mod p) aj ľubovoľnej celočíselnej lineárnej kombinácie $g(x) = c_2 f^2(x) + c_1 f(x) + c_0 n$
- chceme nájsť vhodnú lin. komb., v ktorej budú koeficienty $g(x)$ malé
  - $|g(x)| = |g_2 x^2 + g_1 x + g_0| < |g_2|\, R^2 + |g_1|\, R + |g_0|$
  - ak $|g(m)| < p$, tak m je koreňom $g(x)$ nad $\mathbb{Z}$ a vieme ho efektívne nájsť

- analogicky ako v predchádzajúcom prípade, teraz:

$$g(x) = c_2 f^2(x) + c_1 f(x) + c_0 n = c_2(a+x)^2 + c_1(a+x) + c_0 n$$
$$= x^2(c_2) + x(2c_2 a + c_1) + \left(c_2 a^2 + c_1 a + c_0 n\right)$$

- v maticovom tvare (báza mriežky sú škálované koeficienty polynómov, ktoré kombinujeme):

$$(c_2, c_1, c_0) \cdot \begin{pmatrix} R^2 & 2aR & a^2 \\ 0 & R & a \\ 0 & 0 & n \end{pmatrix} = \begin{pmatrix} c_2 R^2 \\ 2c_2 aR + c_1 R \\ c_2 a^2 + c_1 a + c_0 n \end{pmatrix}^{\mathrm{T}}$$

Poznámky

- riešenie SVP (LLL) a následne, po odstránení R-faktorov hľadanie koreňa (demo)
- takáto mriežka uspeje pre $|m| < n^{1/6}$
  - teda cca. $1/3$ bitov p je neznámych
  - lepší postup uspeje pre cca. $1/2$ neznámych bitov p

Krátky súkromný exponent v RSA

- v RSA skúsime zvoliť najskôr relatívne krátke d a následne dopočítame e
  - rýchlejšia súkromná transformácia (dešifrovanie, podpisovanie)
- Wiener: efektívna rekonštrukcia d, ak $d < \frac{1}{3}n^{1/4}$
  - originálne použité reťazové zlomky
  - alternatívne je možné sformulovať útok na mriežkach
- Boneh, Durfee: efektívna rekonštrukcia d, ak $d < n^{0,292}$
  - využívané mriežky

Útok na krátke d

$$ed \equiv 1 \pmod{\overbrace{(p-1)(q-1)}^{\varphi(n)}} \quad \Rightarrow \quad ed = 1 + k(p-1)(q-1)$$

$$ed = 1 + k(n + 1 - (p+q)) \quad \text{označme } s = p + q$$

$$\underline{ks} + e\underline{d} - 1 \equiv 0 \pmod{(n+1)}$$

- $s = (p+q) \approx \sqrt{n}$
- $k \leq d$, lebo $k\varphi(n) = ed - 1$ a $e < \varphi(n)$ (obykle), teda $k\varphi(n) < ed < \varphi(n)d$

Polynóm s predpísanými koreňmi

- uvažujme polynóm $f(x, y) = x + ey - 1$
- $x = ks, y = d$ sú riešením $f(x, y) \equiv 0 \pmod{(n+1)}$
- ak $d < n^{1/4}$, tak vieme ohraničiť riešenia takto: $x < n^{3/4} = X$ a $y < n^{1/4} = Y$
- hľadáme vhodnú lineárnu kombináciu polynómov $f(x, y)$, $y(n+1)$ a $n+1$:

$$g(x, y) = c_2 \cdot f(x, y) + c_1 \cdot y(n+1) + c_0(n+1)$$

  - korene/riešenia mod $(n+1)$ sú zachované, chceme však aj nad $\mathbb{Z}$

$$|g(x, y)| = |g_2 x + g_1 y + g_0| < |g_2|\, X + |g_1|\, Y + |g_0| < n + 1$$

  - teda potrebujeme čo najmenšie koeficienty

Iný pohľad

- $h(x, y) = -dx + (ks - 1)y + d$ má rovnaké korene a malé koeficienty
  - je vhodnou lineárnou kombináciou $f(x, y)$, $y(n + 1)$ a $n + 1$:

$$h(x, y) = c_2(x + ey - 1) + c_1 y(n + 1) - c_0(n + 1) \quad \Rightarrow c_2 = -d$$

$$h(x, y) = -dx + y(-ed + c_1(n + 1)) + d + c_0(n + 1)$$

$$= -dx + y(ks - 1 + l(n + 1) + c_1(n + 1)) + d + c_0(n + 1) \quad \Rightarrow c_1 = -l$$

$$h(x, y) = -dx + y(ks - 1) + d + c_0(n + 1) \quad \Rightarrow c_0 = 0$$

- ak nájdeme h, nemusíme hľadať korene, koeficienty prezradia d
- škálujeme stĺpce tak, aby najkratší vektor mriežky bol dlhý cca. ako želeané riešenie

Mriežka pre útok na krátke d

- vytvoríme mriežku, bázy zodpovedajú kombinovaným polynómom
- škálované na minimalizáciu $|g(x, y)|$
- hľadáme najkratší vektor (malé koeficienty) pomocou LLL

$$(c_2, c_1, c_0) \cdot \begin{pmatrix} X & eY & -1 \\ 0 & Y(n+1) & 0 \\ 0 & 0 & n+1 \end{pmatrix} = \begin{pmatrix} c_2 X \\ 2c_2 eY + c_1 Y(n+1) \\ -c_2 + c_0(n+1) \end{pmatrix}^{\mathsf{T}}$$

- nech (a_2, a_1, a_0) je nájdený najkratší vektor
- očakávame $d = |a_2|/X$, resp. $d = |a_0|$ (demo)
- analýza, pre aké dĺžky to funguje, je náročnejšia

