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 6.12.2015

....

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 kľúč tvoria matice S, G, P.

Algoritmus 1 McEliece - Algoritmus šifrovania

Vstup: Správa m dĺžky k

Výstup: Zašifrovaná správa c

$c' \leftarrow mG'$

Ku zakódovanej správe pripočítame náhodný chybový vektor s váhou t.

$c \leftarrow c' + e$, $wt(e) = t$

return c

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

Algoritmus 2 McEliece - Algoritmus dešifrovania

Vstup: Zašifrovaná správa c

Výstup: Otvorená správa m

Správu c vynásobíme s P^{-1}

$c' \leftarrow cP^{-1} = mSG + eP^{-1}$

$m' \leftarrow Decode(c') = mS;$

$m \leftarrow m'S^{-1}$

return m

$\phi_{n,t}(m)$. Verejný kľúč tvorí matica $H' = SHP$ a parameter t. Matica S je nahodná regulárna 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

Vstup: Správa m

Výstup: Zašifrovaná správa c

$m' \leftarrow \phi(m)$, dostaneme chybové slovo dĺžky n s váhou t

$c \leftarrow H'm^T$

return c

Algoritmus 4 Niederreiter - Algoritmus dešifrovania

Vstup: Vektor c, ktorý predstavuje šifrovanú správu m

Výstup: Dešifrovaná správa, pôvodné m

$c' \leftarrow S^{-1}c$

$e' \leftarrow Decode(c')$

$e \leftarrow P^{-1}e'$

$m \leftarrow \phi^{-1}(e)$

2.2.1 Porovnanie McEliece a Niederreiter

Zhrňme si a porovnajme parametre oboch kryptosystémov a ako sa zvolené parametre kódu prejavia na veľkosti správ a kľúčov.

Tabuľka 1: Porovnanie parametrov McEliece a Niederreiter

	McEliece	**Niederreiter**
Verejný kľúč	G', t	H', t
Privátny kľúč	S, G, P	S, H, P
Veľkosť VK	$k \times n$	$n - k \times n$
Veľkosť PK	$k \times k,\ k \times n,\ n \times n$	$n - k \times n - k,\ n - k \times n,\ n \times n$
Veľkosť otvorenej správy	k	n
Veľkosť šifrovanej správy	n	$n - k$
Počet možných správ	2^k	$\sum_{i=0}^{t} \binom{n}{i}$

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

Máme správu m, ktorú chceme podpísať a odtlačkovú funkciu H

Vypočítame odtlačok $h = H(m)$

Vypočítame podpis tak, že dešifrujeme odtlačok h pomocou privátneho kľúča

Podpísanú správu tvorí dvojica (m, 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 $t!$.

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 ďaľších 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 6 Algoritmus podpisovania v CFS

Vstup: Správa m, odtlačková funkcia H ktorá vracia odtlačky dĺžky $n - k$

Výstup: Podpis správy m, ozn. sig

```
i ← 0
repeat
    h ← H(m||i)
    if h nie je dekódovateľné slovo then
        i ← i + 1
    end if
until h je dekódovateľné slovo
e ← Decode(h)
sig ← (e, i)
return sig
```

Algoritmus 7 Algoritmus overovania v CFS

Vstup: Podpis (e, i), správa m, verejný kľúč H', odtlačková funkcia H ktorá vracia odtlačky dĺžky $n - k$

Výstup: True/False - podpis prijímame/zamietame

```
s1 ← H'e^T
s2 ← H(m||i)
return s1 = s2
```

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 generovaciou maticou sa v niektorých prípadoch dajú zapísať kompaktne pomocou cirkulantných matíc. Generovacia 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 $k_0 = k/p$.

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

Každé $C_{i,j}$ je $p \times p$ cirkulatná matica. Vďaka tomu nám stačí uložiť z každého bloku iba jeden riadok. Tým zmenšíme veľkosť klúča 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 $z \times r_0$, $z \leq r_0$

Vypočítame maticu $R \leftarrow a^T b \otimes 1_{p,p}$

Určíme maticu T poskladanú z $r_0 \times r_0$ cirkulantných matic tak, aby váha každého riadku aj stĺpca bola w_t a aby $rank(R+T) = r$

$Q \leftarrow R + T$

Pozn. $r_0 = n_0 - k_0$, $1_{p,p}$ *- matica* $p \times p$ *samé jednotky,* $\otimes$ *- Kroneckerov súčin*

Maticu S určíme ako náhodnú maticu poskladanú z $n_0 \times n_0$ 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 $H' = Q^{-1} H S^{-1}$. Spôsob, ktorým počítame matice Q a S zachovávajú QC vlastnosti pôvodnej matice H, čo nám umožnuje zmenšenie veľkosti verejného kľúča.
Pri generovaní musíme riešiť podobný problém ako pri CFS schéme. Potrebujeme výstup z hashovacej funkcie transformovať na vektor, ktorý spĺňa podmienky určené štruktúrou kódu. Prepokladajme, že máme funkciu ϕ, ktorá jednoznačne priradí vektoru dĺžky l vektor dĺžky r s váhou w a funkciu ψ, ktorá pre každú správu m vyberie kódové slovo s nízkou váhou w_c z kódu generovaného maticou G. Generovanie podpisu je opísane v nasledovnom algoritme.
Overenie podpisu je rýchle a prebieha takto.

