Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Plne homomorfné šifrovacie schémy

2011

Jakub Vaňo

Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Plne homomorfné šifrovacie schémy

bakalárska práca

Študijný program:	Informatika
Študijný odbor:	2508 Informatika
Školiace pracovisko:	Katedra Informatiky
Školiteľ:	doc. RNDr. Martin Stanek PhD.

Bratislava, 2011

Jakub Vaňo

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Jakub Vaňo
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: 9.2.1. informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský

Názov: Plne homomorfné šifrovacie schémy

Cieľ: Naštudovať návrhy aktuálnych schém realizujúcich plne homomorfné šifrovanie. Porovnať ich vlastnosti z hľadiska kryptoanalytickej odolnosti, výkonu a praktickej použiteľnosti.

Vedúci: doc. RNDr. Martin Stanek, PhD.

Dátum zadania: 05.10.2011

Dátum schválenia: 10.10.2011

doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

.....
študent

.....
vedúci

Abstrakt

V tejto práci predstavujeme niektoré z plne homomornfých šifrovacích schém z hľadiska kryptoanalytickej odolnosti, výkonu a praktickej použiteľnosti. Konkrétne sa zameriavame na Gentryho plne homomorfnú schému nad mriežkami, chimérickú schému prezentovanú Gentrym a Halevim, a schému založenú na škálovaní rozsahu prezentovanú Brakerskim, Gentrym a Vaikuntanathanom.

Kľúčové slová: plne homomorfné šifrovanie, FHE, bootstrapping, škálovanie rozsahu, chimérická schéma

Abstract

In this work we present some of fully homomorphic encryption schemes, with focus on security, performance and practical application. Specifically, we describe Gentrys fully homomorphic encryption scheme over ideal lattices, chimeric scheme published by Gentry and Halevi, and encryption scheme based on modulus scaling published by Brakerski, Gentry and Vaikuntanathan.

Keywords: fully homomorphic encryption, FHE, bootsrapping, modulus scaling, chimeric scheme

Obsah

Úvod

Idea plne homomorfnej šifrovacej schémy sa objavila už pri vzniku RSA schémy a je pomerne prirodzená: chceme šifrovaciu schému, ktorá nielen bezpečne utají obsah dát pred neoprávneným prístupom, ale zároveň umožní na zašifrovaných dátach vykonávať ľubovoľné operácie bez odhalenia skrytej informácie.

Samotná RSA schéma je multiplikatívne homomorfná, t.j. ak máme k dispozícii c_1, c_2 – zašifrované podoby čísel m_1, m_2 – dokážeme získať zašifrovanú podobu $m_1 \cdot m_2$ len za pomoci verejne známych informácií. Viacero známych schém je homomorfných na jednu operáciu. Napríklad El Gamal-ova schéma je multiplikatívne homomorfná a Palierov systém je aditívne homomorfný. Dlho však neexistovala bezpečná šifrovacia schéma homomorfná vzhľadom na sčítanie aj násobenie, pričom existuje mnoho potenciálnych aplikácií. Jedným z príkladov uplatnenia plne homomorfného šifrovania by mohol byť bezpečný cloud-computing.[1] Používateľ by poskytol zašifrované dáta, na ktorých by mohol cloud pracovať bez možnosti odhalenia utajených dát.

Hlavným problémom homomorfných schém je ich bezpečnosť, keďže schopnosť homomorfne pracovať so šifrovými textami otvára možnosti útoku na tieto schémy. Napríklad žiadna homomorfná schéma nemôže byť IND-CCA2 bezpečná.[2] Boneh a Lipton [BL96] ukázali, že každú algebraicky homomorfnú schému je za rozumných predpokladov možné zlomiť v subexponenciálnom čase.

Prvú bezpečnú, skutočne plne homomorfnú šifrovaciu schému [Gen09a, Gen09b] skonštruoval Craigh Gentry v roku 2009, čo znamenalo prelom v tejto oblasti. Jeho postup spočíval v konštrukcii čiastočne homomorfnej schémy, ktorú po istej modifikácii dokázal pomocou tzv. bootstrappingu rozšíriť na plne homomorfnú schému. Následne boli prezentované viaceré optimalizácie Gentryho schémy, ako aj iné schémy, ktoré ale využívali rovnaký, Gentrym navrhnutý postup konštrukcie.

[1] Aj keď Dijk a Juels [VDJ10] argumentujú, že ani ideálne plne homomorfné šifrovanie na tento účel úplne nepostačuje.

[2] t.j. mať nerozlíšiteľné šifrové texty pri adaptívnom CCA.

Prvým odklonením od tohto postupu bola tzv. chimérická schéma [GH11a] predstavená Gentrym a Halevim. Ich prínosom bol iný prístup k homomorfnému vyhodnocovaniu dešifrovacej funkcie, čo umožnilo odstrániť tzv. squashing fázu konštrukcie prinášajúcu dodatočné bezpečnostné predpoklady.

Ostatným pokrokom bol úplne iný prístup ku konštrukcii plne homomorfnej schémy predstavený Brakerskim, Gentrym a Vaikuntanathanom [BGV11] založený na škálovaní priestoru šifrových textov.

Cieľom tejto práce je poskytnúť čitateľovi prehľad o spôsoboch konštrukcie plne homomorfných schém, prezentovať výpočtové problémy, na ktorých je postavená teoretická bezpečnosť týchto schém, popísať asymtotickú zložitosť a demonštrovať praktickú použiteľnosť týchto schém na existujúcich implementáciách.

V prvej kapitole predstavíme pôvodnú Gentryho schému spolu s rôznymi optimalizáciami a prezentujeme implementáciu tejto schémy. V druhej kapitole prezentujeme myšlienku chimérických schém, a v tretej kapitole popíšeme schému založenú na škálovaní šifrových textov.

Kapitola 1

Schéma nad ideálnymi mriežkami

V tejto kapitole budeme popisovať prvú plne homomorfnú šifrovaciu schému [Gen09a, Gen09b] ktorej autorom je Craigh Gentry. Najprv definujeme pojmy plne homomorfnej a stupňovito plne homomorfnej schémy. Následne popíšeme čiastočne homomorfnú schému a predstavíme bootstrapping – základnú myšlienku Gentryho konštrukcie, pomocou ktorej skonštruujeme stupňovito plne homomorfnú schému. Na záver analyzujeme výkon a uvedieme optimalizácie a implementácie tejto schémy. .

Pre tento text podstatné definície a tvrdenia o mriežkach možno nájsť v prílohe. Všetky vety, lemy a asymtotické odhady zložitosti uvedené v tejto kapitole sú prebraté z Gentryho prác [Gen09a, Gen09b]

1.1 Definície pojmov

Definícia 1. *Homomorfná šifrovacia schéma* ξ *je* 5*-tica* $(KeyGen_\xi, E_\xi, D_\xi, Eval_\xi, \lambda)$*, kde:*

- $\lambda \in \mathbb{N}$ *je bezpečnostný parameter*
- $KeyGen_\xi(1^\lambda) \to (\mathcal{P}_\xi, \mathcal{C}_\xi, pk, sk)$ *je znáhodnený polynomiálny algoritmus pre generovanie okruhu otvorených textov* $\mathcal{P}$*, okruhu šifrových textov* $\mathcal{C}$*, verejného kľúča* pk *a súkromného kľúča* sk*.*
- $E_\xi(pk, m) \to c$ *je znáhodnený polynomiálny šifrovací algoritmus,* $m \in \mathcal{P}_\xi, c \in \mathcal{C}_\xi$
- $D_\xi(sk, c) \to m$ *je polynomiálny dešifrovací algoritmus,* $c \in \mathcal{C}_\xi, m \in \mathcal{P}_\xi$

- $Eval_\xi(pk, O, c_1, \ldots, c_k) \to c$ *je polynomiálny algoritmus,* $c, c_1, \ldots, c_k \in \mathcal{C}$*,* O *je obvod nad* $\mathcal{P}_\xi$*.* [1]

Definícia 2. *Hovoríme, že homomorfná schéma* ξ *je korektná, ak pre ľubovoľné* $(\mathcal{P}_\xi, \mathcal{C}_\xi, pk, sk) \leftarrow KeyGen_\xi(1^\lambda)$ *platí:*
$\forall c \in \mathcal{C}_\xi, m \in \mathcal{P}_\xi : c \leftarrow E_\xi(pk, m) \Rightarrow D_\xi(sk, c) = m$

Intuitívne, algoritmus $Eval_\xi$ homomorfne, pomocou operácií na šifrových textoch, vyhodnocuje obvod pracujúci nad otvorenými textami.

Definícia 3. *Množina prípustných obvodov* $\mathcal{O}_\xi$ *je množina tých obvodov, ktoré je* ξ *schopná homomorfne vyhodnotiť.*
$\mathcal{O}_\xi = \{O \mid \forall m_1, \ldots, m_k \in \mathcal{P}_\xi : D_\xi(Eval_\xi(O, E_\xi(m_1), \ldots, E_\xi(m_k))) = O(m_1, \ldots, m_k)\}$
Hovoríme, že ξ *je korektná pre obvody z* $\mathcal{O}_\xi$*.*

Definícia 4. *Schéma* ξ *je plne homomorfná, ak je korektná pre všetky obvody nad* $\mathcal{P}_\xi$*. Plne homomorfnú schému budeme skrátene označovať FHE (fully homomorphic encrytpion).*

Uvidíme, že analyzovaná schéma (ako aj schémy v nasledujúcich kapitolách) sú konštruované stupňovitým spôsobom, t.j. z čiastočne homomorfnej schémy vieme pre ľubovoľné d skonštuovať schému ξ^d korektnú pre obvody s hĺbkou najviac d. Takáto konštrukcia ale nevyhovuje definícii plne homomorfnej schémy, preto zavedieme o čosi voľnejší pojem stupňovito plne homomorfnej schémy.

Definícia 5. *Trieda schém* $\{\xi^d \mid d \in \mathbb{N}\}$ *s rovnakým parametrom* λ *a* $KeyGen$ *algoritmami generujúcimi rovnaký okruh otvorených textov* $\mathcal{P}$ *je stupňovito plne homomorfná, ak každá schéma* ξ^d *je korektná pre všetky obvody nad* $\mathcal{P}$ *hĺbky najviac* d *a všetky jej algoritmy majú zložitosť polynomiálnu od* λ, d *a (v prípade* $Eval_{\xi^d}$*) veľkosti vyhodnocovaného obvodu.*

1.2 Označenia

Podrobnejší popis označení, respektíve zdôvodnenie platnosti niektorých vzťahov možno nájsť v prílohe v časti o mriežkach.

[1] V texte pod obvodom O nad okruhom R budeme rozumieť obvod $O : R^k \to R$ pre nejaké $k \in N$ skladajúci sa z hradiel realizujúcich operácie súčtu, súčinu a inverzného prvku v okruhu R.

Budeme používať okruh $R = \mathbb{Z}[x]/(f(x))$, kde $f(x)$ je monický ireducibilný polynóm stupňa n. Na prvky tohto okruhu sa budeme pozerať ako na vektory v $\mathbb{Z}^n$, alebo ako na polynómy stupňa $n-1$.

$\gamma_{Mult}(R)$ budeme označovať konštantu prislúchajúcu k okruhu R takú, že $\forall \vec{u}, \vec{v}$: $|\vec{u} \cdot \vec{v}| \leq |\vec{u}| \cdot |\vec{v}| \cdot \gamma_{Mult}(R)$. Vhodnou voľbou $f(x)$ vieme dosihnuť $\gamma_{Mult}(R)$ polynomiálne od stupňa $f(x)$. Napríklad pre $f(x) = x^n \pm 1$ je $\gamma_{Mult}(R) = \sqrt{n}$.

$\mathcal{B}(r)$ označuje guľu s polomerom r, t.j. $\mathcal{B}(r) = \{\vec{v} \in R \mid |\vec{v}| \leq r\}$. Ak J je mriežka v R s bázou $B = \{\vec{b}_1, \ldots, \vec{b}_n\}$, tak $P(B)$ označuje polootvorený rovnobežnosten $P(B) = \{a_1\vec{b}_n + \ldots + a_n\vec{b}_n \mid a_1, \ldots a_n \in \langle -1/2, 1/2)\}$.

Pod onačením $\log x$ budeme rozumieť $\log_2 x$. Ak $\vec{x} \in \mathbb{R}^n$, tak výsledkom operácií $\lceil \vec{x} \rfloor$, $\lceil \vec{x} \rceil$, resp. $\lfloor \vec{x} \rfloor$, bude vektor s koeficientami zaokrúhlenými na najbližšie, najbližšie väčšie, resp. najbližšie menšie celé číslo.

Pre bázu B ideálnej mriežky $J \subseteq R$ a $\vec{v} \in R$ definujeme $\vec{v} \bmod B = \vec{u}$, tak, že $\vec{v} - \vec{u} \in J$ a $\vec{u} \in P(B)$. $\vec{v} \bmod B$ vieme efektívne rátať ako $\vec{v} - \lceil \vec{c} \cdot B^{-1} \rfloor \cdot B$.

1.3 Čiastočne homomorfná schéma

Popíšeme konštrukciu čiastočne homomorfnej schémy ξ_1, ktorá bude schopná vyhodnocovať obvody určitej hĺbky.

Jednou z paradigiem – fungujúcou aj pre iné čiastočne homomorfné schémy – je pozerať sa na šifrový text ako na objekt skladajúci sa zo "skrývajúcej" časti a tzv. šumu. Na základe súkromného kľúča vieme oddeliť tieto dve časti, a zo šumu vieme vyextrahovať otvorený text. Potom pri sčítavaní, resp. násobení šfrových textov sa veľkosť šumu zväčšuje, pričom korektnosť dešifrovania je podmienená veľkosťou šumu - ak tá presiahne určitú hranicu, nevieme korektne dešifrovať.

Čiastočne homomorfné schémy sú stavebným kameňom plne homomorfných schém, ktoré navyše zavádzajú nejakú techniku redukcie šumu: transformáciu jedného šifrového textu na iný, šifrujúci rovnaký otvorený text, ale s menším šumom.

V našom prípade bude šifrovým textom vektor $\vec{c} \in R$, ktorý môžme rozložiť na $\vec{c} = \vec{e} + \vec{j}$, kde $\vec{e}$ predstavuje šum a $\vec{j}$ je najbližší vektor v ideálnej mriežke $J \subseteq R$. Súkromným a verejným kľúčom budú dve bázy B_J^{pk}, B_J^{sk}, pričom B_J^{sk} je "dobrá" báza, t.j. $\vec{c} \bmod B_J^{sk} = \vec{e}$, zatiaľ čo B_J^{pk} je "zlá" báza: dostatčne popisuje mriežku, ale nevieme s ňou efektívne rátať najbližšie vektory.

Generovanie kľúča:[2]

1. Vygenerujeme ireducibilný monický polynóm $f(x) \in \mathbb{Z}[x]$ a okruh $R = \mathbb{Z}[x]/(f(x))$.
2. Vygenerujeme $\vec{s} \in R$ definujúci hlavný ideál $I = (\vec{s})$. Označíme rotačnú bázu prislúchajúcu k $\vec{s}$ ako B_I. Položíme $P_{\xi_1} \subseteq P(B_I)$ a $\mathcal{C}_{\xi_1} = R$.
3. Vygenerujeme ideál $J \subseteq R$ tak, aby $J + I = \{\vec{j} + \vec{i} \mid \vec{j} \in J, \vec{i} \in I\} = R$, a dve bázy prislúchajúcej mriežky B_J^{sk} a B_J^{pk}.
4. Zvolíme $l_{max} \in \mathbb{R}^+$.
5. Položíme $KeyGen_{\xi_1}(1^\lambda) \to (\mathcal{P}_{\xi_1}, \mathcal{C}_{\xi_1}, pk = (B_I, B_J^{pk}, l_{max}), sk = B_J^{sk})$.

Šifrovanie:

1. Rovnomerne náhodne vygenerujeme vektor $\vec{r} \in \mathcal{B}(l_{max})$
2. Položíme $Err_{\xi_1}(pk, \vec{m}) = \vec{m} + \vec{r} \cdot \vec{s}$.
3. $E_{\xi_1}(pk, \vec{m}) = Err_{\xi_1}(pk, \vec{m}) \bmod B_J^{pk}$.

