SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Evidenčné číslo: FEI-5384-8739

PODPISOVÉ SCHÉMY V POSTKVANTOVEJ KRYPTOGRAFII

DIPLOMOVÁ PRÁCA

2015 **Pavol Dobročka**

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Evidenčné číslo: FEI-5384-8739

PODPISOVÉ SCHÉMY V POSTKVANTOVEJ KRYPTOGRAFII

DIPLOMOVÁ PRÁCA

Študijný program:	Aplikovaná informatika
Číslo študijného odboru:	2511
Názov študijného odboru:	9.2.9 Aplikovaná informatika
Školiace pracovisko:	Ústav informatiky a matematiky
Vedúci záverečnej práce:	doc. Ing. Pavol Zajac, PhD.

Bratislava 2015 **Pavol Dobročka**

SÚHRN

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Študijný program:	Aplikovaná informatika
Autor:	Pavol Dobročka
Diplomová práca:	Podpisové schémy v postkvantovej kryptografii
Vedúci záverečnej práce:	doc. Ing. Pavol Zajac, PhD.
Miesto a rok predloženia práce:	Bratislava 2015

Abstract SK

Kľúčové slová:

ABSTRACT

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Study Programme:	Applied Informatics
Author:	Pavol Dobročka
Diploma Thesis:	Signature schemas in postquantum cryptography
Supervisor:	doc. Ing. Pavol Zajac, PhD.
Place and year of submission:	Bratislava 2015

Abstract EN

Keywords:

Vyhlásenie autora

Podpísaný Pavol Dobročka čestne vyhlasujem, že som diplomovú prácu Podpisové schémy v postkvantovej kryptografii vypracoval na základe poznatkov získaných počas štúdia a informácií z dostupnej literatúry uvedenej v práci.

Vedúcim mojej diplomovej práce bol doc. Ing. Pavol Zajac, PhD.

Bratislava, dňa 1.11.2015

.....

podpis autora

Poďakovanie

I would like to express a gratitude to my thesis supervisor.

Obsah

Zoznam obrázkov a tabuliek

Zoznam skratiek a značiek

WWW - World Wide Web

Zoznam algoritmov

Úvod

Uvod SK

1 Úvod do postkvantovej kryptografie

1.1 Motivácia

Preco skumat postkvantovu kryptografiu, aku vyhodu ponukaju...

1.2 Súčasný stav

Popis ako sa momentalne pouzivaju, ci sa pouzivaju (aky maju podiel).
Velmi strucny opis (pripadne len vymenovanie) toho ake rozne postkvantove kryptosystemy pozname (hash-based, code-based..)

2 Code-based kryptografia

2.1 Úvod

Jednu triedu z postkvantových kryptosystémov tvoria code-based systémy, teda kryptosystémy vychádzajúce z teórie kódovania. Bezpečnosť takýchto systémov je založená na zložitosti takzvaného dekódovacieho problému. V súčasnosti nie je známy algoritmus, ktorý by efektívne dekódoval ľubovoľný kód ako na klasickom, tak aj na kvantovom počítači. Existujú však triedy lineárnych kódov, ktoré efektívne dekódovať vieme. Tento poznatok má kryptografické využitie. Podstata code-based kryptosystémov je skonštruovať kód, ktorý vieme dekódovať a následne tento kód zmodifikovať na kód, ktorý dekódovať nevieme bez toho, aby sme poznali "inverznú" modifikáciu.

2.2 McEliece a Niederreiter

Najstarším a pravdepodobne najznámejším code-based kryptosystémom je McEliecov kryptosystém. Jadro systému tvorí kód C dlžky n s dimenziou k a minimálnou vzdialenosťou $d \geq 2t+1$, kde t je počet chýb, ktorý vie kód opraviť. Podľa pôvodného návrhu sa používajú Goppove kódy, ku ktorým existuje efektívny dekódovací algoritmus.
Verejný a súkromný kľúč zostrojíme nasledovne. Určíme generujúcu maticu G s rozmermi $k \times n$ pre kód C. Ďalej zvolíme náhodnú binárnu regulárnu maticu S s rozmermi $k \times k$ a permutačnú maticu P s rozmermi $n \times n$. Verejný kľúč tvorí matica $G' = SGP$ a parameter t. Súkromný kľuč tvoria matice S, G, P.

