Pokročilá kryptologie

Multivariační kryptografie

prof. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra informační bezpečnosti

Obsah přednášky

- Úvod
- Matematický základ
- Unbalanced Oil and Vinegar
- MC – útoky

Úvod - motivace

- Znovu: Kryptografické systémy veřejného klíče jsou založeny na těžce řešitelných matematických problémech
  - RSA je založené na problému faktorizace velkých čísel
  - DH a ElGamal na problému diskrétního logaritmu
  - Problém s příchodem kvantových počítačů: Shorův algoritmus ...
- Východisko – algoritmy post-kvantové kryptografie
- Další ze zástupců těchto algoritmů je Multivariační kryptografie (MC). (*Multivariate Cryptography*)
- MC má jednosměrnou funkci padacích vrátek v podobě vícerozměrné nelineární polynomické mapy na konečném tělese
- Nelineární je obvykle myšleno kvadratický. Pak jsou to MQ (*Multivariate Quadratic*) systémy

Matematický základ 1

MQ problém

Pro daných m kvadratických polynomů

$$p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)$$

s n proměnnými $\mathbf{x} = x_1, \ldots, x_n$ nad konečným tělesem $\mathbb{F}_q$,
najít vektor $\mathbf{x}'$ takový, že

$$p_1(\mathbf{x}') = \ldots = p_m(\mathbf{x}') = 0$$

.

Řešení MQ problému je NP-úplný problém a obecně je to dvojnásobně exponenciální složitost nad jakýmkoli konečným tělesem.

Matematický základ 2

$\mathbb{F} = \mathbb{F}(q)$ s q prvky:

$$p_1(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$p_2(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p_m(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

d – stupeň polynomů v systému rovnic
n – počet proměnných
m – počet rovnic

MC je velmi rychlý a vyžaduje pouze malé výpočetní zdroje, což ho činí atraktivním pro aplikace v levných zařízeních.

Příklad

$\mathbb{F}_2$

$$
\begin{aligned}
y_1 &= x_1x_2 + x_1x_3 + x_2x_4 + x_2x_5 + x_4x_5 + x_2 + x_4\\
y_2 &= x_1x_4 + x_2x_3 + x_4x_6 + x_1 + 1\\
y_3 &= x_1x_2 + x_1x_4 + x_2x_3 + x_3x_4 + x_3x_5 + x_4x_5 + x_1\\
y_4 &= x_1x_2 + x_3x_5 + 1\\
y_5 &= x_1x_3 + x_1x_4 + x_2x_3 + x_3x_5 + x_3 + x_4
\end{aligned}
$$

Matematický základ 3

- Veřejným klíčem MC je systém polynomů
- K vytvoření tohoto systému založeného na problému MQ potřebuje snadno invertibilní kvadratické zobrazení $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$, takzvaný *central map*
- Protože je snadno invertovatelné, musí být skryté ve veřejném klíči pomocí invertovatelných afinních transformací: $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ a $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$.
- Veřejným klíčem tohoto systému je složené zobrazení:

$$\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}^n \to \mathbb{F}^m$$

- a soukromý klíč se skládá ze tří zobrazení $\mathcal{S}$, $\mathcal{F}$ and $\mathcal{T}$, tvořících *padací vrátka*

Matematický základ 4

Konstrukce

- Snadno invertovatelné kvadratické zobrazení $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$
- Dvě invertovatelné zobrazení $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ a $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- Veřejný klíč: $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ vypadající jako náhodný systém
- Soukromý klíč: $\mathcal{S}, \mathcal{F}, \mathcal{T}$ umožňující invertovat veřejný klíč

Definice

Dva polynomiální systémy $\mathcal{G} : \mathbb{F}^n \to \mathbb{F}^m$ a $\mathcal{H} : \mathbb{F}^n \to \mathbb{F}^m$ jsou isomorfní

$\Leftrightarrow \exists$ lineární (afinní) zobrazení $\mathcal{L}_1$ a $\mathcal{L}_2$ tak, že $\mathcal{H} = \mathcal{L}_1 \circ \mathcal{G} \circ \mathcal{L}_2$

- Zabezpečení MC je také založeno na **Problému EIP** (Extended Isomorphism of Polynomials):
- K veřejnému klíči $\mathcal{P}$ MC vyhledejte afinní zobrazení $\bar{\mathcal{S}}$ a $\bar{\mathcal{T}}$ a invertibilní kvadratické zobrazeni $\bar{\mathcal{F}}$ takové, že $\mathcal{P} = \bar{\mathcal{T}} \circ \bar{\mathcal{F}} \circ \bar{\mathcal{S}}$.
- Obtížnost problému silně závisí na struktuře central map $\mathcal{F}$