Dešifrovanie: $D_{\xi_1}(sk, \vec{c}) = (\vec{c} \bmod B_J^{sk}) \bmod B_I$

Homomorfné vyhodnocovanie:

Pri homomorfnom vyhodnocovaní sa budeme zaoberať obvodmi nad R/I, kde jednotlivé triedy reprezentujeme prvkami z $P(B_I)$. Teda

$$\mathcal{O}_{\xi_1} \subseteq \{O : P(B_I) \to P(B_I)\}$$

kde obvody sa skladajú z hradiel ($k, l \geq 2$ sú počty vstupov hradla):

$$Add_{B_I}(\vec{m_1}, \ldots, \vec{m_k}) = (\vec{m_1} + \ldots + \vec{m_2}) \bmod B_I$$
$$Mult_{B_I}(\vec{m_1}, \ldots, \vec{m_l}) = (\vec{m_1} \cdot \ldots \cdot \vec{m_2}) \bmod B_I$$

Zavedieme pojem generalizovaného obvodu, ktorý budeme využívať pri homomorfnom vyhodnocovaní.

Definícia 6. *Ak O je obvod nad R/I, potom obvod, ktorý získame nahradením hradiel Add_{B_I}, resp. $Mult_{B_I}$ za hradlá realizujúce súčet, resp. súčin v R nazývame generalizovaný obvod, označujeme $g(O)$.*

Potom $Eval_{\xi_1}(pk, O, \vec{c_1}, \ldots, \vec{c_k}) = g(O)(\vec{c_1}, \ldots, \vec{c_k}) \bmod B_J^{pk}$.

[2]Konkrétne parametre ako napríklad voľba $f(x)$ či $\vec{s}$ špecifikujeme pri prezentácii konkrétnej implementácie.

1.3.1 Korektnosť

Definícia 7. *Pre vyššie popísanú schému ξ_1 označíme veľkosť prvotnej odchýlky šifrového textu od mriežky J ako $r_E = min\{l \in \mathbb{R} \mid Im_{Err_{\xi_1}} \subseteq \mathcal{B}(l)\}$ a veľkosť maximálnej prípustnej odchýlky $r_D = max\{r \in \mathbb{R} \mid \mathcal{B}(r) \subseteq P(B_J^{sk})\}$.*

Teda veľkosť šumu v "čerstvom" šifrovom texte – šifrovom texte ktorý je výstupom E_{ξ_1} – je nanajvýš r_E, a r_D označuje "kritickú" veľkosť šumu, t.j. po prekročení tejto hranice už dešifrovanie nemusí byť korektné.

Veta 1. *Ak $r_E \leq r_D$, potom je schéma ξ_1 korektná.*

Dôkaz. Zrejme $E_{\xi_1}(pk, \vec{m}) = Err_{\xi_1}(\vec{m}) + \vec{j}$ pre nejaký $\vec{j} \in J$. Ak $r_E \leq r_D$, tak $Err_{\xi_1}(\vec{m}) \in P(B_J^{sk})$ a teda

$(E_{\xi_1}(pk, \vec{m}) \bmod B_J^{sk}) \bmod B_I = Err_{\xi_1}(\vec{m}) \bmod B_I = \vec{m}$ □

1.3.2 Homomorfnosť schémy

Zrejme $E_{\xi_1}(pk, \vec{m_k}) \to \vec{c_k} = \vec{m_k} + \vec{s} \cdot \vec{r_k} + \vec{j_k} = \vec{m_k} + \vec{i_k} + \vec{j_k}$ pre nejaké $\vec{i_k} \in I, \vec{j_k} \in J$. Nech $\vec{e_k} = \vec{m_k} + \vec{i_k}$, potom z vlastností ideálov vyplýva ($k \in \{1, 2\}$):

$$\vec{c_1} + \vec{c_2} = \underbrace{(\vec{m_1} + \vec{m_2}) + (\vec{i_1} + \vec{i_2})}_{e_{1+2}} + (\vec{j_1} + \vec{j_2})$$

$$\vec{c_1} \cdot \vec{c_2} = \underbrace{(\vec{m_1} \cdot \vec{m_2}) + (\vec{m_1} \cdot \vec{i_1} + \vec{m_2} \cdot \vec{i_1} + \vec{i_1} \cdot \vec{i_2})}_{e_{1 \cdot 2}} + (\vec{e_1} \cdot \vec{j_1} + \vec{e_2} \cdot \vec{j_1} + \vec{j_1} \cdot \vec{j_2})$$

Teda pokiaľ $e_{1+2} \leq r_D$, resp. $e_{1 \cdot 2} \leq r_D$, potom $D_{\xi_1}(sk, c_1 + c_2) = m_1 + m_2$, resp. $D_{\xi_1}(sk, c_2 \cdot c_2) = m_1 \cdot m_2$.

Vidíme teda, že ξ_1 je korektná pre nejaký obvod O, ak pri jeho homomorfnom vyhodnocovaní nepresiahne veľkosť šumu v šifrových textoch r_D. Nasledujúca veta špecifikuje prípustné obvody na základe ich hĺbky.

Veta 2. *Ak O je obvod nad R/I, jeho Add_{B_I} hradlá majú počet vstupov $\gamma_{Mult}(R)$, $Mult_{B_I}$ hradlá majú počet vstupov 2, a jeho hĺbka je nanajvýš*

$$\log\log r_D - \log\log(\gamma_{Mult}(R) \cdot r_E)$$

potom $O \in \mathcal{O}_{\xi_1}$

Dôkaz. Nech $\vec{m_1}, \ldots, \vec{m_k} \in \mathcal{P}_{\xi_1}$, $Err_{\xi_1}(pk, \vec{m_i}) \to \vec{e_i}$.

Budeme vyhodnocovať obvod $g(O)(\vec{e_1}, \ldots, \vec{e_k})$, zrejme má rovnakú hĺbku ako O, označme d. Označíme maximálnu veľkosť výstupu hradla na i-tej úrovni r_i, zrejme $r_0 = r_E$.

Keďže $|\vec{u}+\vec{v}| \leq |\vec{u}|+|\vec{v}|$, tak veľkosť výstupu súčtového hradla na úrovni $i+1$ je nanajvýš $\gamma_{Mult}(R) \cdot r_i$. Keďže $|\vec{u} \cdot \vec{v}| \leq \gamma_{Mult}(R) \cdot |\vec{u}| \cdot |\vec{v}|$, tak veľkosť výstupu súčinového hradla na úrovni $i+1$ je nanajvýš $\gamma_{Mult}(R) \cdot r_i^2$. Teda

$$r_{i+1} \leq \gamma_{Mult}(R) \cdot r_i^2$$

Keďže $r_0 = r_E$, tak

$$r_i \leq \gamma_{Mult}(R)^{2^i-1} \cdot r_E^{2^i} \leq (\gamma_{Mult}(R) \cdot r_E)^{2^i}$$

A pre $i \leq d$

$$\begin{aligned} r_i &\leq (\gamma_{Mult}(R) \cdot r_E)^{2^{\log\log r_D - \log\log(\gamma_{Mult}(R)\cdot r_E)}} \\ r_i^{\log(\gamma_{Mult}(R)\cdot r_E)} &\leq (\gamma_{Mult}(R) \cdot r_E)^{\log r_D} \\ \log r_i \cdot \log(\gamma_{Mult}(R) \cdot r_E) &\leq \log r_D \cdot \log(\gamma_{Mult}(R) \cdot r_E) \\ r_i &\leq r_D \end{aligned}$$

To znamená, že počas homomorfného vyhodnocovania O veľkosť odchýlky šifrového textu od mriežky J nikdy neprekročí r_D, a teda $O \in \mathcal{O}_{\xi_1}$. □

Táto veta hovorí, že pre maximalizovanie hĺbky prípustných obvodov potrebujeme maximalizovať podiel r_D/r_E. Ako ukážeme v časti 1.6, pre príliš veľké r_D/r_E shéma nie je bezpečná, preto musíme podiel udržať subexponenciálny, napr $r_D/r_E = 2^{n^c}$, pre $c < 1$, čo umožňuje hĺbku prípustných obvodov $c \cdot \log n$.

Ak chceme maximalizovať r_D, tak potrebujeme, aby $P(B_J^{sk})$ obsahoval guľu s čo najväčším polomerom, čo vieme dosiahnuť napríklad ak za B_J^{sk} zvolíme rotačnú bázu vektora takmer paralelného s $\vec{e_1} = (1, 0, \ldots, 0)$.[3]

Veta 3. *Nech B_J^{sk} je rotačná báza prislúchajúca k vektoru $\vec{v} \in \{t \cdot \vec{e_1} + \vec{r} \mid \vec{r} \in \mathcal{B}(l), t \in \mathbb{Z}\}$. Potom ak $t \geq 4 \cdot n \cdot \gamma_{Mult}(R) \cdot l$ tak $r_D \geq t/4$.*

Hodnotu prvotnej odchýlky môžme ohraničiť

$$r_E = max\{|\vec{m} + \vec{r} \cdot \vec{s}|\} \leq (n \cdot |B_I|) + \gamma_{Mult}(R) \cdot l_{max} \cdot |B_I|$$

Teda minimalizovať r_E môžme zvolením krátkeho $\vec{s}$ – čo implikuje malú veľkosť rotačnej bázy B_I, alebo malého l_{max}.[4]

[3] Ak by sme zvolili B_J^{sk} ako rotačnú bázu vektora $(t, 0, \ldots, 0), t \in \mathbb{Z}$, tak B_J^{sk} je v Hermiteho normálnom tvare (HNF), a teda ju vieme v polynomiálnom čase získať z ľubovoľnej bázy J.

[4] Ako uvidíme v časti 1.6, veľkosť l_{max} ovplyvňuje bezpečnosť schémy, teda nemôže byť ľubovoľne malá.

1.4 Bootstrapping

Skonštruovali sme homomorfnú schému ξ_1, kotrá je schopná vyhodnocovať obvody istej hĺbky. Hlavnou myšlienkou Gentryho konštrukcie je spôsob rozšírenia tejto čiastočne homomorfnej schémy (SWHE - somewhat homomorpic encryption) na plne homomorfnú schému.

Bootstrapping je technika redukcie šumu v šifrovom texte - v našej schéme ξ_1 zodpovedá šumu odchýlka od mriežky J. Ako sme videli, sčítavaním a násobením sa táto odchýlka zväčšuje, a keď presiahne určitú hranicu, tak korektné dešifrovanie nie je možné. Taktiež sme videli, že "čerstvé" šifrové texty – t.j. výstupy E_{ξ_1} – majú túto odchýku pomerne malú.

Pri bootstrappingu redukujeme veľkosť šumu tak, že k šifrovému textu v nejakej inštancii schémy vygenerujeme čerstvý šifrový text v inej inštancii taký, že oba šifrujú rovnaký otvorený text. Tento nový šifrový text generujeme pomocou homomorfného vyhodnotenia dešifrovacieho algoritmu: Zvolíme nejaké kódovanie [5] súkromného kľúča a šifrových textov pomocou prvkov P_{ξ_1} a skonštruujeme obvod $O_{D_{\xi_1}}$ nad R/I realizujúci dešifrovací algoritmus na takto kódovaných vstupoch. Následne zašifrujeme kód šifrového textu a súkromného kľúča v inej inštancii a homomorfne vyhodnotíme $O_{D_{\xi_1}}$.

Definícia 8. *Nech* $(\mathcal{P}_{\xi_1}, \mathcal{C}_1, pk_1, sk_1)$ *a* $(\mathcal{P}_{\xi_1}, \mathcal{C}_2, pk_2, sk_2)$ *sú nejaké inštancie* ξ_1. *Nech* $(\vec{m}_{sk_1,1}, \ldots, \vec{m}_{sk_1,k}) \in \mathcal{P}_{\xi_1}^k$ *je kód* sk_1 *a* $(\vec{m}_{c,1}, \ldots, \vec{m}_{c,l}) \in \mathcal{P}_{\xi_1}^l$ *je kód* $\vec{c} \in \mathcal{C}_1$. *Nech* $E_{\xi_1}(pk_2, \vec{m}_{sk_1,i}) \to \vec{c}_{sk_1,i}$ *a* $E_{\xi_1}(pk_2, \vec{m}_{c,i}) \to \vec{c}_{c,i}$. *Nech* $O_{D_{\xi_1}}$ *je obvod nad* R/I *realizujúci* D_{ξ_1} *na zakódovaných vstupoch, potom definujeme algoritmus prešifrovania:*

$$Recrypt_{\xi_1}(pk_2, (\vec{c}_{sk_1,1}, \ldots, \vec{c}_{sk_1,k}), \vec{c}) = Eval_{\xi_1}(pk_2, O_{D_{\xi_1}}, \vec{c}_{sk_1,1}, \ldots, \vec{c}_{sk_1,k}, \vec{c}_{c,1}, \ldots, \vec{c}_{c,l})$$

Veta 4. *Ak* $O_{D_{\xi_1}} \in \mathcal{O}_{\xi_1}$ *a* $Recrypt_{\xi_1}(pk_2, (\vec{c}_{sk_1,1}, \ldots, \vec{c}_{sk_1,k}), \vec{c}) = \vec{z} \in \mathcal{C}_2$, *potom*

$$D_{\xi_1}(sk_1, \vec{c}) = D_{\xi_1}(sk_2, \vec{z})$$

Dôkaz. Ak $O_{D_{\xi_1}} \in \mathcal{O}_{\xi_1}$, tak

$$\begin{aligned} D_{\xi_1}(sk_2, \vec{z}) &= O_{D_{\xi_1}}(\vec{m}_{sk_1,1}, \ldots, \vec{m}_{sk_1,k}, \vec{m}_{c,1}, \ldots, \vec{m}_{c,l}) \\ &= D_{\xi_1}(sk_1, \vec{c}) \end{aligned}$$

□

[5] Napríklad ak $|\mathcal{P}_{\xi_1}| = k$, tak si očíslujeme prvky v $\mathcal{P}_{\xi_1}$ a budeme kódovať súradnice vektorov v k-árnej sústave.

Označíme obvod skladajúci sa z dvoch $O_{D_{\xi_1}}$ spojených Add_{B_I} resp. $Mult_{B_I}$ hradlom ako $O_{Add_{\xi_1}}$ resp. $O_{Mult_{\xi_1}}$. Ďalej ukážeme, ako pomocou čiastočne homomorfnej schémy schopnej homomorfne vyhodnotiť svoje $O_{Add_{\xi_1}}$ a $O_{Mult_{\xi_1}}$ obvody dokážeme zostrojiť stupňovito plne homomorfnú schému.

Podstatou konštrukcie je pri homomorfnom vyhodnocovaní obvodu nahradiť sčítanie, resp. násobenie šifrových textov $\vec{c}_1, \vec{c}_2$ vyhodnotením $O_{Add_{\xi_1}}$ resp. $O_{Mult_{\xi_1}}$ obvodu, kde vstupmi sú kódy $\vec{c}_1$ a $\vec{c}_2$ zašifrované pod inou inštanciou SWHE schémy. Kvôli tomu potrebujeme pre každú úroveň vyhodnocovaného obvodu novú inštanciu SWHE schémy, čo produkuje stupňovitú FHE.

Veta 5. *Ak ξ_1 je homomorfná schéma taká, že $O_{Add_{\xi_1}}, O_{Mult_{\xi_1}} \in \mathcal{O}_{\xi_1}$, tak existuje stupňovito plne homomorfná trieda schém $\{\xi_1^d | d \in N\}$.*

Dôkaz. Skonštruujeme ξ_1^d nasledovne:

Označíme $\langle sk_i \rangle = (\vec{m}_{sk_i,1}, \ldots, \vec{m}_{sk_i,k}) \in \mathcal{P}_{\xi_1}^k$ kód súkromného kľúča sk_i, $\langle sk_i \rangle_{pk_j}$ kód sk_i po častiach zašifrovaný verejným kľúčom pk_j.