Algoritmus 1 McEliece - Algoritmus šifrovania

```
1 Správu m dĺžky k vynásobíme s verejnou maticou G'.
2 c' = mG'
3 Ku zakódovanej správe pripočítame náhodný chybový vektor s váhou t.
4 c = c' + e,  wt(e) = t
5 c tvorí zašifrovaný text
```

Pre praktickú bezpečnosť sa hodnoty parametrov kódu volia približne $n = 1000, k = 500, t = 50$.
K McEliecovmu kryptosystému existuje varianta, ktorá namiesto generujúcej matice G využíva kontrolnú maticu H. Táto duálna forma sa označuje ako Niederreiterov kryptosystém. V tomto kryptosystéme sa správa m najskôr transformuje na vektor m' dĺžky n s Hammingovou váhou t. Funkciu, ktorá vykonáva túto transformáciu označujeme $\phi_{n,t}(m)$. Verejný kľúč tvorí matica $H' = SHP$ a parameter t. Matica S je nahodná reg-

Algoritmus 2 McEliece - Algoritmus dešifrovania

```
1 Správu c vynásobíme s inv(P)
2
3 c = mG'inv(P) = mSG + e*inv(P)
4 m' = decode(mSG + e*inv(P)) = mS;
5 m = m'inv(S)
6
7 m tvorí dešifrovanú správu
```

ulárna binárna matica s rozmermi $(n-k) \times (n-k)$ a P je permutačná matica s rozmermi $n \times n$ a súkromný kľuč tvoria matice S,H,P. Šifrovaný text sa vypočíta ako syndróm slova m', $c = H'm'^T$ Na dešifrovanie slova c vlastník súkromného kľúča najskôr vynásobi slovo c maticou S^{-1} zľava, následne aplikuje dekódovací algoritmus a výsledok vynásobí maticou P^{-1} zľava. $m = P^{-1}decode(S^{-1}SHPm)$

Algoritmus 3 Niederreiter - Algoritmus šifrovania

```
1 Vstup: Správa m
2
3 Vypočítame m' = phi(m), dostaneme chybové slovo dĺžky n s váhou t
4 c = H'*trans(m)
5 c tvorí zašifrovaný text
```

Algoritmus 4 Niederreiter - Algoritmus dešifrovania

```
1 Vstup: Šifrovaný text c
2 c' = inv(S)*c
3 e' = decode(c')
4 e  = inv(P)*e'
5 m = invphi(e)
6
7 e je pôvodné chybové slovo. Po inverznej transformácii z e dostaneme m - o
```

2.2.1 Porovnanie McEliece a Niederreiter

Porovnanie velkosti sprav, klucov pripadne tabulka z CFS clanku

3 Code-based podpisové schémy

3.1 Úvod

Prechod na postkvantovú kryptografiu so sebou prináša aj potrebu implementovať podpisové schémy pomocou postkvantového kryptosystému. Vo všeobecnosti sa na realizáciu digitálneho podpisu využívajú asymetrické kryptosystémy, respektíve kryptosystémy s verejným kľúčom. Kryptosystémy, ktoré sme si predstavili v predchádzajúcej časti spĺňajú toto kritérium. Všeobecná schéma na vytvorenie digitálneho podpisu správy má podľa definície tieto časti

- Algoritmus na generovanie páru privátnych a verejných kľúčov
- Podpisový algoritmus závislý od privátneho kľúča, ktorý vytvorí podpis pre danú správu
- Overovací algoritmus závislý od verejného kľúča, ktorý pre správu prijme alebo zamietne zodpovedajúci podpis

Niektoré kryptosystémy túto schému implementujú tak, že ako podpisovú funkciu použijú dešifrovací algoritmus s prívatným kľúčom a ako overovaciu zvolia šifrovací algoritmus s verejným kľúčom. Podpis a overenie v tejto implementácii môže vyzerať takto

Algoritmus 5 Schéma digitálneho podpisu

```
1 Máme správu m, ktorú chceme podpísať a odtlačkovú funkciu H
2 Vypočítame odtlačok h = H(m)
3 Vypočítame podpis tak, že dešifrujeme odtlačok h pomocou privátneho kľúča
4 Podpísanú správu tvorí dvojica m a s
```

Možnosť tejto implmentácie je silne závisla od toho, ako sa prekrývajú množiny šifrovaných textov a odtlačkov v konkrétnom kryptosystéme. Ako si ukážeme v ďalších častiach práce, nie všetky odtlačky musia byť dešifrovateľné správy.

3.2 Prehľad code-based podpisových schém

V ďalších častiach práce sa už budeme zaoberať iba code-based podpisovými schémami, teda schémami, ktoré využívajú code-based kryptosystémy. Veľkou prekážkou týchto kryptosystémov je v súčasnosti veľkosť kľúča, ktorá je v porovnaní s dnešnými kryptosystémami rádovo tisícnásobne väčšia. Pri implementácii a následne v praxi je dôležité nájsť vhodný kompromis medzi požadovanou bezpečnosťou a výpočtovou a dátovou náročnosťou,

ktorá zavisí od voľby veľkosti kľúča.
Existuje niekoľko potenciálnych návrhov code-based kryptosystémov, z ktorých si bližšie prejdeme CFS (Courtois-Finiasz-Sendrier) a LDGM (Low-density generator matrix).