Matematický základ 5

- Obecně není o složitosti známo mnoho, protože bezpečnostní analýza *multivariete schemes* je těžký úkol
- Vztah jednotlivých zobrazení u MC s veřejným klíčem

$$\begin{array}{ccc} \mathbf{z} \in \mathbb{F}^n & \xrightarrow{\mathcal{P}} & \mathbf{w} \in \mathbb{F}^m \\ \mathcal{T}\big\downarrow & & \big\uparrow\mathcal{S} \\ \mathbf{y} \in \mathbb{F}^n & \xrightarrow{\mathcal{F}} & \mathbf{x} \in \mathbb{F}^m \end{array}$$

Šifrování

- Pro zašifrování zprávy $\mathbf{z} \in \mathbb{F}^n$ s použitím veřejného klíče $\mathcal{P}$ platí:

$$\mathbf{w} = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^m$$

Dešifrování

- Pro dešifrování šifrovaného textu je potřebné vypočítat otevřený text ve třech krocích se znalostí soukromého klíče:

$$\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^m,\ \mathbf{y} = \mathcal{F}^{-1}(\mathbf{x}) \in \mathbb{F}^n,\ \mathbf{z} = \mathcal{T}^{-1}(\mathbf{y}) \in \mathbb{F}^n$$

Matematický základ 5

Dešifrování

- Musí být splněna nerovnost $m \geq n$, která zabezpečí, že dešifrování bude prosté zobrazení (klíč $\mathcal{P}$ injektivní)
- Takto bude dešifrování jednoznačné a dá jedinečný otevřený text

Podepisování

- Pro generování podpisu zprávy d použijeme nejdřív hash funkci:
$$\mathcal{H} : \{0, 1\}^* \to \mathbb{F}^m$$
- Vypočteme hash zprávy d :
$$\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^m$$
- Následně vypočítáme rekurzivně:
$$\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^m, \; \mathbf{y} = \mathcal{F}^{-1}(\mathbf{x}) \in \mathbb{F}^n, \; \mathbf{z} = \mathcal{T}^{-1}(\mathbf{y}) \in \mathbb{F}^n,$$
- kde $\mathbf{z}$ je podpis zprávy d

Matematický základ 6

- Podmínka $m \leq n$ je nutná pro surjektivitu zobrazeni $\mathcal{F}$, tj. každá zpráva musí mit svůj podpis

Ověření podpisu

- Pro ověření podpisu $\mathbf{z} \in \mathbb{F}^n$ zprávy d nejdřív vypočítáme hash funkci zprávy d:

$$\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^m$$

a pak s použitím veřejného klíče (zobrazení) $\mathcal{P}$ vypočítáme

$$\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^m$$

- Pokud $\mathbf{w}' = \mathbf{w}$, pak podpis platí, jinak je odmítnut

MC wokflow

Dešifrování / Generování podpisu

$$\mathbf{w} \in \mathbb{F}^m \xrightarrow{\mathcal{S}^{-1}} \mathbf{x} \in \mathbb{F}^m \xrightarrow{\mathcal{F}^{-1}} \mathbf{y} \in \mathbb{F}^n \xrightarrow{\mathcal{T}^{-1}} \mathbf{z} \in \mathbb{F}^n$$

$$\longleftarrow \mathcal{P} \longleftarrow$$

Šifrování / Ověřování podpisu

Unbalanced Oil and Vinegar – UOV 1

- Název **Unbalanced Oil & Vinegar** (UOV) ukazuje na to, že proměnné polynomů jsou seskupeny do dvou skupin: ocet a olej
- Tyto dvě skupiny proměnných jsou v polynomech smíšené
- Nevyvážený charakter znamená, že poměr proměnných je vždy v prospěch octa (více proměnných octa než olejových proměnných)
- Schéma podpisu navrhli Kipnis a Patarin v roce 1999
- Schéma UOV je jednoduché
- Podepisování je rychlé
- Nevýhodou jsou jeho velké veřejné klíče

Unbalanced Oil and Vinegar – UOV 2

- Nechť je $\mathbb{F}$ konečné těleso, $v, o \in \mathbb{N}$ and $n = v + o$, $V = \{1, \ldots, v\}$, $O = \{v + 1, \ldots, n\}$
- Proměnné $x_1, \ldots, x_v$ jsou proměnné Octa and $x_{v+1}, \ldots, x_n$ proměnné Oleje
- Pokud $v = o$, pak říkáme že máme metodu vyváženého poměru Oleje a Octa (Oil & Vinegar (OV))
- V případě, že $v > o$, je to UOV
- Centrální zobrazení (*central map*) $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^o$ je složené z o kvadratických polynomů $f_1, \ldots, f_o$:

$$f_k = \sum_{i,j \in V} \alpha_{ij}^{(k)} \cdot x_i x_j + \sum_{i \in V, j \in O} \beta_{ij}^{(k)} \cdot x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} \cdot x_i + \delta^{(k)}$$

where $\alpha_{ij}^{(k)}$, $\beta_{ij}^{(k)}$, $\gamma_i^{(k)}$, $\delta^{(k)} \in \mathbb{F}$ and $1 \le k \le o$.