Generovanie kľúča:

1. $KeyGen_{\xi_1}(1^\lambda) \to (\mathcal{P}, \mathcal{C}_i, pk_i, sk_i)$ pre $0 \leq i \leq d$[6]
2. $pk'_i = (pk_i, \langle sk_i \rangle_{pk_{i+1}})$ pre $1 \leq i \leq d-1$
3. $pk = (pk_0, pk'_1 \ldots, pk'_{d-1})$
4. $sk = (sk_0, \ldots, sk_d)$
5. $\mathcal{C} = \{(\vec{c}, i) \mid \vec{c} \in \mathcal{C}_i, 0 \leq i \leq d\}$
6. $KeyGen_{\xi_1^d}(1^\lambda) \to (\mathcal{P}, \mathcal{C}, pk, sk)$

Šifrovanie: $E_{\xi_1^d}(pk, \vec{m}) = (E_{\xi_1}(pk_0, \vec{m}), 0)$

Dešifrovanie: $D_{\xi_1^d}(sk, (\vec{c}, i)) = D_{\xi_1}(sk_i, \vec{c})$

Homomorfné vyhodnocovanie:

Budeme uvažovať obvody nad $\mathcal{P}_{\xi_1}$ s počtom vstupov hradiel 2.

Pri vyhodnocovaní $Eval_{\xi_1^d}(pk, O, (\vec{c}_1, 0), \ldots (\vec{c}_k, 0))$ budeme postupne, po úrovniach priradzovať hodnoty výstupom jednotlivých hradiel.

[6]pre jednoduchosť budeme predpokladať, že $KeyGen_{\xi_1}(1^\lambda)$ generuje vždy rovnaké $\mathcal{P}$, čo môžme bez narušenia bezpečnosti schémy.

Výstupu hradla Add_{B_I} na úrovni $1 \leq i \leq d$ so vstupmi $(\vec{c_1}, i-1)$ a $(\vec{c_2}, i-1)$ priradíme hodnotu $(\vec{c}, i)$, pričom

$$\vec{c} = Recrypt_{\xi_1}(pk_i, \langle s_i \rangle, \vec{c_1}) + Recrypt_{\xi_1}(pk_i, \langle s_i \rangle, \vec{c_2})$$

Analogicky priradíme hodnotu výstupu $Mult_{B_I}$ hradla. Korektnosť takéhoto vyhodnotenia vyplýva z korektnosti schémy ξ_1 pre obvody $O_{Add_{\xi_1}}$ a $O_{Mult_{\xi_1}}$ a polynomiálna zložitosť algoritmov vyplýva z polynomiálnej zložitosti algoritmov ξ_1. □

Ukázali sme, ako pomocou SWHE zostrojiť stupňovitú FHE. Ak by sme navyše predpokladali KDM-bezpečnosť schémy (key dependent messages security), t.j. že zverejnenie $\langle sk_i \rangle_{pk_j}$ nijako nepomôže útokom na schému, potom môžme pre každú úroveň vyhodnocovaného obvodu používať rovnakú inštanciu schémy, čím dostávame plne homomorfnú schému.

1.5 Plne homomorfná schéma

Aby sme dokázali využiť bootstrapping a rozšíriť ξ na stupňovitú FHE, potrebujeme nájsť prípustný O_{D_ξ} realizujúci dešifrovanie. Preto Gentry uviedol dve modifikácie schémy, ktoré zjednodušujú výpočet nutný na dešifrovanie.

1.5.1 Modifikácie

Pri dešifrovaní $D_\xi(sk, \vec{c})$ potrebujeme zrátať

$$(\vec{c} \bmod B_J^{sk}) \bmod B_I$$

čo môžme vyjadriť ako:

$$(\vec{c} - \lceil \vec{c} \cdot (B_J^{sk})^{-1} \rfloor \cdot B_J^{sk}) \bmod B_I$$

Modifikácia 1

Prvou modifikáciou bude zjednodušenie dešifrovacieho výpočtu, na tvar

$$(\vec{c} - \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor) \bmod B_I$$

pre $\vec{v}^{sk} \in J^{-1}$. To síce nezmení hĺbku dešifrovacieho obvodu, keďže násobenie maticou vieme rátať v rovnakej hĺbke ako vektorové násobenie, ale zredukuje veľkosť obvodu, ako aj súkromného kľúča. Cenou za túto optimalizáciu bude zmenšenie

maximálnej prípustnej odchýlky r_D na $r_D/(n^{2.5} \cdot |f| \cdot |B_I|)$, čo ale spôsobí len zanedbateľné zmenšenie hĺbky prípustných obvodov. Popíšeme konštrukciu $\vec{v}^{sk}$ ak B_J^{sk} je rotačná báza.

Ak B_J^{sk} je rotačná báza prislúchajúca k vektoru $\vec{v}$ a označíme $\vec{x} = (\vec{v})^{-1}$, tak podľa Lemy 17 je $(B_J^{sk})^{-1}$ rotačná báza mriežky $J^{-1} \subseteq \mathbb{Q}[x]/(f)$ prislúchajúca k vektoru $\vec{x}$. Keďže $I = (\vec{s})$, označíme $\vec{w} = \vec{x} \cdot \vec{s}$ a B_w rotačnú bázu prislúchajúcu k $\vec{w}$. Zrejme $\mathcal{L}(B_w) \subseteq J^{-1}I = \{\vec{j} \cdot \vec{i} \mid \vec{j} \in J, \vec{i} \in I\} \subseteq J^{-1}$. Položíme $\vec{v}^{sk} = \vec{1} \bmod B_w$ a označíme rotačnú bázu prislúchajúcu k $(\vec{v}^{sk})^{-1}$ ako B'_J.

Vo všeobecnom prípade, keď B_J^{sk} nie je rotačná báza, korý tu nebudeme analyzovať, je náročnejšie získať bázu B_x generujúcu podmriežku J^{-1}. Ak označíme $r'_D = \max\{r \in \mathbb{R} \mid \mathcal{B}(r) \subseteq P(B'_J)\}$, dá sa ukázať, že $r'_D \geq r_D/(n^{2.5} \cdot |f| \cdot |B_I|)$.

Lema 1. *Ak veľkosť odchýlky v šifrovom texte $\vec{c}$ je nanajvýš r'_D, potom*

$$\vec{c} - \lceil \vec{c} \cdot (B_J^{sk})^{-1} \rfloor \cdot B_J^{sk} = \vec{c} - \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot (\vec{v}^{sk})^{-1}$$

Dôkaz. Zrejme $\vec{c} - \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot (\vec{v}^{sk})^{-1} = \vec{c} - \lceil \vec{c} \cdot (B'_J)^{-1} \rfloor \cdot B'_J$.

Keďže odchýlka $\vec{c}$ je nanajvýš r'_D, tak platí $\vec{c} = \vec{e} + \vec{j}, \vec{j} \in J, \vec{e} \in \mathcal{B}(r'_D)$. Keďže $\mathcal{B}(r'_D) \subseteq P(B_J^{sk})$, tak $\vec{e}$ je dané jednoznačne a

$$\vec{e} = \vec{c} - \lceil \vec{c} \cdot (B_J^{sk})^{-1} \rfloor \cdot B_J^{sk}$$

Keďže $\vec{v}^{sk} \in J^{-1}$, tak $\mathcal{L}((B'_J)^{-1}) \subseteq J^{-1}$ a teda $\mathcal{L}(B'_J) = \mathcal{L}((B'_J)^{-1})^{-1} \supseteq J$, teda $\vec{j} \in \mathcal{L}(B'_J)$. Keďže $\mathcal{B}(r'_D) \subseteq P(B'_J)$ platí:

$$\vec{e} = \vec{c} - \lceil \vec{c} \cdot (B'_J)^{-1} \rfloor \cdot B'_J$$

□

Potrebujeme ešte ukázať, že z dešifrovacej rovnice môžme "vynechať" $(\vec{v}^{sk})^{-1}$, teda že

$$\lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot (\vec{v}^{sk})^{-1} \equiv \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \bmod B_I$$

Keďže $J + I = R$, tak existuje $\vec{j} \in J \cap (\vec{1} + I)$. Nech $\vec{r} = \vec{j} \cdot \vec{v}^s k$. Keďže $\vec{v}^{sk} \in J^{-1}$, tak $\vec{r} \in R$. Navyše, keďže $\vec{v}^{sk} \in 1 + J^{-1}I$, tak $\vec{r} \in 1 + I$. Keďže $\lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot (\vec{v}^{sk})^{-1} \in R$ (korektnosť dešifrovania), tak platí:

$$\begin{aligned} \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot (\vec{v}^{sk})^{-1} &\equiv \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot (\vec{v}^{sk})^{-1} \cdot \vec{r} \bmod B_I \\ &\equiv \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \cdot \vec{j} \bmod B_I \\ &\equiv \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor \bmod B_I \end{aligned}$$

Modifikácia 2

Cieľom tejto modifikácie bude zabezpečiť, aby vektory získané pri dešifrovaní operáciou $\vec{c}\cdot\vec{v}^{sk}$ mali koeficienty blízke celým číslam. To umožní rátať pri dešifrovaní len s malým počtom zlomkových miest, čo bude nevyhnutné pri homomorfnom dešifrovaní. Aby sme to dosiahli, opäť obmedzíme maximálnu prípustnú odchýlku šifrového textu z r'_D na $r'_D/2$. Obmedzenie hĺbky prípustných obvodov bude opäť zanedbateľné.

Lema 2. *Nech B je báza mriežky plnej dimenzie, nech $\mathcal{B}(k\cdot r) \subseteq P(B), r \in \mathbb{R}, k \geq 1$. Nech $\vec{t} \in \mathcal{B}(r)$. Potom koeficienty $\vec{v} = \vec{t}\cdot B^{-1}$ patria do intervalu $\langle -1/2k, 1/2k)$.*

Dôkaz. Nech $\vec{v} = (v_1, \ldots, v_n)$, nech $\vec{b}_1, \ldots, \vec{b}_n$ sú bázové vektory B. Ak $k > 1$, tak najprv zväčšíme koeficienty $\vec{t}$ k-krát. Teda BÚNV $k = 1$.

Potom $\vec{t} = \vec{v}\cdot B = v_1\vec{b_1} + \ldots + v_n\vec{b}_n$. Keďže $\vec{t} \in P(B)$, z definície $P(B)$ vyplýva, že $\forall i : v_i \in \langle -1/2, 1/2)$. □

Ak odchýlka šifrového textu $\vec{c}$ je menšia než $r'_D/2$, t.j. $\vec{c} = \vec{e}+\vec{j}, \vec{e} \in \mathcal{B}(r'_D/2), \vec{j} \in J$, tak koeficienty

$$\begin{aligned}\vec{c}\cdot\vec{v}^{sk} &= \vec{c}\cdot(B'_J)^{-1} \\ &= \vec{e}\cdot(B'_J)^{-1} + \vec{j}\cdot(B'_J)^{-1}\end{aligned}$$

budú vo vzdialenosti $1/4$ od najbližšieho celého čísla.

Obmedzenie

Pri vyhodnocovaní dešifrovacieho obvodu budeme potrebovať pomocou prvkov $\mathcal{P}_{\xi_2}$ kódovať súkromný kľúč a šifrové texty. Zdá sa, že najefektívnejší spôsob je obmedziť $\mathcal{P}_{\xi_2} = \{0 \bmod B_I, 1 \bmod B_I\}$ a kódovať koeficienty vektorov binárne.[7] Ak by sme použili $I = (\vec{2})$, potom operácie v okruhu R/I priamo zodpovedajú operáciam v $\mathbb{Z}_2$. V opačnom prípade operácia $1 \bmod B_I - \vec{x}\cdot\vec{y}$ pre $\vec{x}, \vec{y} \in \{0 \bmod B_I, 1 \bmod B_I\}$ zodpovedá operácii NAND na príslušných booleovských hodnotách. Keďže pomocou NAND hradla vieme vyskladať základné booleovské operácie, dokážeme ľubovoľný booleovský obvod s konštantým počtom vstupov hradiel simulovať obvodom nad R/I s asymptoticky rovnakou hĺbkou.

[7] Tu notáciou $0 \bmod B_I$ resp. $1 \bmod B_I$ označujeme reprezentanta neutrálneho prvku vzhľadom na ščitovanie resp. násobenie vo faktorovom okruhu R/I

1.5.2 Zložitosť dešifrovacieho obvodu

Pokúsime sa skonštruovať obvod $\mathcal{O}_{D_{\xi_2}} \in \mathcal{O}_{\xi_2}$, t.j. obvod so vstupmi v $\mathcal{P}_{\xi_2}$ a s hradlami realizujúcimi operácie $Add_{B_I}(\vec{m}_1, \ldots, \vec{m}_{\gamma_{Mult}(R)}) = \sum \vec{m}_i \bmod B_I$ a $Mult_{B_I}(\vec{m}_1, \vec{m}_2) = \vec{m}_1 \cdot \vec{m}_2$, ktorý má hĺbku $2^{n^c}, c < 1$ a realizuje D_{ξ_2}, t.j. počíta

$$(\vec{c} - \lceil \vec{c} \cdot \vec{v}^{sk} \rfloor) \bmod B_I$$

kde súradnice vstupných vektorov sú binárne kódované pomocou prvkov $\mathcal{P}_{\xi_2}$.

Autorom schémy sa nepodarilo nájsť požadovaný obvod,[8] preto zaviedli tzv. squashing fázu konštrukcie - pridali do verejného kľúča informáciu o súkromnom kľúči, ktorá zjednoduší dešifrovací obvod za cenu dodatočného bezpečnostného predpokladu.

Najprv uvedieme myšlienku konštrukcie obvodu a ukážeme, prečo nefunguje pre schému ξ_2. Rozdelíme výpočet do troch krokov:

Krok 1: Nájsť $\vec{x_1}, \ldots, \vec{x_n} \in \mathbb{Q}^n : \sum_{i=1}^n \vec{x_i} = \vec{c} \cdot \vec{v}^{sk}$

Krok 2: Z $\vec{x_1}, \ldots, \vec{x_n}$ vyrobiť $\vec{y_1}, \ldots, \vec{y_{n+1}} \in \mathbb{Z}^n : \lceil \sum_{i=1}^n \vec{x_i} \rfloor = \sum_{i=1}^{n+1} \vec{y_i}$

Krok 3: Získať $\vec{m} = (\vec{c} - \sum_{i=1}^{n+1} \vec{y_i}) \bmod B_I$

V časti 1.5.3 ukážeme, že krok 3 vieme realizovať obvodom konštantej hĺbky. V kroku 1 vieme požadované vektory získať čiastočným roznásobením $\vec{x}_i = \vec{c} \cdot v_i x^i$, ak $v_1, \ldots, v_n$ su koeficienty $\vec{v}^{sk}$, v hĺbke $O(\log K)$, ak K je dĺžka binárneho zápisu. Zameriame sa teda na krok 2, ktorý je hlavným problémom pri konštrukcii obvodu pre ξ_2.

Prirodzeným riešením je položiť

$$\vec{y}_i = \lfloor \vec{x}_i \rfloor \qquad 1 \leq i \leq n$$

$$\vec{y}_{n+1} = \lceil \sum_{i=1}^{n} \vec{x}_i - \lfloor \vec{x}_i \rfloor \rfloor$$

čo redukuje krok 2 na zrátanie súčtu n vektorov zo súradnicami v $\langle 0, 1)$, keďže $\vec{x}_i - \lfloor \vec{x}_i \rfloor \in \langle 0, 1)^n$, a zaokrúhlenie koeficientov na najbližšie celé číslo. Vďaka lemme 2 vieme, že súčty jednotlivých súradníc sa budú od najbižšieho celého čísla líšiť nanajvýš o $1/4$, čo znamená, že nám stačí počítať s presnosťou $K = \log n + 2$ bitov.

Lema 3. *Nech $x_1, \ldots, x_n \in \langle 0, 1)$ sú binárne kódované a pre $1 \leq i \leq n$ získame y'_i z y_i zachovaním len prvých $\log n + 2$ zlomkových bitov. Nech $x = \sum_{i=1}^n y_i$ a $y = \sum_{i=1}^n y_i$. Potom ak $x - \lceil x \rfloor \in (-1/4, 1/4)$ tak $\lceil x \rfloor = \lceil y \rfloor$.*

[8] To samozrejme neznamená že taký obvod neexistuje. Dokonca v kapitole 2 uvidíme, že s iným prístupom ku konštrukcii obvodu je možné odstrániť squashing fázu.

Dôkaz. Zrejme $\forall i : x_i - y_i \leq 2^{-(\log n+2)}$, teda $x - y \leq n \cdot 2^{-(\log n+2)} = 1/4$. □

Jedným zo spôsob rátania súčtu K-bitových čísel je použiť tzv. "3 za 2" algoritmus, ktorý v konšantnej hĺbke redukuje súčet troch K-bitových čísel na súčet dvoch (K+1)-bitových čísel, kde prvé číslo je súčet vstupných troch bez prenosov medzi bitmi, a druhé číslo sú prenosy súčtu jednotlivých bitov.

