MI-PB-7

Algebraická kryptoanalýza – základní principy. Řešení polynomiálních rovnic, Gröbnerovy báze.

Algebraická kryptoanalýza

Převod problému prolomení kryptosystému na problém vyřešení **soustavy polynomiálních rovnic** nad konečným tělesem

Uplatnění: hlavně symetrická kryptografie

Princip:

- Ze specifických vlastností šifry odvodit soustavu polynomiáních rovnic nad konečným tělesem
- Aplikace postupu pro řešení soustavy, vyvození tajného klíče

Problém:
Řešení soustavy polynomiálních rovnic nad konečným tělesem: **NP-úplný** problém

Získání soustavy rovnic:

- Soustava nad $GF(2)$
- **Cíl:** Co nejnižší stupně polynomů v soustavě
  - Pokud pouze lineární rovnice $\Rightarrow$ GEM s kubickou složitostí

Řešení soustavy:

- AES: soustava 8000 rovnic s 1600 proměnnými
- Neexistuje efektivní algoritmus
- **Postupy řešení:**
  - **Guess-and-determine:** uhodnout hodnoty vhodných proměnných, zbytek soustavy dopočítat jednodušeji
  - **Linearizace:** výraz tvaru xy nahradit novou proměnnou z (po dopočítání nutná zkouška)
  - **Groebnerovy báze:** perspektivní

Groebnerovy báze

Ideál: Množina $I \subset k[x_1, ..., x_n]$ je ideál, pokud:

- $0 \in I$
- pokud $f, g \in I$, $f + g \in I$
- pokud $g \in I$ a $h \in k[x_1, ..., x_n]$, potom $hf \in I$

"Obal": Nechť $f_1, ..., f_s$ polynomy v $k[x_1, ..., x_n]$. Potom

$$< f_1, ..., f_s >= \left\{ \sum_{i=1}^{s} h_i f_i : h_1, ..., h_s \in k[x_1, ..., x_n] \right\}$$

$< f_1, ..., f_s >$ je ideál

Monomial ordering $>$ na $k[x_1, ..., x_n]$ je jakákoliv relace $>$ na $\mathbb{N}_0^n$, neboli jakákoliv relace nad množinou jednočlenů $x^\alpha, \alpha \in \mathbb{N}_0^n$, splňující:

- $>$ je totální (nebo lineární) uspořádání
- pokud $\alpha > \beta$ a $\gamma \in \mathbb{N}_0^n$, potom $\alpha + \gamma > \beta + \gamma$
- $>$ je dobře uspořádávající na $\mathbb{N}_0^n$ -- každá neprázdná podmnožina $\mathbb{N}_0^n$ má nejmenší prvek vzhledem k $>$

Lexokografické uspořádání:
$\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}_0^n$.
$\alpha >_{lex} \beta$, pokud v rozdílu $\alpha - \beta$ je nejlevější prvek kladný.
Platí $x^\alpha >_{lex} x^\beta$, pokud $\alpha >_{lex} \beta$

Graded lexikografické uspořádání:
$\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}_0^n$.
$\alpha >_{grlex} \beta$, pokud:

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \text{ nebo } |\alpha| = |\beta| \text{ a } \alpha >_{lex} \beta$$

(řazení podle celkového součtu, potom lexikografické řešení shod)

Příklad:
$(2, 3, 4) >_{lex} (2, 2, 6)$, protože $\alpha - \beta = (0, 1, -2)$

$\Rightarrow x^2y^3z^4 >_{lex} x^2y^2z^6$

Podoba Groebnerovy báze závisí na zvoleném uspořádání -- GRLEX je nejlepší z hlediska složitosti

Pokud $f = \sum_\alpha a_\alpha x^\alpha$ nenulový polynom nad $k[x_1, ..., x_n]$ a $>$ monomiální uspořádání:

- **Multidegree** f: $\text{multideg}(f) = \max(\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0)$
- **Leading coefficient** f: $\text{LC}(f) = a_{\text{multideg}(f)} \in k$
- **Leading monomial** f: $\text{LM}(f) = x^{\text{multideg}(f)}$ (s koeficientem 1)
- **Leading term** f: $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$

Příklad:
$f = 4xy^5 + 3x^2 + xyz^4$, $>$ lexikografické
$\text{multideg}(f) = (2, 0, 0)$
$\text{LC}(f) = 3$
$\text{LM}(f) = x^2$
$\text{LT}(f) = 3x^2$

Pokud $I \in k[x_1, ..., x_n]$ ideál jiný než $\{0\}$:

$$LT(I) = \{cx^\alpha | \exists f \in I : \text{LT}(f) = cx^\alpha\}$$

($\text{LT}(I)$ je množina leading termů prvků z I)