3.3 CFS schéma

Jedným z nádejných návrhov code-based podpisových schém je CFS schéma, ktorá používa na podpisovanie Niederreiterov kryptosystém. Základný problém, ktorý treba vyriešiť pri podpisovaní založenom na kódovaní, je ako získať taký odtlačok správy, ktorý je dekódovateľné slovo. Ak máme lineárny kód $C(n, k, 2t + 1)$, syndróm slova je vektor dĺžky $n - k$. Počet všetkých syndrómov je 2^{n-k} a počet dekódovateľných syndrómov je $\sum_{i=0}^{t} \binom{n}{i}$. To znamená, že $\frac{\sum_{i=0}^{t} \binom{n}{i}}{2^{n-k}}$ všetkých syndrómov je dekódovateľných. Pre Goppove kódy je to približne $\frac{1}{t!}$. Pravdepodobnosť, že odtlačok správy bude zároveň dekódovateľný, je teda približne $p = \frac{1}{t!}$. Nato, aby sme vedeli podpísať každú správu, budeme musieť ku správe pridať bity navyše, a pokúsiť sa podpísať túto upravenú správu. Priemerný počet pokusov na podpísanie jednej správy je približne $t!$.

Algoritmus 6 Algoritmus podpisovania v CFS

```
1 Vstup: Správa m, odtlačková funkcia H ktorá vracia hashe dĺžky n−k (dĺžka
2 Zvolíme i = 0, h = H(m || i)
3 Pokiaľ h nie je dekódovateľné, zvolíme i = i + 1 a opakujeme predošlý krok
4 e = D(s)
5 signature = (e, i)
```

Implementácia uvedeného algoritmu môže byť vylepšená po viacerých stránkach. Prvé vylepšenie sa dá realizovať pri hľadaní dekódovateľného syndrómu. Na začiatku podpisovania si vypočítame hash samotnej správy $h' = H(m)$ a v ďalších krokoch počítame $h = H(h'||i)$. Ďalší priestor na vylepšenie, tentokrát dĺžka výsledného podpisu, sa ponúka v spôsobe uloženia časti e z podpisu. Autori tejto podpisovej schémy navrhli ukladať e ako index I z množiny všetkých n bitových vektorov s váhou t. To predstavuje číslo z rozsahu $< 1, \binom{n}{t} >$

Algoritmus 7 Algoritmus overovania v CFS

```
Vstup: podpis (e, i), správa m, verejný kľúč H', odtlačková funkcia H ktora

Vypočítame s1 = H*e^t
Vypočítame s2 = H(m || i)

Ak s1 = s2, podpis príjimame, inak zamietame
```

3.3.1 Praktické parametre

3.3.2 CFS s pôvodným McEliece systémom

3.4 LDGM podpis

Ďalší z možných návrhov pre code-based kryptografiu sa pokúša zmenšiť potrebnú veľkosť kľúča pomocou vhodne zvoleného kódu, respektíve pomocou vhodne zvolenej generačnej matice. LDGM (Low-density generation matrix) kódy, čiže kódy s riedkou generačnou maticou sa v niektorých prípadoch dajú zapísať kompaktne pomocou cirkulantných matíc. Generačná matica G kódu dĺžky n s dimenziou k sa skladá z $k_0 n_0$ blokov s rozmermi $p \times p$, kde $n_0 = n/p$ a $k_0 = k/p$.

$$G = \begin{pmatrix} C_{0,0} & C_{0,1} & \cdots & C_{0,n_0-1} \\ C_{1,0} & C_{1,1} & \cdots & C_{1,n_0-1} \\ \vdots & \vdots & \ddots & \cdots \\ C_{k_0-1,0} & C_{k_0-1,1} & \cdots & C_{k_0-1,n_0-1} \end{pmatrix}$$

Každé $C_{i,j}$ je $p \times p$ cirkulatná matica. Vďaka tomu nám stačí uložiť z každého bloku iba jeden riadok. Tým zmenšíme veľkosť kľúča p-násobne. Matica v takomto tvare sa nazýva kvázicyklická (QC). K matici G vypočítame kontrolnú maticu H v systematickom tvare, t.j. $H = [X|I]$. Kontrolná matica H je súčasťou súkromného kľúča. Ďalšiu časť kľúča tvoria matice Q a S. Postup ako určiť maticu Q je zhrnutý v nasledovnom algoritme.

Algoritmus 8 Výpočet matice Q

```
Určíme náhodne matice a, b s rozmermi z x r, z <= r (r = n-k)
Vypočítame maticu R = trans(a)*b X ones(p,p)
//ones - matica p x p same jednotky, X Kroneckerov sucin
Určíme maticu T poskladanú z r0*r0 cirkulantných matic tak, aby váha každé
Q = R + T
```

Maticu S určíme ako náhodnú maticu poskladanú z $r_0 \times r_0$ cirkulantných blokov veľkosti $p \times p$ tak, aby váha každého riadku aj stĺpca bola w_s a aby mala plnú hodnosť.
Verejný kľúč tvorí upravená kontrolná matica $H = Q^{-1}HS^{-1}$. Spôsob, ktorým počítame matice Q a S zachovávajú QC vlastnosti pôvodnej matice H, čo nám umožnuje zmenšenie veľkosti verejného kľúča.

3.5 Porovnanie

Záver

Zaver SK

Resumé

Resume SK

Zoznam použitej literatúry

Prílohy