Voľba parametrov podpisovej schémy GeMSS pre použitie v prstencovej podpisovej schéme

Viliam Hromada

18. marca 2021

1 Voľba parametrov podpisovej schémy GeMSS pre použitie v prstencovej podpisovej schéme

1.1 Vplyv rozmerov verejného kľúča na bezpečnosť

Ako uvádzajú autori práce [1] v ich práci v kapitole 4.1, pri prstencovej skupinovej podpisovej schéme skonštruovanej podľa kapitoly 4 článku, je potrebné uvažovať nasledovný možný útok generovania falošného podpisu správy. Aby útočník sfalšoval podpis správy w a vydával sa za účastníka skupiny $\mathcal{R} = \{u_1, u_2, ..., u_k\}$, musí nájsť taký podpis $z_1, z_2, ..., z_k$, pre ktorý platí vzťah:

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

Existujú 2 prístupy:

1. Útočník náhodne vygeneruje k-1 hodnôt $z_1, z_2, ..., z_{k-1} \in \mathbb{F}^n$, vypočíta $\tilde{w} = w - \sum_{i=1}^{k-1} \mathcal{P}_i(z_i)$ a pokúsi sa nájsť riešenie z_k systému $\mathcal{P}_k(z_k) = \tilde{w}$.
2. Útočník sa pokúsi priamo vyriešiť sústavu (1).

Bezpečnosť prvej uvedenej situácie je ekvivalentná zlomeniu jednej inštancie použitej podpisovej schémy.
Bezpečnosť druhej uvedenej situácie, t.j. riešenie sústavy (1), však **nie je taká** ako bezpečnosť prvej uvedenej situácie, teda riešenie sústavy (1) **nie je tak ťažké** ako riešenie jednej inštancie podpisovej schémy. Je to z toho dôvodu, že systém (1) obsahuje oveľa viacej premenných než rovníc, a teda ide o (značne) nedourčenú sústavu rovníc. V práci [1] autori tvrdia, že pri riešení takejto sústavy rovníc platí:

1. Ak pre počet premenných n a počet rovníc m nedourčenej sústavy $\mathcal{P}$ platí, že $n = \omega m$, potom riešenie sústavy $\mathcal{P}$ je tak ťažké, ako riešenie sústavy $m - \lfloor \omega \rfloor + 1$ rovníc o rovnakom počte premenných.
2. Ak pre počet premenných n sústavy $\mathcal{P}$ o m rovniciach platí $n \geq \frac{m(m+3)}{2}$, potom je možné sústavu $\mathcal{P}$ riešiť v polynomiálnom čase.

Preto je potrebné nastaviť parametre použitých podpisových schém tak, aby:

1. Každá inštancia podpisovej schémy každého používateľa spĺňala minimálne požadovanú úroveň bezpečnosti.

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

Ak je použitou podpisovou schémou Rainbow, autori v článku [1] uvádzajú odporúčané parametre, aby bola dosiahnutá požadovaná úroveň bezpečnosti (v práci uvažujú úrovne 80, 100 a 128 bitov) prstencovej podpisovej schémy vzhľadom na počet účastníkov 5, 10, 20 a 50. Keďže pre podpisovú schému GeMSS rovnaké odporúčania chýbajú, na základe dostupných informácií o bezpečnosti systému GeMSS [2] sme sa rozhodli určiť odhad nastavenia parametrov GeMSS, aby bola zachovaná bezpečnosť:

1. Každej inštancie GeMSS každého účastníka prstencovej podpisovej schémy na úrovni 128 bitov.

2. Výsledného skupinového verejného kľúča na úrovni 128 bitov, z hľadiska útoku hľadania riešenia sústavy (1).

1.2 Voľba parametrov GeMSS pre prstencovú podpisovú schému

GeMSS pracuje nad poľom $GF(2)$, základné parametre sú:

- Stupeň rozšírenia poľa n
- Počet odstránených polynómov (modifikátor mínus) Δ
- Počet octových premenných v HFE polynóme v

Pre uvedené parametre je potom verejný kľúč jedného používateľa sústava polynómov nad konečným poľom $GF(2)$, ktorá obsahuje:

- Počet polynómov verejného kľúča: $m = n - \Delta$
- Počet neurčitých v polynómoch verejného kľúča: $n + v$

V prípade, že uvažujeme prstencovú podpisovú schému, ktorej sa zúčastňuje k používateľov, tak vzťah (1) predstavuje sústavu polynómov, ktorá obsahuje

- Počet polynómov v súčte danom vzťahom (1): $m = n - \Delta$
- Počet neurčitých v polynómoch vzťahu (1): $k(n + v)$

V článku [2] v kapitole 8.3.1 sa nachádza vzťah, ktorý udáva asymptotickú zložitosť riešenia kvadratickej sústavy m rovníc o m premenných nad konečným poľom $GF(2)$ ako

$$O(2^{0.792 \cdot m})$$

Aby sme dosiahli požadovanú úroveň bezpečnosti 128 bitov, $m \geq 162$, keďže zložitosť riešenia sústavy $m = 162$ rovníc o 162 premenných je podľa tohto vzťahu $O(2^{128.3})$. Preto aj verzia podpisovej schémy GeMSS so 128 bitovou bezpečnosťou GeMSS128 pre jedného používateľa, ktorá je súčasťou návrhu [2], je navrhnutá tak, aby $m = 162$.
Ak sa použije schéma GeMSS s parametrami (n, Δ, v) na tvorbu prstencovej podpisovej schémy, tak sústava daná vzťahom (1) obsahuje m rovníc a $k(n + v)$ premenných. V takom prípade dochádza k tomu, že riešenie tejto sústavy je tak ťažké, ako riešenie sústavy $(n - \Delta) - \lfloor \frac{k(n+v)}{(n-\Delta)} \rfloor + 1$ rovníc o rovnakom počte premenných [1].
Preto **základné pravidlo** voľby parametrov GeMSS (n, Δ, v) pre použitie v prstencovej schéme k používateľov, ktorá dosahuje 128-bitovú bezpečnosť je, aby pre parametre platilo:

$$(n - \Delta) - \lfloor \frac{k(n + v)}{n - \Delta} \rfloor + 1 \geq 162 \tag{2}$$

