Nový perturbačný modifikátor schémy HFE

Autor: Sabina Daniela Pekareková
Vedúci práce: Ing. Viliam Hromada, PhD.

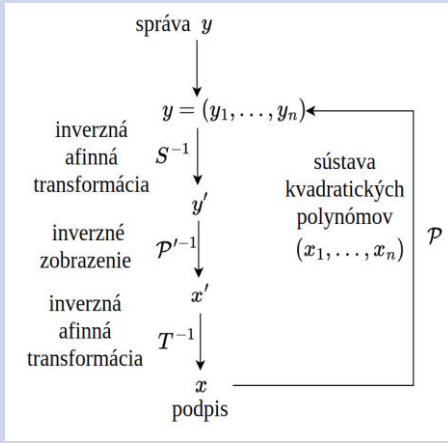
Motivácia

- S príchodom výkonného kvantového počítača prichádza riziko prelomenia bezpečnosti súčasnej asymetrickej kryptografie, ktorú využívame v bežnom živote napr. pri prehliadaní internetového obsahu či online bankovníctve.
- V roku 1994 Peter Shor navrhol algoritmus, ktorým je možné riešiť pomocou kvantového počítača problémy faktorizácie prvočísel a diskrétneho logaritmu, na ktorých sú založené dnešné asymetrické kryptosystémy. Z tohto dôvodu ich považujeme za prelomené a je potrebné sa venovať návrhu nových postkvantových systémov.
- V tejto diplomovej práci sa zaoberáme perturbačným modifikátorom $HFE^{\hat{+}-}$ podpisovej schémy, ktorá patrí medzi systémy založené na sústave kvadratických rovníc. Ide o oblasť postkvantovej kryptografie využívajúcej polynómy viacerých neurčitých nad konečnými poliami. V roku 2022 navrhol kolektív autorov okolo J.C.Faugera nový modifikátor HFE schémy, ktorý by mal zvýšiť jej bezpečnosť.

Ciele práce

Cieľom diplomovej práce bolo implementovať základnú HFE podpisovú schému a schému s perturbačným modifikátorom $HFE^{\hat{+}-}$, ako aj porovnať tieto dve implementácie z hľadiska časovej zložitosti. Taktiež bolo cieľom implementovať perturbačný modifikátor s dvomi možnými inverziami (inverzia cez prehľadávanie všetkých možností a inverzia pomocou projekcie).

HFE schéma



Ide o typ trapdooru, využívajúci teóriu nadpolí. Používa základné pole F_q a jeho n-té rozšírenie F_{q^n}. Tvorí časť P' zo súkromného kľúča (ľahko-invertovateľné zobrazenie). P' sa na začiatku nezadáva priamo ako sústava polynómov, ale polynóm s jednou premennou nad rozšírením poľa. Polynóm v HFE tvare pre pole rozšírenia GF(2^n) by vyzeralo následovne:

$$P'(X) = \sum_{\substack{0 \le i,j \le d \\ 2^i + 2^j \le d}} C_{i,j} X^{2^i + 2^j} + \sum_{\substack{0 \le k \le d \\ 2^k \le d}} B_k X^{2^k} + A$$

Koeficienty A, B_k, $C_{i,j}$ a neurčitá X reprezentujú prvky z rozšírenia poľa GF(2^n).

Perturbačný modifikátor

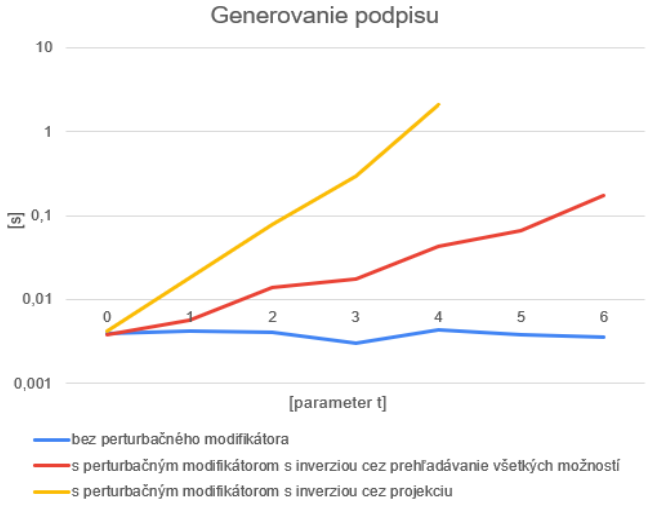
Zavádza parameter ***t*** rozmer perturbácie $\hat{+}$ a parameter ***a*** modifikátora -, ktorý predstavuje počet polynómov, ktoré sa odstránia z verejného kľúča.

Experimenty

Merali sme čas potrebný pre vygenerovanie verejného kľúča, vygenerovanie platného podpisu a overenie platnosti podpisu pre základnú HFE podpisovú schému a dve implementácie $HFE^{\hat{+}-}$ s meniacim sa parametrom ***t***.

Výsledky

Podľa našich zistení je implementácia $HFE^{\hat{+}-}$ s inverziou cez prehľadávanie všetkých možností efektívnejšia než implementácia $HFE^{\hat{+}-}$ s inverziou cez projekciu. Z nameraných hodnôt pre generovanie verejného kľúča a overenie platnosti podpisu vyplýva, že zavedenie perturbačného modifikátora neprináša takmer žiadny nárast času ich trvania.



Prínos práce

Okrem odporúčaných parametrov sme hľadali kompromis medzi rýchlosťou a bezpečnosťou, keďže zvýšenie rýchlosti vedie k zníženiu bezpečnosti a naopak. Podarilo sa nám nájsť také parametre, ktoré by mohli priniesť potencionálne zníženie času potrebného pre vygenerovanie platného podpisu pomocou $HFE^{\hat{+}-}$schémy, so zachovaním požadovanej úrovne bezpečnosti.