SLOVENSKÁ TECHNICKÁ UNIVERZITA

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

SKUPINOVÁ PODPISOVÁ SCHÉMA ZALOŽENÁ NA MPKC

ZÁMER

Práca sa zaoberá konštrukciou prstencových podpisových schém nad kryptosystémami založenými na systéme polynómov viacerých neurčitých. Venujeme sa hlavne prstencovým podpisovým schémam, kde vystupuje ľubovoľný počet účastníkov a tieto prstencové podpisové schémy zaručujú každému členovi úplnú anonymitu. Výsledkom práce je testovacia aplikácia napísaná v jazyku C, vybraných prstencových schém nad kryptosystémami založenými na systéme polynómov viacerých neurčitých, ktoré sme prevzali z práve prebiehajúcej NIST súťaže, kde sa rozhoduje o novom štandarde v podpisovaní.

EXPERIMENTY A VÝSLEDKY PRÁCE

Skúmali sme použitie prstencových schém s použitím kryptosystémov *Rainbow* a *GeMSS*, pričom sme testovali prstencové podpisové schémy s 5, 10, 20 a 50 účastníkmi. Experimentami s testovacou aplikáciou sme zistili, že súčinová podpisová schéma nad *Rainbow* bola pre viac účastníkov efektívnejša, čo sa týka doby vykonania generovania podpisu a verifikácie, ale taktiež aj vo veľkosti verejných kľúčov a vygenerovaných podpisov. Hlavným dôvodom úspechu boli nemenné veľkosti parametrov Rainbowu pri súčinovej podpisovej schéme, pretože celková bezpečnosť súčinovej podpisovej schémy sa nezmení ani s pribúdajúcim počtom účastníkov, čo ale neplatí pri súčtovej podpisovej schéme. Aj tento fakt prispieva k tomu, že súčinová podpisová schéma je výhodnejšia pre použitie do praxe, kedže sa parametre *Rainbowu* nemusia prepočítavať pri zmene počtu účastníkov. Súčtová podpisová schéma dosahuje výborné výsledky hlavne pri nižšom počte úcastníkov (tzn. do 10), ale so zvyšujúcim sa počtom účastníkov sa výkonnostne parametre schémy zhoršujú.

VYUŽITIE V PRAKTICKOM ŽIVOTE

Kryptosystémy založené na polynómoch s viacerými neurčitými sú postkvantové algortimy, ktoré vďaka hrozbe kvantových počítačov budú čoraz viac potrebné pre zaistenie dostatočnej bezpečnosti. Skupinové podpisové schémy budú v budúcnosti viac rozšírené a môžu byť použité napríklad pri elektronických politických voľbách, kde musí byť každému občanovi zaručená úplá anonymita. Podpisové schémy založené na systéme polynómov viacerých neurčitých zaručujú jeden z najkratších podpisov spomedzi mnohých postkvantových algoritmov, čo je pri bežnom používaní veľmi výhodná vlastnosť.

Autor: Ing. Daniela Leščinská

Vedúci práce: Ing. Viliam Hromada, PhD.