Opakovaným aplikovaním tejto procedúry vieme obvodom hĺbky $O(\log n)$ získať dve $O(\log n + K)$- bitové čísla, ktorých súčet je rovnaký ako súčet pôvodných n čísel. Finálne dve čísla sčítame klasickým sčítavaním s kaskádovým prenosom v hĺbke $O(\log(\log n + K))$, teda celková hĺbka obvodu je $O(\log n)$.

Popísali sme booleovský obvod s konštantým počtom vstupov hradiel, ktorý vieme simulovať obvodom nad R/I s hĺbkou $O(\log n)$. V časti 1.3.2 sme ukázali, že schéma je schopná vyhodnotiť obvody hĺbky $c \cdot \log n$ pre $c < 1$, kým konštanta v zložitosti skonštruovaného algoritmu je väčšia než 1, a teda tento prístup nám nepostačuje.

Iným prístupom k sčítaniu n K-bitových čísel je najprv zrátať súčty cifier na jednotlivých bitoch, čím dostaneme $(\log n + 1)$-bitové čísla $a_1, \ldots, a_K \in \mathbb{Z}$ a následne spočítať

$$\sum_{j=1}^{K} a_j \cdot 2^{-j}$$

Keďže vo finálnej sume sú všetky členy $\log n$-bitové, na jej zrátanie nám stačí obvod hĺbky $O(\log \log n)$. Nech $x_{i,j}, 1 \leq i \leq n, 1 \leq j \leq K$ je j-ty zlomkový bit čísla x_i. Potom

$$a_j = \sum_{i=1}^{n} x_{i,j}$$

Ak $e_k(x_{1,j}, \ldots, x_{n,j})$ je k-ty elementárny symetrický polynóm[9] nad premennými $x_{1,j}, \ldots, x_{n,j}$, a $a_{j,1}, \ldots, a_{j,\log n+1}$ sú bity a_j ($a_{j,1}$ je najmenej významný bit), potom

$$a_{j,k} = e_{2^k}(x_{1,j}, \ldots, x_{n,j})$$

Keďže každý zo symetrických polynómov má stupeň nanajvýš n a určite menej než 2^n členov, vieme ho vyjadriť obvodom s hĺbkou $O(\log n)$, ktorého multiplikatívne hradlá majú konštantný a aditiívne polynomiálny počet vstupov. Opäť však je násobok logaritmu v hĺbke obvodu väčší než 1, avšak oproti "2 za 3" algoritmu má

[9] $e_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k}$

tento prístup výhodu v tom, že elementárne symetrické polynómy nad premennými $x_{1,j}, \ldots, x_{n,j}$ vieme efektívne rátať ako koeficienty polynómu

$$p(z) = (z - x_{1,j}) \cdot \ldots \cdot (z - x_{n,j})$$

čo pomôže zredukovať veľkosť obvodu.

Pri výpočte $a_1, \ldots, a_K$ však narážame na problém – aby sme dosiahli logaritmickú hĺbku, potrebujeme aditívne hradlá s polynomiálnym počtom vstupov, čo zabraňuje simuláciu booleovského obvodu pre $I \neq (\vec{2})$.[10] V tomto prípade získame jednotlivé bity a_j nasledovným spôsobom (ktorý funguje aj pre $I = (\vec{2})$) :

Vstupom pre obvod rátajúci symetrické polynómy sú bity $x_{1,j}, \ldots, x_{n,j}$ reprezentované vektormi $\vec{x}_{1,j}, \ldots, \vec{x}_{n,j} \in \{0_{mod_{B_I}}, 1 \bmod B_I\} = \{\vec{0} \bmod B_I, \vec{1} \bmod B_I\}$. Vyhodnotíme symetrické polynómy pomocou Add_{B_I} a $Mult_{B_I}$ hradiel, pričom ľahko vidno, že ak N je počet $\vec{1} \bmod B_I$ vektorov medzi $\vec{x}_{1,j}, \ldots, \vec{x}_{n,j}$ a označíme $N_k = \binom{N}{k}$ pre $k \in \mathbb{N}$, tak

$$e_k(\vec{x}_{1,j}, \ldots, \vec{x}_{n,j}) = \vec{N}_k \bmod B_I$$

Označíme maticu $M \in \mathbb{Z}^{(n+1)\times(n+1)}$, $M_{i,j} = \binom{\vec{i}}{j} \bmod B_I, 0 \leq i, j \leq n$ a nájdeme maticu $M^* \in \mathbb{Z}^{(n+1)\times(n+1)}$ takú, že $M^*M = I$, kde I je jednotková matica v P_{ξ_2}. Maticu M^* máme predrátanú a teda danú konštantami v konštruovanom obvode. Položíme $\vec{v} \in (R/I)^{n+1} = (e_0(\vec{x}_{1,j}, \ldots, \vec{x}_{n,j}), \ldots, e_n(\vec{x}_{1,j}, \ldots, \vec{x}_{n,j}))$ a zrátame

$$(\vec{c_0}, \ldots, \vec{c_n}) = \vec{v} \cdot M^*$$

Tento výpočet vieme realizovať obvodom hĺbky $O(\log n)$. Zrejme platí, že $\vec{c_i} = \vec{0} \bmod B_I$ pre $i \neq N$ a $c_N = \vec{1} \bmod B_I$. Odtiaľ získame binárnu reprezentáciu $a_j = (\vec{a}_{j,1}, \ldots \vec{a}_{j,\log n+1})$ ako:

$$\vec{a}_{j,k} = \sum_{i=0}^{n} \vec{c_i} \cdot \vec{b_{i,k}}$$

kde $b_i = (\vec{b}_{i,1}, \ldots, \vec{b}_{i,\log n+1}), 0 \leq i \leq n$ je binárna reprezentácia n.

1.5.3 Squashing

Z predchádzajúcej analýzy vyplýva, že hlavným problémom dešifrovania je sčítať n vektorov, na čo potrebujeme hĺbku obvodu $> \log n$, kým korektnosť schémy vieme zaručiť len pre obvody s hĺbkou $c \cdot \log n$ pre $c < 1$.

[10] V časti 1.5.1 sme ukázali ako vieme booleovské hradlá simulovať pomocou NAND operácií simulovaných Add_{B_I} a $Mult_{B_I}$ hradlami, avšak pri tomto všeobecnom spôsobe potrebujeme aj na simuláciu boolovského súčtu hradlo $Mult_{B_I}$, u ktorého máme len konštantný počet vstupov.

Tento problém Gentry vyriešil rozšírením verejného kľúča o množinu vektorov, z ktorých malá časť dáva v súčte $\vec{v}^{sk}$. To umožní rozšíriť šifrový text $\vec{c}$ o množinu vektorov, v ktorej existuje podmnožina so sumou rovnou $\lceil \vec{c} \cdot \vec{v}^{sk} \rfloor$, a teda sčítavať pri dešifrovaní len sublineárne veľa čísel. Na druhej, strane toto rozšírenie prinesie ďalší bezpečnostný predpoklad, a síce že je ťažké získať z danej množiny súkromný kľúč $\vec{v}^{sk}$.

Popíšeme rozšírenú schému ξ_3.

Generovanie kľúča:

1. Vygenerujeme $(\mathcal{P}', \mathcal{C}', pk', sk') \leftarrow KeyGen_{\xi_2}(1^\lambda)$ a zvolíme rovnomerne náhodnú permutáciu $\{a_i\}_{i=1}^{\gamma_{set}(n)}$
2. zvolíme $\gamma_{set}(n) - 1$ vektorov $\vec{v}_{a_2}, \ldots \vec{v}_{a_{\gamma_{set}(n)}} \in \mathbb{Q}^n$, $\vec{v}_{a_1} = \vec{v}^{sk} - \sum_{i=2}^{\gamma_{sub}(n)} \vec{v_{a_i}}$. Označíme množinu vekotrov $V = \{\vec{v}_i \mid 1 \leq i \leq \gamma_{set}(n)\}$.
3. vygenerujeme vektor $A^{sk} = (A_1, \ldots, A_{\gamma_{set}(n)}) \in \{0,1\}^{\gamma_{set}(n)}$ taký, že $A_i = 1 \Leftrightarrow i \in \{a_i, a_{\gamma_{set}(n)}\}$.
4. $sk = (sk', A^{sk})$, $pk = (pk', V)$, $\mathcal{C} = \mathcal{C}' \times (\mathbb{Q}^n)^{\gamma_{set}(n)}$
5. $KeyGen_{\xi_3} \rightarrow (\mathcal{P}', \mathcal{C}, pk, sk)$

Šifrovanie:

1. $\vec{c} \leftarrow E_{\xi_2}(pk', \vec{m})$
2. $\vec{c_i} = \vec{c} \cdot \vec{v_i}$ pre $1 \leq i \leq \gamma_{set}(n)$
3. $E_{\xi_3}(pk, \vec{m}) \rightarrow (\vec{c}, \vec{c}_1, \ldots, \vec{c}_{\gamma_{set}(n)})$

Dešifrovanie:

1. $\vec{x}_i = A_i \cdot \vec{c}_i$ pre $1 \leq i \leq \gamma_{set}(n)$
2. $D_{\xi_3}(sk, (\vec{c}, \vec{c}_1, \ldots, \vec{c}_{\gamma_{set}(n)})) = \vec{c} - \lceil \sum_{i=1}^{\gamma_{set}(n)} \vec{x}_i \rfloor$

Koreketnosť dešifrovania vyplýva z korektnosti D_{ξ_2}.

Homomorfné vyhodnocovanie:

Obvody vyhodnocujeme rovnako ako v schéme ξ_2, t.j. nepoužívame "pomocné" $\vec{c}_1, \ldots, \vec{c}_{\gamma_{set}(n)}$. Až po vyhodntení obvodu expandujeme výsledný šifrový text.

Uvedená modifikácia nám umožňuje skonštruovať $O_{D_{\xi_3}} \in \mathcal{O}_{\xi_3}$, keďže teraz potrebujeme v kroku dva sčítať len $\gamma_{sub}(n)$ nenulových vektorov, pričom $\gamma_{sub}(n)$ môže byť sublineárna.

Krok 1: Vygenerujeme $\gamma_{sub}(n)$ vektorov $\vec{x}_1, \ldots, \vec{x}_{\gamma_{sub}(n)}$, kde $\vec{x_i} = A_i \cdot \vec{c_i}$. Zrejme tento krok vieme realizovať obvodom konštantnej hĺbky.

Krok 2: Použijeme obvod využívajúci elementárne symetrické polynómy popísaný v časti 1.5.2. Teraz potrebujeme sčítať $\gamma_{set}(n)$ vektorov, pričom vieme, že len $\gamma_{sub}(n)$ z nich je nenulových.

To znamená, že nám stačí presnosť $K = \log \gamma_{sub}(n) + 2$ zlomkových miest. Ďalej vieme, že pri výpočte $a_1, \ldots, a_K$ budú elementárne symetrické polynómy stupňa väčšieho než $\gamma_{sub}(n)$ nutne nulové a teda ich môžme vynechať. Z toho vyplýva, že na zápis a_i nám stačí $\log \gamma_{sub}(n) + 1$ bitov.

Teda hĺbka obvodu rátajúceho jednotlivé a_i bude $O(\log \gamma_{sub}(n))$, hĺbka obvodu rátajúceho výslednú sumu $O(\log \log \gamma_{sub}(n))$, teda hĺbka celkového obvodu realizujúceho krok 2 bude $O(\log \gamma_{sub}(n))$.

Krok 3: Chceme zrátať $\vec{m} = (\vec{c} - \sum_{i=1}^{\gamma_{set}(n)+1} \vec{y_i}) \bmod B_I$, kde $\vec{c}, \vec{y_1}, \ldots, \vec{y}_{\gamma_{set}(n)} \in R$.

Každý koeficient $\vec{y_i} = (y_{i,0}, \ldots, y_{i,n-1})$ je binárne reprezentovaný prvkami $1 \bmod B_I$ a $0 \bmod B_I$, teda $y_{i,j} = (\vec{y}_{i,j,0}, \ldots \vec{y}_{i,j,d-1})$ kde d je dĺžka binárneho zápisu a $\vec{y}_{i,j,k} \in \{0 \bmod B_I, 1 \bmod B_I\}$.

Vektor $\vec{y_i} \in R$ taktiež interpretujeme ako polynóm $y_0 + y_1 x + \ldots + y_{n-1} x^{n-1}$ a teda $\vec{y_i} \bmod B_I$ vieme vyjadriť ako [11]

$$\begin{aligned} \vec{y_i} \bmod B_I &= \left(\sum_{j=0}^{n-1} x^j \cdot \sum_{k=0}^{d-1} \vec{2^k} \cdot \vec{y}_{i,j,k} \right) \bmod B_I \\ &= \left(\sum_{j=0}^{n-1} \sum_{k=0}^{d-1} x^j \cdot \vec{2^k} \cdot \vec{y}_{i,j,k} \right) \bmod B_I \end{aligned}$$

Keďže hodnoty $\vec{2^k} \bmod B_I$ môžme predvypočítať a použiť ako konštanty, každý z členov sumy vieme zrátať pomocou dvoch $Mult_{B_I}$ hradiel. Ak predpokladáme, že dĺžka zápisu koeficientov je polynomiálna od n, tak sčítať členy sumy vieme

[11] Intuitívne: vlastne sa snažíme previesť binárny zápis koeficientov na "R/I" zápis, v ktorom využijeme všetky prvky, nie len $0 \bmod B_I$ a $1 \bmod B_I$. Podobne, ak by sme chceli zrátať b mod 13, kde $b = (b_0, \ldots, b_k)$ máme reprezentované binárne, teda len pomocou dvoch cifier z trinástich možných, tak vyjadríme $b \bmod 13 = \left(\sum_{i=0}^{k} 2^i \cdot b_i \right) \bmod 13$

obvodom s konštantnou hĺbkou zloženého z Add_{B_I} s polynomiálnym počtom vstupov.

Veta 6. *K schéme ξ_3 existuje prípustný dešifrovací obvod $O_{D_{\xi_3}} \in \mathcal{O}_{\xi_3}$ ak*

$$\gamma_{sub}(n) \leq \frac{\log(r_D/m)}{\alpha \cdot 2^c \cdot \log(\gamma_{Mult}(R) \cdot r_E)}$$

kde m je koeficient zmenšenia r_D modifikáciami, α je konštanta z asymptotickej zložitosti algoritmu sčítavania vektorov v kroku 2 a c je konštanta reprezentujúca súčet hĺbok obvodov realizujúcich ostatné kroky dešifrovania.

1.6 Bezpečnosť schémy

Postupne analyzujeme IND-CPA bezpečnosť [12] čiastočne homomorfnej schémy ξ_1, rozšírenej schémy ξ_3 a stupňovito plne homomorfnej schémy získanej bootstrapingom z ξ_3. Napokon uvedieme výsledky týkajúce sa IND-CCA bezpečnosti.[13]

1.6.1 Čiastočne homomorfná schéma

IND-CPA bezpečnosť schémy ξ_1 je založená na rozhodovacej verzii BDDP:

Definícia 9. *(Rozhodovací BDDP) Náhodne zvolíme $b \in \{0, 1\}$. Ak $b = 0$, rovnomerne náhodne vygenerujeme $\vec{r} \in \mathcal{B}(l_{max})$ a položíme $\vec{t} = \vec{r} \bmod B_J^{pk}$. Ak $b = 1$, rovnomerne náhodne vygenerujeme $\vec{t} \in^R P(B_J^{pk})$.*
Problém: z daného $\vec{t}$ urči b. Hovoríme, že algoritmus rieši problém s výhodou ϵ, ak jeho pravdepodobnosť úspechu je $1/2 + \epsilon$.

Riešenie uvedeného problému spočíva vlastne v určení, či $dist(J, \vec{t}) \leq l_{max}$. V zápornom prípade je hľadané b určite 1, a v kladnom - ak $l_{max} << \lambda_1(J)$ - je s vysokou pravdepodobnosťou $b = 0$.

