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.
Konzultant:	mr. nobody

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.
Konzultant:	mr. nobody
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.
Consultant:	mr. nobody
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 10.10.2015

.....

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 jeho varianty

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 počeť 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 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. V tomto prípade sa správa m najskôr transformuje na vektor dĺžky n s Hammingovou váhou t. A šifrovaný text tvorí syndróm $c = Hx^T$

Algoritmus 2 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
```

3 Code-based podpisové schémy

3.1 Úvod

Popis ake code-base schemy existuju

3.2 CFS schéma

Popis ako funguje, ake parametre su navhrnute

3.3 Podpis s pôvodným McEliece systémom

3.4 Porovnanie

Záver

Zaver SK

Resumé

Resume SK

Zoznam použitej literatúry

Prílohy