Voľba parametrov podpisovej schémy UOV pre použitie v súčtovej kruhovej podpisovej schéme

viliam.hromada

May 2025

Tento článok nadväzuje (a miestami doslovne preberá) časti z predošlého článku o súčtovej kruhovej podpisovej schéme využívajúcej podpisový algoritmus GeMSS [1].

1 Súčtová kruhová podpisová schéma

V práci [2] autori uvádzajú, že pri použití súčtovej kruhovej podpisovej schémy, ktorú v článku navrhli, je potrebné uvažovať nasledovný možný útok falšovania kruhového podpisu. Útočník môže vygenerovať platný kruhový podpis správy w a vydávať sa za účastníka skupiny $\mathcal{R} = \{u_1, ..., u_k\}$, ak sa mu podarí nájsť podpis, resp. vektor hodnôt $(z_1, ..., z_k)$, pre ktoré platí:

$$\mathcal{P}_1(z_1) + \mathcal{P}_2(z_2) + ... + \mathcal{P}_k(z_k) = w, \tag{1}$$

kde $\mathcal{P}_i$ je verejný kľúč účastníka u_i skupiny. V uvedenej schéme je $\mathcal{P}_i$ sústava m kvadratických polynómov o n neurčitých nad konečným poľom $\mathbb{F}$.

Existujú 2 prístupy pre sfalšovanie podpisu správy w:

1. Útočník náhodne vygeneruje $k-1$ hodnôt $(z_1, ..., z_{k-1}), z_i \in \mathbb{F}^n$, vypočíta $\tilde{w} = w - \sum_{i=1}^{k-1} \mathcal{P}_i(z_i)$ a pokúsi sa nájsť hodnotu z_k takú, že $P_k(z_k) = \tilde{w}$.
2. Útočník sa priamo pokúsi nájsť riešenie sústavy (1).

Prvý prístup je ekvivalentný nájdenia podpisu správy $\tilde{w}$ v jednej inštancii použitej podpisovej schémy. Tento prístup by teda mal mať rovnakú náročnosť ako sfalšovanie podpisu v použitej podpisovej schéme, prípadne riešenie sústavy m kvadratických rovníc o n premenných nad konečným poľom.

Druhý prístup, t.j. riešenie sústavy (1), **nie je ekvivalentný** zlomeniu použitej podpisovej schémy. Sústava (1) totiž predstavuje sústavu m rovníc o $n \cdot k$ premenných. S rastúcim počtom účastníkov schémy teda úmerne rastie počet premenných v sústave (1), čím sa sústava stáva viac *nedourčenou*. V práci [2] autori tvrdia:

1. Ak pre počet celkový počet premenných N a počet rovníc M nedourčenej sústavy rovníc $\mathcal{P}$ platí, že $N = \omega M$, potom riešenie sústavy $\mathcal{P}$ je tak ťažké, ako riešenie sústavy $M - \lfloor \omega \rfloor + 1$ rovníc o $M - \lfloor \omega \rfloor + 1$ premenných.

2. Ak pre počet premenných N sústavy $\mathcal{P}$ o M rovniciach platí $N \geq \frac{M(M+3)}{2}$, potom je sústava $\mathcal{P}$ riešiteľná v polynomiálnom čase.

Z toho vyplýva, že pri voľbe parametrov použitých podpisových schém je nutné tieto parametre voliť tak, aby:

1. Každá inštancia použitej podpisovej schémy spĺňala minimálne požadovanú úroveň bezpečnosti.

2. Výsledný verejný kľúč skupiny predstavoval systém polynómov, ktorého hľadanie koreňov má zložitosť minimálne na požadovanej úrovni bezpečnosti.

2 Voľba parametrov UOV pre súčtovú kruhovú podpisovú schému

Základná schéma UOV je podľa popisu [4] parametrizovateľná:

1. parameter q udávajúci počet prvkov použitého konečného poľa $\mathbb{F}_q$

2. počtom polynómov vo verejnom kľúči m

3. počtom neurčitých v polynómoch verejného kľúča n

Autori [4] uvádzajú bitové zložitosti útokov, ktoré ohrozujú bezpečnosť UOV. Parametre q, n, m sú potom volené tak, aby výsledné zložitosti útokov boli na požadovanej úrovni. Napríklad pre 128-bitovú bezpečnosť musia tieto útoky mať zložitosť aspoň 2^{143} [4].