Ak $\lambda_1(J)/l_{max} \geq 2^n$, tak varianta LLL algoritmu dokáže nájsť vektor v J najbližší k $\vec{t}$ v polynomiálnom čase a teda zlomiť bezpečnosť schémy. Aktuálne ale nie je známy žiaden polynomiálny útok ak napr. $\lambda(J)/l_{max} = 2^{n^c}, c < 1$.

Veta 7. *Ak existuje algoritmus A, ktorý s výhodou 2ϵ zlomí IND-CPA bezpečnosť schémy ξ_1, potom existuje algoritmus B s rovnakou časovou zložitosťou, ktorý rieši rohodovací BDDP s výhodou ϵ.*

[12] nerozlíšiteľnosť šifrových textov pri CPA
[13] nerozlíšiteľnosť šifrových textov pri CCA

Dôkaz. B dostane na vstupe $\vec{t}$ a začne simulovať A. Keď si A vyžiada šifrový text jedného z $\vec{m_1}, \vec{m_2}$, B zvolí $q \in^R \{0,1\}$ a pošle A šifrový text $\vec{c} = (\vec{m_q} + \vec{t} \cdot \vec{s}) \bmod B_J^{pk}$. Keď A vráti q', B určí $b = q \oplus q'$.

Ak $b = 0$, tak $\vec{c}$ je správne zostavený šifrový text, a teda A určí $q' = q$ s výhodou 2ϵ čo znamená výhodu 2ϵ pre B. Ak $b = 1$, tak $\vec{t} \in^R P(B_J^{pk})$. Keďže $J + I = R$, tak

$$\forall \vec{v} \in P(B_J^{pk}) : \exists \vec{t} \in P(B_J^{pk}), \exists \vec{j} \in J : \vec{v} - \vec{m}_q = \vec{t} \cdot \vec{s} + \vec{j}$$

a teda aj $\vec{c} \in^R P(B_J^{pk})$ a výhoda A je 0. Celková výhoda B je potom ϵ. □

V časti 1.3.2 sme ukázali, že vieme vygenerovať J tak, aby r_D bolo len polynomiálne menšie než $\lambda_1(J)$ (Veta 3). Taktiež sme ukázali, že zvolením krátkeho $\vec{s}$ získame r_E len polynomiálne väčšie než l_{max}, čo znamená, že bez narušenia bezpečnosti môžme mať $r_D/r_E = 2^{n^c}, c < 1$.

1.6.2 Squashing

Pri squashingu potrebujeme zaručiť, že je ťažké získať súkromný kľúč z poskytnutej dodatočnej informácie, čo Gentry postavil na predpoklade, že SSSP (sparse subset sum problem) je ťažký pre zvolené $\gamma_{set}(n)$ a $\gamma_{sub}(n)$.

Definícia 10. *(SSSP) Zvolíme $b \in \{0,1\}$. Ak $b = 0$, položíme $\tau = \{a_1, \ldots, a_{\gamma_{set}(n)}\}$, a_i sú volené rovnomerne náhodne z intervalu $\langle -q/2, q/2) , q \in \mathbb{Z}^+$ tak, že existuje $S \subset \tau, |S| = \gamma_{sub}(n) : \sum_{a_i \in S} a_i = 0 \bmod q$. Ak $b = 1$, zvolíme τ bez podmienky existencie S.*
Problém: z daného τ urči b.

Gentry ukázal, že ak zvolíme $\gamma_{set}(n) = \omega(n)$ a $\gamma_{sub}(n) = \omega(\log n)$, tak nepoznáme polynomiálny algoritmus riešiaci SSSP.

Definícia 11. *(SVSSP - sparse vector subset sum problem) Nech B_{IJ} je báza mriežky $I \cdot J$ v HNF. Zvolíme $b \in^R \{0,1\}$. Ak $b = 0$, položíme $\tau = \{\vec{u}_1, \ldots, \vec{u}_{\gamma_{set}(n)}\}$, $\vec{u}_i$ sú volené rovnomerne náhodne z $P(B_{IJ})$ tak, aby existovala $S \subseteq \tau, |S| = \gamma_{sub}(n)$ taká, že $\sum_{\vec{v} \in S} \vec{v} \equiv 0 \bmod B_{IJ}$. Ak $b = 1$, zvolíme τ bez podmienky existencie S.*
Problém: z daného τ urči b.

Gentry ukázal redukciu bepečnosti squashingu na SVSSP, ktorý potom redukoval na SSSP za prepokladu $\gamma_{set}(n) \geq \log det(IJ)$. Ak táto podmienka platí, tak známe útoky na SSSP majú zložitosť zhruba $2^{\gamma_{sub}(n)}$. Na druhej strane, ak $\lambda(J)/l_{max} = 2^k$, tak známe algoritmy dokážu riešiť BDDP v čase zhruba $2^{n/k}$. Aby

boli boli oba problémy približne rovnako ťažké, môžme položiť $\gamma_{sub}(n) = \sqrt{n}$. Aby zložitosť útoku na schému bola 2^λ, kde λ je bezečnostný parameter, potrebujeme $n \approx \lambda^2$.

1.6.3 Plne homomorfná schéma

Dá sa ukázať, že ak schéma ξ_3 je IND-CPA bezpečná, tak potom aj každá schéma ξ_3^d z bootstrappingom získanej stupňovito plne homomorfnej triedy schém $\{\xi_3^d \mid d \in \mathbb{Z}^+\}$ je IND-CPA bezpečná.

Verejná informácia ξ_3^d sa líši od ξ_3 v tom, že obsahuje navyše reťaz $d-1$ súkromných kľúčov rôznych inštancií šifrovaných verejným kľúčom predchádzajúcej inštancie. Na základe toho sa dá usúdiť, že prelomenie ξ_3^d implikuje prelomenie aspoň jednej z inštancií ξ_3.

Veta 8. *Nech l je maximum z dĺžok kódov súkromných kľúčov inštancií ξ_3 obsiahnutých v ξ_3^d. Potom ak existuje algoritmus A, korý zlomí IND-CPA bezpečnosť schémy ξ_3^d v čase t s výhodou ϵ, tak existuje algoritmus B, ktorý zlomí IND-CPA bezpečnosť schémy ξ_3 v čase $t' \approx l \cdot t$ s výhodou $\epsilon' \geq \epsilon/2l(d+1)$.*

1.6.4 CCA bezpečnosť

Vieme, že skonštruovaná FHE schéma je za istých predpokladov IND-CPA bezpečná. Loftus, May, Smart a Vercauteren [LMSV12] ukazujú CCA útok na Gentry - Halevi implementáciu [GH11b] čiastočne homomorfnej schémy. Zároveň transformujú Smart - Vercauteren [SV10] implementáciu na tzv. ccSWHE pridaním kontroly validity šifrového textu počas dešifrovania na IND-CCA1 bezpečnú čiastočne homomornú schému. Ďalej analyzovali prísnejšie kritériá na bezpečnosť FHE schémy a ukázali, že ccSWHE nie je odolná voči CVA útokom[14].

Autori taktiež poukázali na to, že v niektorých aplikáciách je potrebné zaručiť istú formu IND-CCA2 bezpečnosti a zaviedli preto pojem CCA-vnoriteľnej schémy, čo je vlastne IND-CPA homomorfná schéma, ktorej šifrový text možno pomocou verejných informácií extrahovať z šifrového textu nejakej IND-CCA2 schémy. Ukázali že analyzovaná schéma je CCA-vnoriteľná v modeli s náhodným orákulom.

[14]CVA - ciphertext validity attack; scenár, keď útočník má prístup k orákulu overujúcemu validitu šifrového textu.

1.7 Zložitosť schémy

Z analýzy bezpečnosti vyplýva, že potrebujeme $n \approx \gamma_{sub}(n)^2 \approx \lambda^2$. Keďže $\mathcal{B}(r_D) \subseteq P(B_J^{sk})$ a r_D je exponenciálne od $\gamma_{sub}(n)$ môžeme odhadnúť $\gamma_{set}(n) \approx \log det(IJ) \approx \log r_D^n \approx n \cdot \gamma_{sub}(n) \approx \lambda^3$.

Odhadneme parametre schémy ξ_3: veľkosť súkromného kľúča je $\gamma_{set}(n) = O(\lambda^3)$, veľkosť šifrového textu bez expanzie je $\log det(J) = O(\lambda^3)$, veľkosť verejného kľúča je súčet veľkostí B_J^{pk}, množiny V a zašifrovaných bitov súkromného kľúča, čo je $O(\lambda^6)$. Expanzia šifrového textu sa skaldá z $\gamma_{set}(n)$ vektorov, na požadovanú presnosť nám stačí logaritmická veľkosť koeficientov, teda veľkosť expanzie je $\gamma_{set}(n) \cdot n \cdot polylog(n) = \widetilde{O}(\lambda^5)$.[15]

Pri homomorfnom dešifrovaní v kroku 1 potrebujeme vygenerovať zašifrované podoby vektorov $\vec{x}_1, \ldots, \vec{x}_{\gamma_{sub}(n)}$, t.j. homomorfne vynásobiť zašifrované podoby A_i a bitov $\vec{c}_i$. Jednoduchou optimalizáciou je, že nemusíme "naozaj" šifrovať jednotlivé bity $\vec{c}_i$. Namiesto toho môžme šifrovú podobu bitu b reprezentovať ako vektor $b0^{n-1}$, čo je validný šifrový text. Keďže $\vec{c}_i$ má n koeficientov, každý veľkosti $\log n$- bitov, veľkosť šifrových textov reprezentujúcich $A_i = O(\lambda^3)$, tak zložitosť tohto kroku je $O(\gamma_{sub}(n) \cdot n \cdot \log n \cdot \lambda^3) = \widetilde{O}(\lambda^8)$.

V nasledujúcom výpočte je dominujúce rátanie elementárnych symetrických polynómov. Konkrétne potrebujeme pre každý bit $\vec{x}_i$ - t.j. $\widetilde{O}(\lambda^2)$ krát - zrátať elemntárne symetrické polynómy s $\gamma_{set}(n)$ premennými, t.j. koeficienty polynómu

$$p(z) = (z - x_{1,i}) \cdot \ldots \cdot (z - x_{\gamma_{set}(n),i})$$

S použitím FFT násobenia polynómov[16] vieme jednotlivé koeficienty zrátať v čase $\widetilde{O}(\gamma_{set}(n))$ na nešifrovaných bitoch. Homomorfne potrebujeme na každé násobenie šifrových textov čas $\widetilde{O}(\lambda^3)$, teda celkovo na zrátanie symetrických polynómov potrebujeme $\widetilde{O}(\lambda^8)$. Teda celková časová zložitosť homomorfného vyhodnotenia jedného hradla obvodu je $\widetilde{O}(\lambda^8)$.

1.7.1 Optimalizácie

Optimalizácia 1. Navrhnutá Gentrym [Gen09a]. Ak zvolíme ideál $I = (2)$, $\mathcal{P}_\xi = \{0, 1\}$ a $m \in \mathcal{P}_\xi$ kódujeme ako $\vec{m} = m0^{n-1}$, potom šifrový text má tvar $\vec{m} + \vec{i} + \vec{j}, \vec{i} \in I, \vec{j} \in J$, ktorý sa homomorfným vyhodnocovaním nemení a výsledný otvorený

[15] $\widetilde{O}(f(n)) = \bigcup_{k=1}^{\infty} O(f(n) \cdot \log^k f(n))$

[16] algoritmus realizujúci násobenie polynómov n-tého stupňa v čase $O(n \log n)$, ak jednotlivé koeficienty vieme násobiť v konštantnom čase.

text m je stále prvý koeficient $\vec{m}$. Pri dešifrovaní nám teda stačí počítať len prvý koeficient výrazu

$$\vec{c} - [\vec{c} \cdot \vec{v}^{sk}] = \vec{c} - [\sum_{\vec{v_i} \in V} \vec{c} \cdot \vec{v_i}]$$

To znamená, že v expanzii šifového textu nám stačí udržiavať len prvé koeficienty $\vec{c_i}$, čo znamená redukciu veľkosti šifrového textu na $\widetilde{O}(\lambda^3)$ a redukciu časovej zložitosti homomorfného dešifrovania na $\widetilde{O}(\lambda^6)$.

Podobná optimalizácia sa dá uplatniť ak $det(I)$ je prvočíslo, no prevedenie je podstatne komplikovanejsie.

Optimalizácia 2. Navrhnutá Gentrym [Gen09a]. Zvolíme $f(x) = x^n + 1, n = 2^k$, čo umožňuje efektívne rátať rotačné vektory $\vec{v} \cdot x^i$. Zmeníme veľkosť množiny vektorov vo verejnom kľúči $|V| = 2 \cdot \gamma_{subset}(n)$, pričom na $\vec{v^{sk}}$ sa bude sumovať $\gamma_{subset}(n)$ vektorov získaných rotáciou vektorov z V.

Konkrétne existuje $s \in \{0,1\}^{2 \cdot \gamma_{subset}(n)}, \sum s_i = \gamma_{subset}(n)$ a $r \in \mathbb{Z}_n^{2 \cdot \gamma_{subset}(n)}$

$$\sum s_i \cdot \vec{v_i} \cdot x^{r_i} \bmod f(x) = \vec{v}^{sk} \bmod B_I$$

Táto optimalizácia spolu s optimalizáciou 1 redukuje veľkosť súkromného kľúča na $\widetilde{O}(\lambda)$ a verejného kľúča na $\widetilde{O}(\lambda^4)$. Homomorfné dešifrovanie zrýchli na $\widetilde{O}(\lambda^4)$.

Avšak pri použití tejto optimalizácie je bezpečnosť schémy otázna, keďže autori nedokázali bezpečnosť takto modifikovaného rozdelenia súkromného kľúča redukovať na SSSP.

Optimalizácia 3. Navrhnutá Stehlém a Steinfieldom [SS10]. Autori analyzovali zložitosť SVSSP (namiesto SSSP) a ukázali, že známe útoky zlyhávajú pri $\gamma_{set}(n) = \widetilde{\Omega}(\sqrt{\log(det(IJ)) \cdot \lambda})$. Ďalej ukázali, že ak pri expanzii šifrového textu použijú pre c_i presnosť len $p = \widetilde{O}(\frac{1}{2} \log \gamma_{subset}(n))$ bitov, tak dokážu podstatne zredukovať hĺbku dešifrovacieho obvodu za cenu zanedbateľnej pravdepodobnosti chyby pri dešifrovaní.

V skratke, nech e_i sú odchýlky vzniknuté znížením presnosti, zrejme $e_i \in (-2^{-p}, 2^{-p})$. Keďže c_i boli volené navzájom nezávisle, aj e_i sú navzájom nezávislé (konkrétne požadujeme aby ich stredná hodnota bola 0), čo znamená že $\sum e_i$ bude s vysokou pravdepodobnosťou zanedbateľne malá.

Celková časová zložitosť homomorfného dešifrovania dosiahli $\widetilde{O}(\lambda^{3.5})$, veľkosť súkromného kľúča $\widetilde{O}(\lambda^{1.5})$, verejného kľúča $\widetilde{O}(\lambda^{3.5})$ a expandovaného šifrového textu $\widetilde{O}(\lambda^2)$.

1.8 Implementácia schémy

Tu budeme prezentovať doposiaľ najúspešnejšiu implementáciu tejto schémy [GH11b] publikovanú Gentrym a Halevim vychádzajúcu z implementácie Smarta a Vercauterena [SV10], ktorým sa ale nepodarilo urobiť ich SWHE schému bootstrapovateľnou. Najprv zhrnieme špecifiká implementácie.

Použitý je okruh $R = \mathbb{Z}[x]/(x^n+1), n = 2^k$, ideál $I = (2)$, $\mathcal{P} = \{0, 1\}$, otvorený text m je kódovaný ako vektor $\vec{m} = m0^{n-1}$. Ideál $J = (\vec{v})$, koeficienty $\vec{v}$ sú volené ako náhodné t-bitové čísla také, aby $HNF(J)$ mala tvar

$$\begin{pmatrix} d & 0 & 0 & 0 & ... & 0 \\ -r & 1 & 0 & 0 & ... & 0 \\ -[r^2]_d & 0 & 1 & 0 & ... & 0 \\ -[r^3]_d & 0 & 0 & 1 & ... & 0 \\ ... & & & & & \\ -[r^{n-1}]_d & 0 & 0 & 0 & ... & 1 \end{pmatrix}$$

kde $d = det(J)$ a r je koreň $(x^n+1) \bmod d$. Verejný kľúč SWHE sa skladá s týchto dvoch čísel. Pri šifrovaní $\vec{m}$ sa zvolí vektor $\vec{u} \in^R \{-1, 0, 1\}^n$, vyráta sa $\vec{a} = 2 \cdot \vec{u} + \vec{m}$ a položí sa $\vec{c} = \vec{a} \bmod HNF(J)$, ktorý možno vyjadriť ako $\vec{c} = ([a(r)]_d, 0, 0, \ldots, 0)$, teda šifrový text môže byť efektívne reprezentovaný ako $c \in \mathbb{Z}_d$. Autori ukázali ako možno k bitov efektívne zašifrovať v čase $O(\sqrt{kn})$.