3.4.1 Ukážkový príklad

Pre lepšiu predstavu ako LDGM podpisová schéma funguje si predvedieme generovanie, podpisovanie a overenie na príklade. Hodnoty parametrov použité v príklade sú odlišné od hodnôt vhodných pre praktické využitie.

Generovanie kľúčov Majme kód $C(15, 9)$ s kontrolnou maticou H v systematickom tvare

Algoritmus 9 Podpis v LDGM

Vstup: Správa m

Výstup: Podpis správy m, ozn. sig

Vypočítame odtlačok správy m
$h \leftarrow H(m)$
$i \leftarrow 0$, $|h| + |i| = l$
repeat
  $s \leftarrow \phi(h||i)$
  $b_1 \leftarrow b \otimes 1_{1,p}$
  if $b_1 s \neq 0$ **then**
    $i \leftarrow i + 1$
  end if
until $b_1 s = 0$
$s' \leftarrow Qs$
$e \leftarrow [0_{1,k}||s'^{\mathrm{T}}]$
$c \leftarrow \psi(m)$
$e' \leftarrow (e + c)S^T$
$sig \leftarrow (e', i)$
return sig

Pozn. $0_{1,k}$ *- nulový vektor dĺžky k*

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Rozmer cirkulantných matíc je $p \times p$, $p = 3$, $n_0 = 5$, $r_0 = 2$.
Ďalej vypočítame maticu Q. Matica Q je tvorená ako súčet matíc R a T. Na výpočet matice R zvolíme matice a, b s rozmermi $z \times r_0$, kde $z \leq r_0$.

$$a = \begin{bmatrix} 1 & 0 \end{bmatrix}$$

$$b = \begin{bmatrix} 0 & 1 \end{bmatrix}$$

Algoritmus 10 Overenie v LDGM

Vstup: Správa m, podpis (e', i)

Výstup: True/False - podpis prijímame/zamietame

  if $wt(e') \leq (w_t w + w_c)w_s$ **then**

    return False

  else

    $s \leftarrow \phi(H(m)||i)$, $wt(s) = w$

    if $wt(s) \neq w$ **then**

      return False

    else

      $s_1 \leftarrow H'e'^{\mathrm{T}}$

      return $s = s_1$

    end if

  end if

Matica $R = (a' \times b) \otimes 1_{p,p}$

$$R = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Maticu T vyberáme tak, aby sa skladala z $r_0 \times r_0$ cirkulatných blokov, váha každého stĺpca a riadku bola w_t a hodnosť $R + T$ bola $r = r_0 p$. Zvolme $w_t = 1$.

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Matica S je regulárna matica tvorená z $n_0 \times n_0$ cirkulatných blokov, každý stĺpec a riadok má hodnosť w_s. Nech $w_s = 1$, potom matica S môže vyzerať nasledovne

$$S = \begin{bmatrix} 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \end{bmatrix}$$

Keď máme matice Q a S, môžeme vypočítať maticu $H' = Q^{-1}HS^{-1}$, ktorá tvorí verejný kľúč

$$H' = \begin{bmatrix} 0&1&1&0&0&1&1&0&0&1&1&1&0&1&1 \\ 1&0&1&1&0&0&0&1&0&1&1&1&1&0&1 \\ 1&1&0&0&1&0&0&0&1&1&1&1&1&1&0 \\ 1&0&0&0&0&0&0&0&0&0&1&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&1&1&0&0 \\ 0&0&1&0&0&0&0&0&0&1&0&0&0&1&0 \end{bmatrix}$$

Vytvorenie podpisu Predpokladajme, že máme správu m, pre ktorú je výstup z funkcie ϕ vektor s váhou w

$$s = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}^{\mathrm{T}} \qquad w = 2$$

Ďalej vypočítame $s' = Q \cdot s$

$$s' = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}^{\mathrm{T}}$$

Vektoru s' zodpovedá chybové slovo v tvare $e = [0_{1\times k}, s'^{\mathrm{T}}]$

$$e = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Predstavme si, že funkcia $\psi(m)$ vyberie kódové slovo c s váhou $w_c = 4$ pre správu m

$$c = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Posledný krok podpisu je výpočet $e' = (e + c) \cdot S^{\mathrm{T}}$

$$e' = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Podpis tvorí dvojica (e', i). V tomto príklade však i neuvádzame.