$\langle \text{LT}(I) \rangle$ je ideál generovaný prvky $\text{LT}(I)$

Groebnerova báze:
Konečná podmnožina $G = \{g_1, ..., g_t\}$ ideálu I je Groebnerova báze (nebo standardní báze), pokud

$$\langle \text{LT}(g_1), ..., \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle$$

Neformálně: $g_1, ..., g_t \in I$ je Groebnerova báze I, právě když leading term libovolného prvku I je dělitelný jedním z $\text{LT}(g_i)$

Vlastnosti GB:

- Každý ideál $I \in k[x_1, ..., x_n]$ jiný než $\{0\}$ má Groebnerovu bázi. Každá GB ideálu I je báze I
- Každý ideál $I \in k[x_1, ..., x_n]$ má konečnou generující množinu. Tj.: $I = \langle g_1, ..., g_t \rangle$ pro nějaká $g_1, ..., g_t \in I$

Afinní varieta definovaná polynomy $f_1, ..., f_m$:

$$V(f_1, ..., f_m) = \{(a_1, ..., a_n) \in k^n : f_i(a_1, ..., a_n) = 0 \forall 0 \leq i \leq m\}$$

- Pokud $f_1, ..., f_s$ a $g_1, ..., g_t$ jsou báze stejného ideálu nad $k[x_1, ..., x_n]$ tak, že $\langle f_1, ..., f_s \rangle = \langle g_1, ..., g_t \rangle$, platí $V(f_1, ..., f_s) = V(g_1, ..., g_t)$

Pokud $G = \{g_1, ..., g_t\}$ Groebnerova báze ideálu $I \subset k[x_1, .., x_n]$ a $f \in k[x_1, ..., x_n]$, potom $f \in I$ právě když zbytek po dělení f bází G je nula.
Zbytek se značí $\bar{f}^G$
(dělení polynomu ideálem: rozklad polynomu na $\alpha \cdot g_1 + \beta \cdot g_2 \cdot ... \cdot \gamma \cdot g_t$)

S-polynom:
$f, g \in k[x_1, ..., x_n]$ nenulové polynomy

- Pokud $\mathrm{multideg}(f) = \alpha$ a $\mathrm{multideg}(g) = \beta$, pak x^γ, kde $\gamma = (\gamma_1, ..., \gamma_n)$, kde $\gamma_i = \max(\alpha_i, \beta_i)$ je **nejmenší společný násobek $\mathrm{LM}(f)$ a $\mathrm{LM}(g)$**: $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$
- **S-polynom f a g:**

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$

- Příklad:
  $f = x^3y^2 - x^2y^3 + x$
  $g = 3x^4y + y^2$
  Potom $\mathrm{multideg}(f) = (3, 2), \mathrm{multideg}(g) = (4, 1)$
  $\Rightarrow \gamma = (4, 2)$

$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x \cdot f - (1/3) \cdot y \cdot g = -x^3y^3 + x^2 - (1/3)y^3$$

Buchbergerovo kritérium:
I ideál polynomů. Potom báze $G = \{g_1, ..., g_t\}$ v I je Groebnerova báze I, právě když pro všechny dvojice $i \neq j$ zbytek po dělení $S(g_i, g_j)$ bází G je nula
(Jednoduchý důkaz, že báze je GB. Vede k algotimu konstrukce GB pro ideál)

Buchbergerův algoritmus:
$I = \langle f_1, ..., f_s \rangle$ ideál polynomů

- **Vstup:** $F = (f_1, ..., f_s)$, *(nějaká báze I)*
- **Výstup:** Groebnerova báze $G = (g_1, ..., g_t)$ ideálu I, kde $\langle F \rangle = \langle G \rangle$

```
G = F
opakuj:
    G' = G
    pro každou dvojici p,q z G', kde p != q:
        S = zbytek po dělení S(p,q) množinou G'
        pokud S != 0:
            G = G sjednoceno {S}
dokud G == G'
```

GB v algebraické kryptoanalýze:

- Ze soustavy rovnic sestavit Groebnerovu bázi G Buchbergerovým algoritmem
- Soustava polynomiálních rovnic z G má stejnou množinu řešení jako původní soustava (řešení závisí pouze na generovaném ideálu -- **afinní variety** bází se rovnají)
- Řešení soustavy GB je jednodušší *(proměnné se "oddělí od sebe" -- místo členů typu $3x^2y^9z^7$ obsahují rovnice více členů s pouze jednou proměnnou -- matematicky **nepodloženo,** někde jsem to četl)*