Nech $\vec{w} = (w_0, \ldots, w_{n-1})$ je škálovaný inverzný prvok ku $\vec{v}$, t.j. $\vec{v} \cdot \vec{w} = d \bmod x^n + 1$. Nech V, W sú rotačné bázy prislúchajúce k $\vec{v}, \vec{w}$, zrejme $V \cdot W = W \cdot V = d \cdot I$. Pri dešifrovaní treba zrátať ($\vec{v}^*$ označuje vektor zlomkových častí koeficientov).

$$m = \vec{c} - \lceil \vec{c} \cdot W/d \rfloor \cdot V \bmod 2 = (\vec{c} \cdot W/d)^* \cdot V \bmod 2$$

Informácia je šifrovaná v odchýlke $\vec{c}$ od mriežky J, takže $\vec{c} = \vec{y} \cdot V + \vec{a}$, pre nejaký celočíselný vektor $\vec{y}$ a $\vec{a} \in P(V)$, a platí

$$\vec{a} \bmod 2 = m = ((\vec{y} \cdot V + \vec{a}) \cdot W/d)^* \cdot V \bmod 2 = (\vec{a} \cdot W/d)^* \cdot V \bmod 2$$

Teda dešifrovanie je korektné, ak $(\vec{a} \cdot W/d) = (\vec{a} \cdot W/d)^*$, t.j. koeficienty $(\vec{a} \cdot W)$ v absolútnej hodnote nepreshujú $d/2$, takže $(\vec{a} \cdot W/d)^* = [\vec{a} \cdot W]_d$.

Keďže $\vec{c} = (c, 0, \ldots, 0)$ dostávame

$$[\vec{c} \cdot W]_d = [c \cdot (w_0, \ldots, w_{n-1})]_d = ([cw_0]_d, \ldots, [cw_{n-1}]_d)$$

Zároveň

$$[\vec{c} \cdot W]_d = \vec{a} \cdot W = (2 \cdot \vec{u} + \vec{m}) \cdot W = m \cdot (w_0, \ldots, w_{n-1}) \bmod 2$$

Teda dostávame $\forall i : [cw_i]_d = mw_i \bmod 2$, takže nám stačí ako súkromný kľúč používať jeden (nepárny) koeficient $\vec{w}$.

Autori ukazujú, ako efektívne zrátať potrebný koeficient $\vec{w}$ a zároveň overiť, že $HNF(J)$ má požadovaný tvar.

Pri modifikácii na bootstrapovateľnú schému autori rozšíria verejný kľúč o s množín $X_1, \ldots, X_s$, skladajúcich sa z S čísel $x \in \mathbb{Z}_d$, pričom existuje binárna matica $\sigma \in \{0,1\}^{s \times S}$ taká, že v každom riadku je práve jedna jednotka a $\sum \sigma_{i,j} \cdot x_{i,j} = w$. Táto matica je súkromným kľúčom modifikovanej schémy.

Kvôli zníženiu veľkosti verejného kľúča je každá množina X_i definovaná pomocou jedného čísla x_i: $X_i = \{[x_i \cdot R^k]_d; 1 \leq k \leq S\}$, kde R je parameter schémy. Zašifrovaný súkromný kľúč je namiesto $s \cdot S$ šifrových textov reprezentovaný pomocou c šifrových textov pre každý riadok matice, z ktorých práve dve sú zašifrované jednotky. Tak i-tu hodnotu v danom riadku matice získame ako súčin niektorých dvoch šifrových textov. Autori ukázali ako možno prelievať časovú zložitosť homomorfného dešifrovania a priestorovú zložitosť verejného kľúča manipuláciou veľkosti c.

1.8.1 Výkon

Vo svojej implementácii zvolili za bezpečnostný parameter $\lambda = 72$, ktorý vyjadruje zložitosť prehľadávania a narodeninových útokov. Zložitosť útokov snažiacich sa riešiť BDDP ovplyvňuje najmä dimenzia mriežok, konkrétne testovali dimenzie $2^{11}, 2^{13}, 2^{15}$, zodpovedajúce bezpečnostnému parametru vzhľadom na rôzne predpoklady o sile použiteľných útokov. Veľkosť koeficientov $\vec{v}$ generujúceho ideál J používali 380 bitov. Výkon schémy autori testovali systéme so 64 bitovým 4-jadrovým Intel Xeon E5450 procesorom a 24GB RAM. Výsledky uvádzame v tabuľke:

n	pk	KeyGen	Šifrovanie	Dešifrovanie	Hom. dešifrovanie
2048	69 MB	41 sec	1.8 sec	0.02 sec	32 sec
8192	284 MB	8.4 min	19 sec	0.13 sec	2.8 min
32768	2.25 GB	2.2 hod	3 min	0.66 sec	31 min

1.8.2 Útoky

Schmidt [Sch11] sa snažil implementovať útoky na BDDP časť bezpečnosti schémy. Implementácia bola testovaná na Intel i7 1.6 GHz procesore s 4GB RAM. Implementovalný bol útok založený na LLL algoritme, útok extrahovaním vektora z podmriežky pomocou LLL, a tiež útok s pomocou BKZ algoritmu. Útoky boli

úspešné len po dimenziu mriežky 128, pričom autor sa pokúsil extrapolovať množstvo potrebného času na vyššie dimenzie s výsledkom $1.4, 92, 6024$ roka postupne pre $2^{11}, 2^{13}, 2^{15}$.

Chunsheng [Chu11] popísal útok založený na blokovej redukcii mriežok, ktorý ukazuje, že implementácia pre $n = 2^{11}$ nie je bezpečná. S dodatočnými predpokladmi by mal byť útok úspešný aj pre $n = 2^{13}$. Chunsheng taktiež ukazuje že za istých predpokladov LLL algoritmus dokáže zlomiť schému pre $n \approx 6000$. Zatiaľ nám ale implementácia útokov pre tieto dimenzie nie je známa.

Pri analýze CCA bezpečnosti [LMSV12] schémy Loftus, Smart, May a Vercauteren predstavili jednoduchý IND-CCA1 útok na túto implementáciu schémy potrebujúci $O(\log d)$ dotazov na dešifrujúce orákulum.

Kapitola 2

Chimérická schéma

V predchádzajúcej kapitole sme sa zaoberali FHE založenou na bootstrappingu. Videli sme, že problémom priamočiareho aplikovania boostrappingu na SWHE je cyklická závislosť medzi zložitosťou dešifrovacieho obvodu a hĺbkou prípustných obvodov: zväčšenie hĺbky prípustných obvodov vyžadovalo zväčšenie hĺbky dešifrovacieho obvodu. Východiskom bola modifikácia SWHE, ktorá vyžadovala zavädenie dodatočných bezpečnostných predpokladov.

V tejto kapitole načrtneme iné riešenie tohto problému navrhnuté Gentrym a Halevim [GH11a] spočívajúce v sofistikovanejšom vyhodnocovaní dešifrovacieho obvodu, ktoré umožňuje postaviť bezpečnosť schémy len na SVP v ideálnych mriežkach. Hlavnou myšlienkou je vyjadriť dešifrovací obvod schémy v $\Sigma\Pi\Sigma$ tvare a použiť nezávislú multiplikatívne homomorfnú schému (napr. ElGamal) na vyhodnotenie Π časti, respektíve použiť aditívne homomorfnú schému a pracovať s logaritmami šifrových textov.

Pokúsime sa ilustrovať túto metódu na SWHE ξ popísanej v predchádzajúcej kapitole, s modifikáciou 1 umožňujúcou skompaktnenie dešifrujúcej funkcie, s modifikáciou 2 umožňujúcou obmedziť počet zlomkových miest koeficientov na $\kappa \in O(\log \lambda)$ a s optimalizáciou 1 obmedzujúcou $\mathcal{P}_\xi$ na $\mathbb{Z}_p$ pre nejaké prvočíslo p.

Všetky lemy a vety v tejto kapitole sú prebraté z Gentryho a Haleviho práce [GH11a].

2.1 $\Sigma\Pi\Sigma$ obvody

Definícia 12. *Nech $\mathcal{L} = \{L(x_1, \ldots, x_n)\}$ je množina polynómov s rovnakými n premennými nad poľom F. Hovoríme, že aritmetický obvod O je $\mathcal{L}$-obmedzený ob-*

vod hĺbky 3 nad F, ak existujú multi-množiny $S_1, \ldots, S_t \subseteq \mathcal{L}$ *a konštanty* $\lambda_0, \ldots, \lambda_t \in F$ *také, že*

$$O(x_1, \ldots, x_n) = \lambda_0 + \sum_{i=1}^{t} \lambda_t \cdot \prod_{L_j \in S_i} L_j(x_1, \ldots, x_n)$$

Hovoríme, že O *má* $\mathcal{L}$*-stupeň* $d = \max\{|S_i|\}$.

V nasledujúcom texte sa budeme snažiť vyjadriť dešifrovaciu funkciu $D_\xi(\vec{v}^{sk}, \vec{c})$ ako $\mathcal{L}$-obmedzený obvod hĺbky 3 nad $\mathbb{Z}_p$ kde p je prvočíslo, $|\mathcal{L}| \in poly(\lambda)$, $\vec{c}$ je zadaný implicitne pri konštrukcii obvodu a vstupy závisia len od $\vec{v}^{sk}$.

Dešifrovacia funkcia ξ má tvar:

$$D_\xi(\vec{v}^{sk}, \vec{c}) = \vec{c} - [\vec{c} \cdot \vec{v}^{sk}] \bmod B_I$$

Ak binárne zakódujeme koeficienty $\vec{v}^{sk} = \langle s_1, \ldots, s_N \rangle$, rozšírime verejný kľúč [1] o množinu $\{\vec{v}_i = \langle 0^{i-1}, 1, 0^{N-i} \rangle \mid 1 \leq i \leq N\}$ a expandujeme šifrový text $\vec{c}$ o množinu $\{\vec{u}_i = \vec{c} \cdot \vec{v}_i \mid 1 \leq i \leq N\}$, tak môžme vyjadriť D_ξ ako

$$\vec{c} - \lceil \sum_{i=1}^{N} s_i \cdot \vec{u}_i \rfloor \bmod B_I$$

Vďaka optimalizácii 2 nám stačí počítať len jeden koeficient:

$$c - \lceil \sum_{i=1}^{N} s_i \cdot u_i \rfloor \bmod p$$

a ak rozdelíme u_i na celú a zlomkovú časť $u_i = u_i' + 2^{-\kappa} u_i''$ dostávame:

$$\underbrace{c - \sum_{i=1}^{N} s_i \cdot u_i'}_{A} - \underbrace{\lceil 2^{-\kappa} \cdot \sum_{i=1}^{N} s_i \cdot u_i'' \rfloor}_{B} \bmod p \tag{2.1}$$

Keďže časť A vieme rátať jednoduchým obvodom, budeme sa ďalej sústrediť na časť B.

[1] Je dôležité si uvedomiť, že toto rozšírenie, na rozdiel od squashingu v kapitole 1, neposkytuje žiadnu informáciu o súkromnom kľúči.

Lema 4. *Nech $p \geq 2N^2$ je prvočíslo, $\kappa \leq \lceil \log(N+1) \rceil$, $u_i \leq 2^\kappa - 1$, $s_i \in \{0,1\}$ pre $1 \leq i \leq N$. Potom existuje polynóm f stupňa nanajvýš $2N^2$ taký, že*

$$f(\sum_{i=1}^{N} s_i \cdot u_i'') = \lceil 2^{-\kappa} \cdot \sum_{i=1}^{N} s_i \cdot u_i'' \rfloor \bmod p$$

Dôkaz. Z ohraničení pre parametre vyplýva, že $\sum_{i=1}^{N} s_i \cdot u_i'' \in \langle 0, N(2^\kappa - 1) \rangle \subseteq \langle 0, 2N^2 \rangle$, Teda potrebujeme dodržať hodnoty funkcie v nanajvýš $2N^2 + 1$ bodoch, čo vieme polynómom syupňa $2N^2$ splniť vždy. □

Lema 5. *Nech $p \geq n+1$ je prvočíslo, $A \subseteq \mathbb{Z}_p, |A| = n+1$, nech $\vec{x} = (x_1, \ldots, x_n)$ sú premenné a $\mathcal{L}_A = \{a + x_i \mid a \in A, 1 \leq i \leq n\}$. Pre každý multilineárny symetrický polynóm $M(\vec{x})$ nad $\mathbb{Z}_p$ existuje obvod $O(\vec{x})$ taký, že:*

- *O je $\mathcal{L}_A$-obmedzený obvod hĺbky 3 nad $\mathbb{Z}_p$ s $\mathcal{L}_A$-stupňon n taký, že $O(\vec{x}) = M(\vec{x})$*
- *O má $n+1$ multiplikatívnych hradiel, pričom j-te hradlo realizuje výpočet $\lambda_j \cdot \prod_{i=1}^{N} (a_j + x_i)$ pre nejaké $\lambda_j \in \mathbb{Z}_p$.*
- *O vieme efektívne skonštruovať na základe hodnôt $M(\vec{x})$ v bodoch $1^i 0^{n-i}, 0 \leq i \leq n$.*

Dôkaz. Každý multilineárny symetrický polynóm vieme vyjadriť ako lineárnu kombináciu elementárnych symetrických polynómov $M(\vec{x}) = \sum_{i=0}^{n} l_i \cdot e_i(\vec{x})$. Zrejme $l_0 = M(0^n)$. Ďalšie koeficietny vieme rekurzívne vyrátať:

$$\begin{aligned} M(1^i 0^{n-1}) &= \sum_{j=0}^{n} l_j \cdot e_j(1^i 0^{n-1}) \\ &= l_i + \sum_{j=0}^{i-1} l_j \cdot e_j(1^i 0^{n-1}) \\ l_i &= M(1^i 0^{n-1}) - \sum_{j=0}^{i-1} l_j \cdot \binom{i}{j} \end{aligned}$$

Teda ak ukážeme, že tvrdenie platí pre elementárne symetrické polynómy, potom požadovaný $\mathcal{L}_A$-obmedzený obvod pre ľubovoľný multilineárny symetrický polynóm vieme získať ako kombináciu obvodov pre elementárne polynómy.

Pre každé $0 \leq i \leq n$ vieme hodnotu $e_i(\vec{x})$ získať ako koeficient pri z^{n-i} polynómu $p(z) = \prod_{i=0}^{n}(z + x_i)$. Každý z koeficientov vieme získať interpoláciou hodnôt polynómu $p(z)$ v bodoch $a_0, \ldots a_n \in A$, teda

$$e_i(\vec{x}) = \sum_{j=0}^{n} \lambda_j \cdot p(a_j)$$

pre nejaké $\lambda_0, \ldots, \lambda_j \in \mathbb{Z}_p$ závisiace len od A, ktoré vieme získať napr. riešením sústavy lineárnych rovníc. □

Lema 6. *Nech $T, n \in \mathbb{N}$, $p \geq Tn + 1$ je prvočíslo a f(x) je polynóm nad $\mathbb{Z}_p$. Potom existuje multi-lineárny symetrický polynóm M s Tn premennými, taký, že pre všetky $t_1, \ldots t_n \in \{0, \ldots, T\}$, $b_1, \ldots, b_n \in \{0, 1\}$ platí:*

$$f(b_1 t_1 + \ldots + b_n t_n) = M(b_1^{t_+} 0^{T-t_+}, \ldots, b_n^{t_n} 0^{T-t_n})$$

Navyše $\mathcal{L}_A$-obmedzený obvod hĺbky 3 realizujúci M vieme získať v čase poly(Tn), ak máme prístup k hodnotám $f(x)$.