Overenie podpisu Ako prvé overíme, či $wt(e') \leq (w_t \cdot w + w_c) \cdot w_s$. V našom príklade $w_t = 1$, $w = 2$, $w_c = 4$ a $w_s = 1$. Potom $6 \leq (1 \cdot 2 + 4) \cdot 1$, $6 \leq 6$ Prvá podmienka je splnená. Ďalej pomocou verejného kľúča zrekonštruujeme odtlačok správy $s_0 = H' \cdot e'^{\mathrm{T}}$

$$s_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}^{\mathrm{T}}$$

Vidíme, že $s = s_0$ a podpis teda akceptujeme.

3.5 Porovnanie

Pozrime sa na porovnanie CFS a LDGM schémy.

Tabuľka 2: Porovnanie CFS a LDGM schémy

	CFS	**LDGM**
Velkosť VK	$n - k \times n$	$(n - k \times n)/p$
Veľkosť PK	$n - k \times n - k, n - k \times n, n \times n$	$(n - k \times n, n - k \times n - k, n \times n)/p$
Veľkosť podpisu	n	n

Vidíme, že pri rovnakých parametroch kódu LDGM schéma ponúka p-násobnú úsporu pamäte. Treba však podotknúť, že kódy použité v každej schéme sa líšia a z praktického hľadiska sa volia iné hodnoty parametrov.

3.6 Návrh implementácie pre LDGM

V tejto časti navrhneme implementáciu LDGM podpisovej schémy a predstavíme konkrétne algoritmy na generovanie kľúčov, podpisov a overovacie funkcie.

3.6.1 Voliteľné parametre

Zhrňme si najskôr všetky voliteľné parametre a funkcie pre celú podpisovú schému LDGM

Tabuľka 3: Parametre a funkcie LDGM

Parameter	**Popis**
n	dĺžka kódu ($n_0 p$)
k	dimenzia kódu ($k_0 p$)
t	počet opraviteľných chýb
p	veľkosť cirkulantných matíc
z	počet riadkov matice a,b pozn. ($z \leq (n-k)$)
w_t	váha riadku/stĺpca matice T
w_s	váha riadku/stĺpca matice S
w_c	váha slova c, ktoré určuje funkcia ψ
ψ	funkcia, ktorá jednoznačne priradí správe m kódové slovo c
ϕ	funkcia, ktorá zobrazuje slová dĺžky x na vektory dĺžky y s váhou z

3.6.2 Funkcia ϕ

Prvou dôležitou súčasťou pre celú implementáciu, je zvoliť funkciu ϕ, ktorá jednoznačne mapuje vektor dĺžky n na vektor dĺžky l s váhou t a má inverziu. Pre tento účel zvolíme algoritmus, ktorý navrhol Sendrier v [xx], ktorý má lineárnu zložitosť. Implementácia (mierne upravená pre naše potreby) a jej inverzia vyzerá nasledovne.

Algoritmus 11 Funkcia ϕ

Vstup: Vektor dĺžky n, parameter t

Výstup: Vektor dĺžky l s váhou t

Algoritmus 12 Funkcia ϕ^{-1}

Vstup: Vektor dĺžky l, parameter n, parameter t

Výstup: Vektor dĺžky n

3.6.3 Funkcia ψ

3.6.4 Generovanie matice Q

Ako bolo uvedené v predošlej časti, matica Q sa skladá z matíc R a T, ktoré su blokovo cirkulantné. Matica R vznikne ako produkt $a^T b \otimes 1_{p,p}$, matice a, b náhodne vygenerujeme v závislosti od parametra z. Matica T sa skladá z cirkulantných matíc s rozmerom $p \times p$. A váha každého riadku a stĺpca je w_t, nepárne. Uvedieme si algoritmus na generovanie matice T.

Algoritmus 13 Generovanie regulárnej matice z cirkulantných blokov

Vstup: Počet cirkulantných blokov - r_0, veľkosť bloku - p, predpísaná váha w_t

Výstup: Regulárna matica z cirkulatných blokov s predpísanou váhou riadkov a stĺpcov

Vytvorime riadok z blokov tak, aby prvy blok bol jednotkova matica, zvysok su bloky s parnou vahou

Ostatne riadky vytvorime posuvanim blokov z prveho "riadku"

Dostaneme na diagonale jednotkove matice, zvysok matice s parnym poctom jednotiek

Premiesame blokovo riadky a stlpce

Ak súčet R+T nie je regulárna matica, skúsime vygenerovať T znova.

Záver

Zaver SK

Resumé

Resume SK

Zoznam použitej literatúry

Prílohy