Ak spĺňajú parametre vzťah (2), potom možno predpokladať, že zložitosť riešenia sústavy (1) je aspoň 2^{128}.
Samozrejme, parametre (n, Δ, v) musia zároveň spĺňať predpoklady zachovania 128-bitovej bezpečnosti pre jednotlivé inštancie systému GeMSS. V kapitole 8.7 článku [2] autori uvádzajú spôsob výpočtu parametrov, aby bola schéma GeMSS bezpečná na požadovanej úrovni λ. V našom prípade $\lambda = 128$. Ďalší dôležitý parameter GeMSS je stupeň použitého HFE polynómu D. V našom prípade $D = 513$

1. Pre počet polynómov verejného kľúča m musí platiť

$$m \geq 1.26\lambda = 161.28 \tag{3}$$

2. Pre stupeň regularity D_{reg} sústavy polynómov verejného kľúča musí platiť

$$O(\binom{m}{D_{reg}}^2) \geq 2^{\lambda} \tag{4}$$

3. Zároveň v kapitole 8.5 článku [2] autori uvádzajú, že pre počet $\Delta + v$ by malo platiť

$$\Delta + v = 3 \times (D_{reg} - D_{reg}^{HFE}), \tag{5}$$

D_{reg}^{HFE} je stupeň regularity centrálneho HFE zobrazenia bez modifikátorov.

4. Hodnota D_{reg}^{HFE} sa dá podľa [2] aproximovať

$$D_{reg}^{HFE} \approx 2,03 + 0,36 \log_2(D) \approx 6. \tag{6}$$

Na základe uvedených vzťahov sme určili hodnoty parametrov (n, Δ, v) pre rôzne počty účastníkov prstencovej podpisovej schémy, $k = 5, 10, 20, 50$. Hodnoty boli zvolené tak, aby výsledna prstencová podpisová schéma spĺňala vzťah (2) a zároveň, aby každá inštancia GeMSS s danými parametrami spĺňala vzťahy (3), (4), (5), (6). Parametre boli odvodené od schémy GeMSS128 pre jedného používateľa, pre ktorú platí $(n, \Delta, v) = (174, 12, 12)$ [2]. Vo všetkých prípadoch sa jedná o schémy nad **konečným poľom** $GF(2)$, **stupeň HFE polynómu je** $D = 513$ a parameter nb_ite $= 4$.
Hodnoty parametrov uvádzame v tabuľke. Parametre sú platné pre uvedený počet účastníkov k v záhlaví stĺpca, alebo pre prípadný menší počet účastníkov.

128-bitová bezpečnosť	$k = 5$	$k = 10$	$k = 20$	$k = 50$
Parametre (n, Δ, v)	(178,12,12)	(184,12,12)	(194,11,11)	(227,11,11)
$m = n - \Delta$	166	172	183	216
Verejný kľúč skupiny (kB)	1 883	4 151	9 661	38 397
Podpis skupiny (bity)	1 310	2 680	5 420	15 200

Tabuľka 1: Navrhované hodnoty parametrov GeMSS pre prstencovú podpisovú schému

Parametre boli zvolené tak, aby v uvedených prípadoch $k = 5, 10, 20, 50$ príslušná schéma vo vzťahu (2) mala hodnotu ľavej strany práve 162. Z hľadiska bezpečnosti jednotlivých inštancií GeMSS :

1. Z tabuľky 1 vidieť, že vo všetkých prípadoch je nerovnosť (3) splnená.

2. Na základe parametra m je požadovaný stupeň regularity D_{reg} podľa vzťahu (4):

	$k = 5$	$k = 10$	$k = 20$	$k = 50$
Parametre (n, Δ, v)	(178,12,12)	(184,12,12)	(194,11,11)	(227,11,11)
D_{reg}	14	14	13	13

Tabuľka 2: Požadované hodnoty D_{reg} pre uvedené verzie GeMSS

3. Potom na základe D_{reg} a vzťahu (5) pre parametre $\Delta + v$ musí platiť:

	$k = 5$	$k = 10$	$k = 20$	$k = 50$
Parametre (n, Δ, v)	(178,12,12)	(184,12,12)	(194,11,11)	(227,11,11)
$\Delta + v$	24	24	21	21

Tabuľka 3: Odporúčané hodnoty $\Delta + v$ pre uvedené verzie GeMSS

V prípade schém pre $k = 5$ a $k = 10$ účastníkov je tento vzťah splnený. V prípade schém pre $k = 20$ a $k = 50$ sme pristúpili k voľbe parametrov kde $\Delta + v = 22$. Je to z toho dôvodu, že autori v článku [2] odporúčajú v kapitole 8.5 aby $\Delta = v$.

Literatúra

[1] MOHAMED, Mohamed Saied Emam; PETZOLDT, Albrecht. RingRainbow–an efficient multivariate ring signature scheme. In: International Conference on Cryptology in Africa. Springer, Cham, 2017. p. 3-20.

[2] CASANOVA, A., et. al.: GeMSS: a great multivariate short signature (2019). Submission to NIST PQC "competition" Round-3.