Dôkaz. Položíme $g : \mathbb{Z}_p^{Tn} \to \mathbb{Z}_p, g(\vec{x}) = f(\sum x_i)$. Potom $g(x)$ je symetrický polynóm a platí

$$f(b_1 t_1 + \ldots + b_n t_n) = g(b_1^{t_1} 0^{T-t_1}, \ldots, b_n^{t_n} 0^{T-t_n})$$

g(x) nemusí byť multi-lineárny, ale pre $x \in \{0, 1\}$ platí $x^k = x$, a teda M získame "zlineárením"g, t.j. zamenením x_i^k za x_i pre všetky i, k.

$\mathcal{L}_A$-obmedzený obvod realizujúci M vieme rovnako ako v lemme 5 získať pomocou hodnôt $M(1^i 0^{Tn-i}) = f(i)$. □

Teraz môžme vysloviť nasledujúcu vetu:

Veta 9. *Nech $p \geq 2N^2$ je prvočíslo. Potom pre $A \subseteq \mathbb{Z}_p, |A| \geq 2N^2 + 1$ vieme dešifrovaciu funkciu (2.1) schémy ξ vyjadriť ako $\mathcal{L}_A$-obmedzený obvod O hĺbky 3 nad $\mathbb{Z}_p$ s $\mathcal{L}_A$-stupňom nanajvýš $2N^2$ a najviac $2N^2 + N + 1$ multiplikatívnymi hradlami.*

Dôkaz. Najprv rozoberieme B časť funkcie. Podľa lemy 4 existuje polynóm $f(x)$ nad $\mathbb{Z}_p$ stupňa nanajvýš $2N^2$, pre ktorý platí

$$f(\sum_{i=1}^{N} s_i \cdot u_i'') = \lceil 2^{-\kappa} \cdot \sum_{i=1}^{N} s_i \cdot u_i'' \rfloor \bmod p$$

Keďže $\forall i : u_i'' \in \{0, 2N\}$, tak podľa lemy 6 existuje multilineárny symetrický polynóm M s $2N^2$ premennými, pre ktorý platí:

$$f(s_1 u_1'' + \ldots + s_N u_N'') = g(s_1^{u_1''} 0^{2N-u_1''}, \ldots, s_N^{u_N''} 0^{2N-u_N''})$$

a ku ktorému vieme zostrojiť $\mathcal{L}_A$-obmedzený obvod O_B hĺbky 3. Podľa lemy 5 má C_B stupeň nanajvýš $2N^2$ a $2N^2 + 1$ multiplikatívnych hradiel.

Ak vyjadríme A časť dešifrujúcej funckie ako

$$c - \sum_{i=1}^{N} s_i \cdot u_i' = (c + \sum_{i=1}^{N} a_1 \cdot u_i') - (\sum_{i=1}^{N} (a_1 + s_i) \cdot u_i')$$

kde $c + \sum_{i=1}^{N} a_1 \cdot u_i'$ je konštanta, tak získame $\mathcal{L}_A$-obmedzený obvod O_A hĺbky 3 s $\mathcal{L}_A$-stupňom 1 a N multiplikatívnymi hradlami. Požadovaný obvod O získame kombináciou O_A a O_B. □

2.2 Konštrukcia FHE

V tejto časti prezentujeme ako skombinovať SWHE, ktorej dešifrovaciu funkciu vieme vyjadriť ako $\mathcal{L}$-obmedzený obvod hĺbky 3, a kompatibilnú multiplikatívne homomorfnú schému (MHE) do stupňovito plne homomorfnej schémy[2].

Pri bootstrapovaní najprv získame šifrové texty prislúchajpce k $L(s_1, \ldots, s_N) \in \mathcal{L}$ v inštancii MHE. Keďže $|\mathcal{L}| \in poly(\lambda)$, vieme šifrované verzie polynómov obsiahnuť vo verejnom kľúči. Potom vyhodnotíme $\prod$ časť obvodu násobením v MHE a takto získané šifrové texty prevedieme naspäť do SWHE pomocou homomorfného vyhodnotenia dešifrovacej funkcie MHE. SWHE schéma takto musí byť schopná homomorfne vyhodnotiť len dešifrovací obvod MHE schémy, čo vieme docieliť vhodnou voľbou parametrov.

Stupňovitú FHE $\Phi = \{\xi^d\}$ skonštruujeme zo SWHE ξ s vlastnosťami popísanými v úvode kapitoly a El Gamal schémy Ψ nad grupou kavdratických rezíduí $QR(p) = \{x \in \mathbb{Z}_p \mid \exists y \in \mathbb{Z}_p : y^2 = x, x \neq 0\}$ pre bezpečné prvočíslo $p = 2q + 1$, kde q je tiež prvočíslo:

- $KeyGen_\Psi \to (QR(p), QR(p)^2, (p, g, g^x), (p, g, x))$, g generuje $QR(p), x \in \mathbb{Z}_q$
- $E_\Psi(pk, m) \to (g^y, mg^{-xy})$, $y \in \mathbb{Z}_q$

[2] s pseudonymom "monstrous chimera"

- $D_\Psi(sk,(a,b)) \to b \cdot a^x$
- $Eval_\Psi(sk, O, (a_1,b_1),\ldots,(a_k,b_k)) \to (O(a_1,\ldots,a_k), O(b_1,\ldots,b_k))$

Generovanie kľúča:

1. Vygenerujeme d inštancií ξ a $\Psi (1 \leq i \leq d)$:

$$KeyGen_\xi(1^\lambda) \to (\mathcal{P}_\xi, \mathcal{C}_{\xi,1}, pk_{\xi,1}, sk_{\xi,1})$$
$$KeyGen_\Psi(1^\lambda) \to (\mathcal{P}_{\Psi,1}, \mathcal{C}_\Psi, pk_{\Psi,1}, sk_{\Psi,1})$$

2. Pre $sk_{\Psi,i} = (p, g_i, x_i)$ binárne zakódujeme súkromný exponent $x_i = (x_{i,1}, \ldots x_{i,l})$ a začifrujeme pomocou verejného kľúča $pk_{\xi,i+1}$ $(1 \leq i \leq d-1)$:

$$E_\xi(pk_{\xi,i+1}, (x_{i,1}, \ldots x_{i,l})) \to (\overline{x_{i,1}}, \ldots, \overline{x_{i,l}}) = \overline{x_i}$$

3. Pre $1 \leq i \leq d-1$ binárne zokódujeme $sk_{\xi,i} \to (s_{i,1}, \ldots, s_{i,N})$, zvolíme množinu [3] $A = \{a \in \mathbb{Z}_p \mid a, a+1 \in QR(p)\}, |A| \in poly(\lambda)$ a pre všetky $a_k \in A, 1 \leq j \leq N, 1 \leq i \leq d-1$:

$$E_\Psi(pk_{\Psi,i} a + s_j) \to \overline{a_k + s_{i,j}}$$

4. $sk = \{sk_{\xi,1}, \ldots, sk_{\xi,d}\}$
5. $pk = \{(pk_{\xi,i}, pk_{\Psi,i}) \mid 1 \leq i \leq d\} \cup \{\overline{x_i} \mid 1 \leq i \leq d-1\} \cup \{\overline{a_k + s_{i,j}} \mid a_k \in A, 1 \leq j \leq N, 1 \leq i \leq d-1\} \cup A$
6. $\mathcal{C} = \{(c,i) \mid 1 \leq i \leq d, c \in \mathcal{C}\xi, i\}$
7. $KeyGen_{\xi^d}(1^\lambda) \to (\mathcal{P}_\xi, \mathcal{C}, pk, sk)$

Šifrovanie: $E_{\xi^d}(pk, m) = (E_\xi(pk_{\xi,1}, m), 1)$

Dešifrovanie: $D_{\xi^d}(pk, (c,i)) = D_\xi(sk_{\xi,i}, c)$

Homomorfné vyhodnocovanie:

Používame bootstrapping popísaný v časti 1.4 s nasledujúcou implementáciou procedúry *Recrypt*:

Na základe vety 9 skonštruujeme $\mathcal{L}_A$ obmedzený obvod O hĺbky 3 nad $\mathbb{Z}_p$. Z konštrukcie daného obvodu popísanej v lemme 4, 5 a 6 vidno, že vstupy tohto

[3] spôsob voľby A, je podrobnejšie popísaný v časti 2.4

obvodu sú jednotlivé bity $(s_1, \ldots, s_N)$, respketíve 0. Vieme teda skonštruovať zašifrované verzie polynómov v inštancii Ψ vstupujúcich do $\prod$ časti - ak je polynóm tvaru $a + s_i, a \in A$, tak jeho podobu máme vo verejnom kľúči, a ak je tvaru $a + 0$, tak ho vieme priamo zašifrovať.

Keďže El Gamal schéma Ψ je neobmedzene multiplikatívne hmomorfná, vieme v nej vyhodnotiť $\prod$ časť obvodu O, čím získame šifrové texty Ψ ktoré potrebujeme na záver sčítať. Najprv prevedieme šifrové texty v Ψ na šifrové texty v ξ pomocou homomorfného vyhodnotenia D_Ψ:

Pre súkromný exponent $x = (x_1, \ldots, x_l)$ vyjadríme $D_\Psi(sk, (a, b))$ ako

$$\begin{aligned} b \cdot a^x &= b \cdot \prod_{i=1}^{l} a^{x_i \cdot 2^i} \\ &= b \cdot \prod_{i=1}^{l} x_i a^{2^i} + 1 - x_i \\ &= b \cdot \prod_{i=1}^{l} x_i (a^{2^i} - 1) + 1 \end{aligned}$$

Ak si predrátame $a^{2^i} - 1$, tak to vieme zrátať obvodom nad $\mathbb{Z}_p$ hĺbky $O(\log l)$. Aby sme mohli homomorfne dešifrovať, stačí nám zašifrovať $(a^{2^i} - 1)$, b, 1 v inštancii ξ, keďže šifrovanú podobu x_i máme vo verejnom kľúči.

Posledným krokom je homomorfne - v schéme ξ - vyhodnotiť posledný stupeň obvodu O, t.j sčítať výsledky $\prod$ častí.

Pdobným spôsobom sa dá skonštruovať stupňovitá schéma, kde za Ψ namiesto El Gamal schémy použijeme aditívne homomorfnú schému - napríklad ξ s vhodnou voľbou parametrov - a budeme rátať s diskrétnymi logaritmami prvkov, t.j. pred konverziou šifrových textov do Ψ vyrátame ich diskrétne logaritmy a po konverzii homomorfným dešifrovaním späť budeme umocňovať.

2.3 Zložitosť schémy

Aby sme predišli útokom na ElGamal schému Ψ, potrebujeme p veľkosti $O(\lambda)$ bitov. Potom z analýzy zložitosti schémy ξ v predchádzajúcej kapitole vyplývajú odhady pre veľkosť súkromného kľúča schémy ξ^d $O(d \cdot \lambda^2)$, veľkosť verejného kľúča $O(d \cdot \lambda^4)$ a veľkosť šifrového textu $O(\lambda^3)$.

Pri homomorfnom dešifrovaní potrebujeme najprv vyhodnotiť $\prod$ časť $\mathcal{L}_A$ obmedzeného obvodu v Ψ, t.j. vynásobiť $2N^2$ $O(\lambda)$ bitových čísel. Keďže N je počet

bitov súkromného kľúča schémy ξ, tak $N = \widetilde{O}(\lambda^2)$, teda časť $\prod$ vieme vyhodnotiť v $\widetilde{O}(\lambda^6)$.

Potom potrebujeme homomorfne dešifrovať $2N^2 + N + 1$ dvojíc $(a, b) \in \mathbb{Z}_p^2$ ktoré sú šifrovými textami výsledkov $\prod$ častí, t.j. homomorfne vyhodnotiť

$$b \cdot \prod_{i=1}^{\log p} a^{x_i \cdot 2^i}$$

kde $(x_1, \ldots, x_{\log p})$ sú bity súkromného exponentu, ktorých začifrované podoby máme vo verejnom kľúči. Potrebujeme zrátať $(a^{2^i} - 1)$ pre $1 \leq i \leq \log p$, čo vieme v $O(\log^3 q)$, zašifrovať jednotlivé bity b a $(a^{2^i} - 1)$ - tu môžme použiť podobnú optimalizáciu ako v predchádzajúcej kapitole, t.j. za šifrovú podobu bitu b budeme považovať $b0^{n-1}$, a napokon vyhodnotiť obvod v čase $\widetilde{O}(\lambda^5 \cdot \log q)$, teda celková časová zložitosť tohto kroku je $\widetilde{O}(\lambda^{10})$.

Napokon potrebujeme sčítať výsledky $2N^2 + N + 1$ $\prod$ častí, čo vieme v $\widetilde{O}(\lambda^7)$. Teda celková zložitosť homomorfného vyhodnocovania je $\widetilde{O}(\lambda^{10})$.

2.4 Kompresia šifrového textu

V tejto časti sa pokúsime popísať techniku, ktorá umožní reprezentáciu šifrového textu schémy Φ pomocou jediného šifrového textu Ψ schémy.

2.4.1 Čiastočná kompresia

Najprv sa budeme sústrediť na B časť dešifrovacej funkcie ξ:

$$\underbrace{c - \sum_{i=1}^{N} s_i \cdot u'_i}_{A} - \underbrace{\lceil 2^{-\kappa} \cdot \sum_{i=1}^{N} s_i \cdot u''_i \rfloor}_{B} \bmod p$$

Pri konverzii B-časti na $\mathcal{L}$-obmedzený obvod O hĺbky 3 mali násobené polynómy špeciálny tvar, keďže multilineárny symetrický polynóm realizovný obvodom sme získali ako:

$$f(s_1 u''_1 + \ldots + s_N u''_N) = g(s_1^{u''_1} 0^{2N - u''_1}, \ldots, s_N^{u''_N} 0^{2N - u''_N})$$

tak O môžme vyjadriť ako ($\vec{x} = (s_1^{u_1''} 0^{2N^2-u_1''}, \ldots, s_N^{u_N''} 0^{2N^2-u_N''})$):

$$\begin{aligned} O(\vec{x}) &= \lambda_0 + \sum_{j=1}^{2N^2} \lambda_j \cdot \prod_{i=1}^{2N^2} (a_j + x_i) \\ &= \lambda_0 + \sum_{j=1}^{2N^2} \lambda_j \cdot \prod_{i=1}^{N} (a_j + s_i)^{u_i''} \cdot (a_j + 0)^{2N-u_i''} \end{aligned}$$

Ak označíme $v = \sum_{i=1}^{N} s_i \cdot u_i''$

$$\lambda_0 + \sum_{j=1}^{2N^2} \lambda_j \cdot \underbrace{(a_j + 1)^v \cdot (a_j + 0)^{2N-v}}_{P(a_j)}$$

Ak poznáme $P(a_1)$ a a_1, tak vieme vyrátať v, a následne $P(a_j)$ pre ľubovoľné a_j. Aby sme to vedeli rátať efektívne, pre $j > 1$ zvolíme a_j tak, aby sme poznali čísla e_j, w_j, pre ktoré platí:

$$\begin{aligned} a_j &= w_j \cdot a_1^{e_j} \\ a_j + 1 &= w_j \cdot (a_1 + 1)^{e_j} \end{aligned}$$

To vieme spraviť tak, že zvolíme $e_j \notin \{0, 1\}$ a dorátame a_j a w_j:

$$\begin{aligned} a_j &= \frac{a_1^{e_j}}{(a_1 + 1)^{e_j} - a_j^{e_j}} \\ w_j &= \frac{1}{(a_1 + 1)^{e_j} - a_j^{e_j}} \end{aligned}$$

Potrebujeme ale zaručiť, že $a_j, a_j + 1 \in \mathcal{P}_\Psi$, v prípade El Gamala, že sú to kvadratické rezíduá. Platí:

$$a_j, a_j + 1 \in QR(p) \Leftrightarrow (a_1 + 1)^{e_j} - a_j^{e_j} \in QR(p) \Leftrightarrow \frac{(a_1 + 1)^{e_j}}{a_1^{e_j}} - 1 \in QR(p)$$

Lema 7. *Nech $p > 5$ je prvočíslo, $S = \{(a, b) \in \mathbb{Z}_p^2 \mid a = b + 1 \wedge a, b \in QR(p)\}$. Potom ak $p \bmod 4 = 3$, tak $|S| = (p - 3)/4$. Ak $p \bmod 4 = 1$, tak $|S| = (p - 5)/4$.*

Dôkaz. Nech $T = \{(u, v) \in \mathbb{Z}_p^2 \mid u \neq 0, v \neq 0, u^2 - v^2 = 1 \bmod p\}$. Keďže každé kvadratické rezíduum má dve odmocniny, $|T| = 4|S|$. Ak označíme $a_{uv} = u + v$,

potom:

$$\begin{aligned} u^2 - v^2 &= 1 \\ (u+v)(u-v) &= 1 \\ (u-v) &= 1/a_{uv} \\ u &= (a_{uv} + a_{uv}^{-1})/2 \\ v &= (a_{uv} - a_{uv}^{-1})/2 \end{aligned}$$

Ak $U = \{a \in \mathbb{Z}_p \mid a \neq 0, a + a^{-1} \neq 0, a - a^{-1} \neq 0\}$, tak $|U| = |T|$. Zrejme

$$a \in U \Leftrightarrow a \neq 0, a^2 \neq -1, a \neq \pm 1$$

Ak $p \bmod 4 = 1$, tak $-1 \in QR(p)$ a teda 5 rôznych prvkov nepatrí do U. Ak $p \bmod 4 = 3$, tak $-1 \notin QR(p)$, a teda 3 rôzne prvky nepatria do U. □

Keďže p je bezpečné prvočíslo, tak $|S| = (p-3)/4$. Keďže $(a_1+1)^{e_j}/a_1^{e_j}$ je generátor $QR(p)$, tak pravdepodobnosť toho , že $a_j, a_j + 1 \in QR(p)$ je približne $1/2$, a teda metóda pokus-omyl hľadania vyhovujúcich e_j postačuje.