Iná mriežka

- polynóm $f^*(x, y) = x + ey$
  - $x = ks - 1$ a $y = d$ sú korene mod $(n + 1)$
  - kombinujeme polynómy $f^*(x, y)$ a $y(n + 1)$
  - *krátka* kombinácia s rovnakými koreňmi je $-dx + (ks - 1)y$
  - mriežka:

$$\begin{pmatrix} X & eY \\ 0 & Y(n+1) \end{pmatrix}$$

  - pre nájdený najkratší vektor (a_1, a_0) očakávame $d = |a_1|/X$ (demo)

Problém skrytého čísla (hidden number problem)

- aplikácie v útokoch na niektoré kryptografické konštrukcie
  - čiastočná znalosť parametrov schém
  - typicky: parameter volený pri podpisovaní v DSA, resp. ECDSA schémach – rekonštrukcia súkromného kľúča

Hidden Number Problem (HNP)

- verejné n, tajné α
- čiastočné informácie o hodnote α v tvare (t_i, a_i), kde
  - t_i je náhodné číslo $0 < t_i < n$ (rovnomerná distribúcia)
  - a_i zodpovedá niekoľkým najvýznamnejším bitom $t_i\alpha \bmod n$
- úloha: nájsť α
- viacero variantov, zovšeobecnení aj prístupov k riešeniu

Riešenie HNP pomocou mriežok (CVP)

- informáciu (t_i, a_i) o α vieme vyjadriť: $t_i\alpha \bmod n = a_i + r_i$
  - teda $\underline{r_i} + a_i - t_i\underline{\alpha} \equiv 0 \pmod{n}$
  - r_i je malé v porovnaní s n, povedzme $|r| < R$

$$\begin{pmatrix} n & 0 & \dots & 0 \\ 0 & n & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & n \\ t_1 & t_2 & \dots & t_m \end{pmatrix}$$

- uvažujme sadu $m + 1$ vektorov (riadky)
- vektor $(t_1\alpha \bmod n, \dots, t_n\alpha \bmod n)$, teda $(a_1 + r_1, \dots, a_n + r_n)$ je ich celočíselnou lineárnou kombináciou

Riešenie HNP pomocou mriežok (CVP) - pokr.

$$\begin{pmatrix} n & 0 & \dots & 0 & 0 \\ 0 & n & \dots & 0 & 0 \\ & & \ddots & & \\ 0 & 0 & \dots & n & 0 \\ t_1 & t_2 & \dots & t_m & \frac{1}{n} \end{pmatrix}$$

- pridaním stĺpca dostaneme bázu mriežky
- $(t_1\alpha \bmod n, \dots, t_m\alpha \bmod n, \alpha/n)$ je bod mriežky
- riešime CVP pre vektor $(a_1, \dots, a_m, 0)$
- Babaiov algoritmus (Babai's nearest plane algorithm)

Poznámka (označme $\boldsymbol{M}$ horeuvedenú maticu mriežky):

- keďže $(-t_1, \dots, -t_m, n) \cdot \boldsymbol{M} = (0, \dots, 0, 1)$, má mriežka aj takýto krátky vektor

– pripomeňme: $\underline{r_i} + a_i - t_i\underline{\alpha} \equiv 0 \pmod{n}$, kde r_i je malé, povedzme $|r| < R$

$$\begin{pmatrix} n & 0 & \dots & 0 & 0 & 0 \\ 0 & n & \dots & 0 & 0 & 0 \\ & & \ddots & & & \\ 0 & 0 & \dots & n & 0 & 0 \\ t_1 & t_2 & \dots & t_m & R/n & 0 \\ -a_1 & -a_2 & \dots & -a_m & 0 & -R \end{pmatrix}$$

– najkratší vektor mriežky $\boldsymbol{M}^*$: $(0, \dots, 0, R, 0)$, získaný lineárnou kombináciou $(-t_1, \dots, -t_m, n, 0) \cdot \boldsymbol{M}^*$

– vektor $\left(r_1, r_2, \dots, r_m, \alpha\frac{R}{n}, -R\right)$ je krátkym vektorom z mriežky

– druhý (nezávislý) najkratší vektor?

– lepšie: chceme krátky vektor s nenulovou poslednou súradnicou (demo)

ECDSA a nevhodný parameter pri podpisovaní

- G bod eliptickej krivky – generátor podgrupy prvočíselného rádu n
- súkromný kľúč: $d \in_R \mathbb{Z}_n^*$; verejný kľúč: $Q = dG$ a iné parametre (krivka)
- podpis (zjednodušene) $\mathrm{Sig}_d(m) = (r, s)$
  - $r = (kG)_x \bmod n$, kde $k \in_R \mathbb{Z}_n^*$
  - $s = k^{-1}(h + dr) \bmod n$, kde $h = H(m)$
- vieme, že znalosť k umožní získať súkromný kľúč z podpisu
  - $d = r^{-1}(sk - h) \bmod n$
- predpokladajme čiastočnú znalosť k z viacerých podpisov
  - napr. implementácia generuje krátke k, útoky postrannými kanálmi a pod.
  - WLOG môžeme predpokladať, že *horné* bity k sú 0 (teda k je krátke)

Prechod na HNP

– upravme podpisovú rovnicu:

$$s = k^{-1}(h + dr) \bmod n$$

$$k = s^{-1}(h + dr) \bmod n$$

$$\underbrace{-s^{-1}h}_{a_i} + k \equiv \underbrace{s^{-1}r}_{t_i} \cdot \underbrace{d}_{\alpha} \pmod{n}$$

... inštancia HNP