Jednotlivé útoky a im odpovedajúce zložitosti sú nasledovné (pre viac detailov pozri [4], nižšie uvedený parameter $r = 8$ podľa odporúčaní autorov):

1. Kolízny útok, zložitosť: $2^{10.7}\sqrt{q^m mr}$

2. Priamy útok (riešenie sústavy rovníc danej verejným kľúčom, $\mathcal{P}_i(x) = y$), zložitosť: $\min_k q^k \cdot 3\binom{n'-k+d_{n'-k,m'}}{d_{n'-k,m'}}^2 \binom{n'-k+2}{2}(2r^2 + r)$, kde $d_{a,b}$ je stupeň regularity XL a je definovaný ako najmenšie $d > 0$ také, že koeficient t^d v mocninovom rade $\frac{(1-t^2)^M}{(1-t)^{N+1}}$ nie je pozitívny.

   Hodnoty $n' = m - 1, m' = m - 1$, kde m je efektívny počet rovníc sústavy, ktoré priamy útok rieši.

3. Útok metódou Kipnis-Shamir, zložitosť $q^{n-2m} n^{2.8}(2r^2 + r)$

4. Útok hľadania vektorov z prieniku olejových podpriestorov (*intersection attack, ∩-útok*, zložitosť uvádzajú autori ako zložitosť priameho útoku, v ktorom by hodnoty $M = \binom{k+1}{2}m - 2\binom{k}{2}$ a $N = kn - (2k-1)m$.

Autori v práci [4] uvádzajú 2 verzie UOV so 128-bitovou bezpečnosťou, UOV-Ip a UOV-Is, ktoré sa primárne líšia v použitom konečnom poli. V tabuľke uvádzame verzie s parametrami a $\log_2$ odhadom zložitosti útokov, **boldom** je označený útok s najmenšou zložitosťou:

Verzia (n, m, q)	Kolízny útok	Priamy útok	KS útok	$\cap$-útok
UOV-Ip $(112, 44, 256)$	191	**145**	218	166
UOV-Is $(160, 64, 16)$	**143**	165	154	176

Keďže s rastúcim počtom členov skupiny v súčtovej kruhovej schéme rastie počet premenných v systéme (1), musíme odhadnúť aj zložitosť riešenia výslednej sústavy rovníc, ktorú dostaneme pre skupinu o veľkosti $|\mathcal{R}|$. Na tento odhad zložitosti použijeme vzťah uvedený pre priamy útok, keďže priamy útok je práve útok, v ktorom sa rieši príslušný systém rovníc. Avšak, ako hodnotu m, teda efektívneho počtu rovníc sústavy, použijeme hodnotu $M - \lfloor \omega \rfloor + 1$, kde M je počet rovníc systému (1) a $\omega = N/M$, kde N je celkový počet premenných systému (1).

Napríklad pri schéme UOV-Ip, ak by sme uvažovali súčtovú kruhovú schému s 5 používateľmi, počet premenných v systéme (1) by stúpol 5-násobne, čo by malo za následok, že podľa vzťahu pre priamy útok by zložitosť riešenia tejto sústavy bola len 2^{116}.

Prehľadávaním rôznych možností sme určili parametre schémy UOV-Ip pre skupiny o veľkostiach 5, 10 a 20 používateľov. Parametre musia spĺňať tú vlastnosť, že výsledná schéma bude bezpečná ako v klasickej inštancii, tak aj v súčtovom kruhovom podpise. Výsledné parametre spolu s príslušnými zložitosťami útokov, veľkosť skupiny označujeme ako $|\mathcal{R}|$:

$\lvert\mathcal{R}\rvert$	Verzia (n, m, q)	Kolízny útok	Priamy útok	KS útok	$\cap$-útok	Priamy útok (1)
5	UOV-Ip $(129, 54, 256)$	231	169	194	**145**	146
10	UOV-Ip $(152, 66, 256)$	279	199	187	**144**	146
20	UOV-Ip $(189, 86, 256)$	359	252	164	**143**	146

Literatúra

[1] HROMADA, VILIAM. Voľba parametrov podpisovej schémy GeMSS pre použitie v prstencovej podpisovej schéme. Dostupné na `https://uim.fei.stuba.sk/wp-content/uploads/2021/03/GeMssSkupina.pdf`.

[2] MOHAMED, Mohamed Saied Emam; PETZOLDT, Albrecht. RingRainbow–an efficient multivariate ring signature scheme. In: Progress in Cryptology-AFRICACRYPT 2017: 9th International Conference on Cryptology in Africa, Dakar, Senegal, May 24-26, 2017, Proceedings 9. Springer International Publishing, 2017. p. 3-20.

[3] BEULLENS, Ward, et al. Mayo. Specification document of NIST PQC Standardization of Additional Digital Signature Scheme, 2023.

[4] BEULLENS, Ward, et al. UOV—Unbalanced Oil and Vinegar. Algorithm Specifications and Supporting Documentation Version, 2023, 1.0-05.