Unbalanced Oil and Vinegar – UOV 3

- Pro utajení mapování $\mathcal{F}$ ve veřejném klíči použijeme invertibilní mapovací funkci $\mathcal{T} : \mathbb{F}^n \rightarrow \mathbb{F}^n$.
- Pro danou metodu je veřejný klíč dán:

$$\mathcal{P} = \mathcal{T} \circ \mathcal{F} : \mathbb{F}^n \rightarrow \mathbb{F}^o$$

- Soukromý klíč je složen z $\mathcal{F}$ a $\mathcal{T}$
- Druhá mapovací funkce $\mathcal{S}$ již není nutná z hlediska bezpečnosti UOV.
- Všimněme si, že v $\mathcal{F}$ mohou mít pouze proměnné Octa kvadratickou formu a koeficienty polynomů mohou být náhodně vybrány

MC – útoky 1

Přímý útok

- Pokusit se vyřešit rovnici $\mathcal{P}(\mathbf{z}) = \mathbf{w}$ jako instanci MQ-problému
- Všechny algoritmy mají exponenciální dobu běhu (pro $m \approx n$)

XL – algoritmus

Jsou dané nelineární polynomy $f_1 \ldots f_m$

1. *eXtend* násobení polynomů $f_1 \ldots f_m$ $\forall$ monomy stupně $\leq D$
2. *Krok v lineární algebře*: aplikace Gaussovy eliminace na rozšířený systém s cílem vygenerování jednorozměrného polynomu p
3. *Řešte*: K řešení polynomu p je použit Berlekampův algoritmus
4. *Opakujte*: Nahraďte řešení p v systému a pokračujte se zjednodušeným systémem
5. Složitost: $3 \binom{n + d_{reg}}{d_{reg}}^2 \binom{n}{2}$

MC – útoky 2

Algoritmus založený na Gröbnerových bázích

- najít “nice” bázi ideálu $\langle f_1, \ldots, f_m \rangle$
- nejprve studoval B. Buchberger
- později vylepšeno Faugère et al. (F_4, F_5) [1]
- aktuálně nejrychlejší algoritmy pro řešení náhodných systémů (hybrid F_5) [2]
- Složitost$(q, m, n) = \min_k q^k \mathcal{O}\left(m \binom{n-k+d_{reg}-1}{d_{reg}}^w\right)$,

  kde $2 < \omega \leq 3$

[1] J.C. Faugère: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139, pp. 61-88 (1999).

[2] L. Bettale, L.C Faugère, L. Perret: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology 3, pp. 177-197 (2009).

MC – útoky 3

Složitost přímého útoku

Kolik rovnic je potřeba pro splnění dané úrovně zabezpečení?

Úroveň bezpečnosti [bit]	počet rovníc		
	GF(16)	GF(31)	GF(256)
80	30	28	26
100	39	36	33
128	51	48	43
192	80	75	68
256	110	103	93

MC – shrnutí

- MC se zabývá systémy nelineárních (obvykle kvadratických) vícerozměrných polynomů
- Je jedním z hlavních kandidátů na postkvantové kryptosystémy
- Odolný vůči útokům na kvantových počítačích
- Velmi rychlý (o hodně než RSA)
- Jenom jednoduché aritmetické operace jsou požadovány
- Vhodné pro low cost zařízení – IoT
- Velmi efektivní podpisová schémata s krátkými podpisy (120 b pro 80 b bezpečnost)
- MC není tak dobrá pro šifrovací schémata
- Velký veřejný klíč ($\approx$ 10 - 100 kB), žádné bezpečnostní důkazy
- Ale teoretické odhady zabezpečení se velmi dobře shodují s experimentálními daty

Zdroje

https://2017.pqcrypto.org/school/slides/1-Basics.pdf

https://www.mathematik.uni-kl.de/ ederc/download/mpkc.pdf

https://www.researchgate.net/publication/319170467
_Current_State_of_Multivariate_Cryptography

Jan Rahm: Multivariate cryptography, Dip. práce, FIT ČVUT, 2020