To znamená, že ak pridáme do verejného kľúča hodnoty w_j a e_j, tak vieme vyjadriť $P(a_j)$ len z $P(a_1)$:

$$P(a_j) = w_j^{2N^2} \cdot P(1)^{e_j}$$

Navyše, tento výpočet vieme uskutočniť homomorfne na šifrových textoch Ψ, keďže potrebujeme len násobiť. To znamená, že ak sa nám podarí vyjadriť celú dešifrovaciu funkciu ako jeden multilineárny symetrický polynóm, tak touto technikou dokážeme komprimovať šifrový text Φ do jedného šifrového textu Ψ.

2.4.2 Kompletná kompresia

Ak obmedzíme množinu otvorených textov na $\mathcal{P}_\Phi = \mathbb{Z}_2$, tak budeme môcť rátať časť A modulo prvočíslo $r \in O(N)$, čo nám umožní vyjadriť dešifrovaciu funkciu ako jeden multilineárny symetrický polynóm v požadovanom tvare.

Lema 8. *Nech $p \in \omega(N^2)$ je prvošíslo, nech $(c, \{u'_i\}, \{u''_i\})$ je expandovaný šifrový text ξ a platí $D_{xi}(sk, c) = m \in \mathbb{Z}_2$. Potom existuje prvočíslo $r \in O(N)$ a polynóm $f(x)$ nad $\mathbb{Z}_p$ stupňa $O(N^2)$, taký že platí $f(t_r) = m \bmod p$, kde*

$$t_r = (2^\kappa \cdot c) \bmod r + \sum_{i=1}^{N} s_i \cdot (-2^\kappa u'_i - u''_i) \bmod r$$

Dôkaz. Nech $t = 2^{\kappa}(c - \sum_{i=1}^{N} s_i \cdot u'_i) - \sum_{i=1}^{N} s_i \cdot u''_i$. Potom

$$m = c - \sum_{i=1}^{N} s_i \cdot u'_i - \lceil 2^{-\kappa} \cdot \sum_{i=1}^{N} s_i \cdot u''_i \rfloor \bmod p = \lceil 2^{-\kappa} \cdot t \rfloor \bmod p$$

Keďže výraz $\lceil 2^{-\kappa} \cdot t \rfloor$ nadobúda len hodnoty $0, 1$, tak ak zvolíme $r > 2^{\kappa+1}$, potom môžeme t nahradiť $(t \bmod r)$. Zrejme $(t \bmod r) = (t_r \bmod r)$, a teda vieme m vyjadriť pomocou t_r. Keďže t_r nadobúda najviac $O(N \cdot r) = O(N^2)$, hľadaný polynóm existuje. □

Veta 10. *Nech $p \in \omega(N^2)$ je prvošíslo, nech $(c, \{u'_i\}, \{u''_i\})$ je expandovaný šifrový text ξ a platí $D_{xi}(sk, c) = m \in \mathbb{Z}_2$. Nech $a = (2^{\kappa} \cdot c) \bmod r$ a $b_i = (-2^{\kappa} \cdot u'_i - u''_i) \bmod r, 1 \leq i \leq N$. Potom existuje prvočíslo $r \in O(N)$ a multilineárny symetrický polynóm M, taký, že platí:*

$$m = M(1^a 0^{r-a}, s_1^{b_1} 0^{r-b_1}, \ldots, s_N^{b_N} 0^{r-b_N}) \bmod p$$

Dôkaz. Priamo vyplýva z lemy 8 a 6. □

Vyjadrili sme celú dešifrovaciu funkciu pomocou multilineárneho symetrického polynómu, a teda dokážeme šifrový text Φ reprezentovať pomocou hodnoty $P(a_1)$ šifrovanej v schéme Ψ, čo v prípade ElGamal schémy Ψ znamená značnú redukciu veľkosti - z $O(\lambda^3)$ na $O(\lambda)$.

Kapitola 3

Škálovanie rozsahu

V tejto kapitole predstavíme iný prístup ku konštrukcii plne homomorfnej schémy prezentovaný Brakerskim, Gentrym a Vaikuntanathanom [BGV11], ktorý nevyužíva bootstrapping ale inú metódu redukcie šumu v šifrovom texte, tzv. škálovanie rozsahu.

Najprv prezentujeme základnú šifrovaciu schému. Potom popíšeme techniky umožňujúce homomorfné vyhodnocovania a redukciu šumu, s použitím ktorých následne zostavíme stupňovito plne homomorfnú schému. Na záver analyzujeme bezpečnosť a uvedieme autormi navrhované optimalizácie.

Všetky lemy, vety a odhady zložitosti v tejto kapitole sú prebrané z práce [BGV11].

3.1 Základná schéma

Budeme používať okruh $R = \mathbb{Z}$, pre $q \in \mathbb{N}$ budeme označovať $R_q = \{r \in R \mid r \in (-q/2, q/2\rangle\}$, pre $a \in R$ budeme označovať $[a]_q = a', a' \in R_q, a' = a \bmod q$. Skalárny súčin vektorov $\vec{u}, \vec{v} \in R^n$ budeme označovať $\langle \vec{u}, \vec{v} \rangle$.

Generovanie kľúčov:

1. Na základe bezpečnostného parametra zvolíme dimenziu $n \in \mathbb{N}$, modulus $q \in \mathbb{N}$ a rozdelenie χ nad $\mathbb{Z}$ také, že existuje $B_\chi \in \mathbb{N}$, že ak zvolíme $a \in \mathbb{Z}$ na základe χ, tak pravdepodobnosť $|a| > B_\chi$ je zanedbateľná.[1]

2. Položíme $\mathcal{P}_\xi = R_2 = \{0, 1\}$ a $\mathcal{C}_\xi = R_q^{n+1}$.

[1] Konkrétnu voľbu parametrov spomenieme pri analýze bezpečnosti schémy, teraz je podstatné, že $B_\chi << q/2$

3. Zvolíme $\vec{s}_0 \in R_q^n$, kde jednotlivé koeficienty volíme na základe rozdelenia χ. Za súkromný kľúč položíme $\vec{s} = (1, \vec{s}_0) \in R_q^{n+1}$.

4. Položíme $N = \lceil (2n+1) \log q \rceil$, zvolíme rovnomerne náhodne maticu $A_0 \in R_q^{n \times N}$ a vektor $\vec{e} \in R_q^N$ na základe rozdelenia χ. Položíme $\vec{b} = \vec{s}_0 \cdot A_0 + 2\vec{e}$. Za verejný kľúč položíme maticu $A \in R_q^{(n+1) \times N}$

$$A = \begin{pmatrix} \vec{b} \\ -A_0 \end{pmatrix}$$

5. $KeyGen_\xi(1^\lambda) \to (\mathcal{P}_\xi, \mathcal{C}_\xi, A, \vec{s})$

Šifrovanie

1. Pre $m \in R_2$ položíme $\vec{m} = (m, 0, \ldots, 0) \in R_q^{n+1}$. Rovnomerne náhodne zvolíme $\vec{r} \in R_2^N$.

2. $E_\xi(A, m) \to \vec{m} + \vec{r} \cdot A^T$

Dešifrovanie $D_\xi(\vec{s}, \vec{c}) = \Big[[\langle \vec{c}, \vec{s} \rangle]_q \Big]_2$

3.1.1 Korektnosť

Lema 9. *Nech $E_\xi(A, m) \to \vec{c}$. Potom (až na zanedbateľné množstvo prípadov) platí:*

$$|\langle \vec{c}, \vec{s} \rangle| \leq 1 + 2 \cdot \lceil (2n+1) \cdot \log q \rceil \cdot B_\chi$$

Dôkaz.

$$\begin{aligned} \langle \vec{c}, \vec{s} \rangle &= \left\langle \vec{m} + \vec{r} \cdot A^T, \vec{s} \right\rangle \\ &= \langle \vec{m}, \vec{s} \rangle + \left\langle \vec{r} \cdot A^T, \vec{s} \right\rangle \\ &= m + \vec{r} \cdot A^T \cdot \vec{s}^T \\ &= m + \vec{r} \cdot 2\vec{e}^T \end{aligned}$$

Teda $|\langle \vec{c}, \vec{s} \rangle| = \left| m + \vec{r} \cdot 2\vec{e}^T \right|$. Ak $\vec{r} = (r_1, \ldots r_N)$ a $\vec{e} = (e_1, \ldots, e_N)$, potom

$$|\langle \vec{c}, \vec{s} \rangle| \leq 1 + 2 \cdot \sum_{i=1}^{N} |r_i| \cdot |e_i| \leq 1 + 2 \cdot N \cdot B_\chi$$

□

Veta 11. *Ak* $1 + 2 \cdot N \cdot B_\chi < q/2$*, tak schéma* ξ *je korektná.*

Dôkaz. $D_\xi(\vec{s}, \vec{c}) = \left[\left[\langle \vec{c}, \vec{s} \rangle\right]_q\right]_2 = \left[\left[m + \vec{r} \cdot 2\vec{e}^T\right]_q\right]_2$ podľa lemy 9 je $|\langle \vec{c}, \vec{s} \rangle| < q/2$ a teda $\left[\left[m + \vec{r} \cdot 2\vec{e}^T\right]_q\right]_2 = \left[m + \vec{r} \cdot 2\vec{e}^T\right]_2 = m$ □

3.2 Zámena klúča

Keďže skalárny súčin je lineárny, vhodnu voľbou parametrov vieme zabezpečiť čiastočnú aditívnu homomorfnosť schémy ξ. Budeme sa teda sústrediť na násobenie.

Dešifrovaciu funkciu $D_\xi(\vec{s}, \vec{c})$ vieme vyjadriť ako $\left[\left[L_{\vec{c}}(\vec{s})\right]_q\right]_2$, kde $L_{\vec{c}}(\vec{s})$ je funkcia lineárne závislá na koeficientoch $\vec{s} = (s_1, \ldots, s_{n+1})$. Ak m_1, m_2 sú otvorené texty a $\vec{c}_1, \vec{c}_2$ ich zašifrované podoby, potom

$$\begin{aligned} m_1 \cdot m_2 &\equiv \left[L_{\vec{c}_1(\vec{s})}\right]_q \cdot \left[L_{\vec{c}_2(\vec{s})}\right]_q \bmod 2 \\ &\equiv \left[L_{\vec{c}_1}(\vec{s}) \cdot L_{\vec{c}_2}(\vec{s})\right]_q \bmod 2 \end{aligned}$$

ak je veľkosť šumu malá, t.j. $|L_{\vec{c}_1}(\vec{s}) \cdot L_{\vec{c}_2}(\vec{s})| < q/2$.

Súčin $L_{\vec{c}_1}(\vec{s}) \cdot L_{\vec{c}_2}(\vec{s})$ môžme vyjadriť ako $Q_{\vec{c}_1,\vec{c}_2}(\vec{s})$ - kvadratickú funkciu koeficientov $\vec{s}$. Ak označíme $\vec{s'} = \vec{s} \otimes \vec{s} = (s_1 s_1, s_1 s_2, \ldots, s_1 s_{n+1}, s_2 s_2, s_2 s_3, \ldots, s_{n+1} s_{n+1})$, potom vieme $Q_{\vec{c}_1,\vec{c}_2}(\vec{s})$ vyjadriť lineárnou funkciou $L^{long}_{\vec{c}_1,\vec{c}_2}(\vec{s'})$. Ak označíme vektor koeficientov $L^{long}_{\vec{c}_1,\vec{c}_2}$ ako $\vec{c'}$, potom $m_1 \cdot m_2$ vieme získať ako $D_\xi(\vec{s'}, \vec{c'})$.

Takto nám ale narastie dimenzia $\vec{s'}, \vec{c'}$ na $n' = \binom{n+2}{2}$. Nebyť tohto nárastu dimenzie, vedeli by sme – do istej hĺbky obvodu – homomorfne vyhodnocovať aj multiplikatívne hradlá. Ukážeme, ako zameniť dvojicu $\vec{s'}, \vec{c'}$ za $\vec{s}, \vec{c}$ (menšej dimenzie) tak, aby $D_\xi(\vec{s'}, \vec{c'}) = D_\xi(\vec{s}, \vec{c})$.

Zavedieme najprv expandujúce procedúry:

- $BitDecomp(\vec{x} \in R_q^n) = (\vec{u}_0, \ldots, \vec{u}_{\lfloor \log q \rfloor}) \in R_2^{n\lfloor \log q \rfloor + 1}$, kde $\vec{u}_i \in R_2^n$ a $\vec{x} = \sum_{i=0}^{\lfloor \log q \rfloor} 2^i \cdot \vec{u}_i \bmod q$
- $Powersof2(\vec{x} \in R_q^n) = (\vec{x}, 2 \cdot \vec{x} \bmod q, \ldots, 2^{\lfloor \log q \rfloor} \cdot \vec{x} \bmod q) \in R_q^{n\lfloor \log q \rfloor + 1}$

Lema 10. *Nech* $\vec{c}, \vec{s} \in R_q^n$*. Potom*

$$\langle BitDecomp(\vec{c}), Powersof2(\vec{s}) \rangle \equiv \langle \vec{c}, \vec{s} \rangle \bmod q$$

Dôkaz.

$$\begin{aligned}\langle BitDecomp(\vec{c}), Powersof2(\vec{s})\rangle &\equiv \sum_{i=0}^{\lfloor \log q \rfloor} \left\langle \vec{u}_i, 2^i \cdot \vec{s}_j \right\rangle \bmod q \\ &\equiv \sum_{i=0}^{\lfloor \log q \rfloor} \left\langle 2^i \cdot \vec{u}_i, \vec{s}_j \right\rangle \bmod q \\ &\equiv \left\langle \sum_{i=0}^{\lfloor \log q \rfloor} 2^i \cdot \vec{u}_i, \vec{s}_j \right\rangle \equiv \langle \vec{c}, \vec{s} \rangle \bmod q\end{aligned}$$

□

Zámena kľúča sa potom skladá z dvoch procedúr $SwitchKeyGen$ a $SwitchKey$, kde prvá zo súkromných kľúčov vygeneruje verejnú informáciu, na základe ktorej druhá dokáže zameniť šifrové texty ($n_1, n_2 \in \mathbb{N}$ sú dimenzie vektorov $\vec{s_1}, \vec{s_2}$, v princípe ľubovoľné).

$SwitchKeyGen_\xi(\vec{s}_1 \in R_q^{n_1}, \vec{s}_2 \in R_q^{n_2})$:

Vygenerujeme verejný kľúč A zodpovedajúci $\vec{s}_2$, ako je popísané v predchádzajúcej časti, s tým rozdielom, že namiesto N použijeme $N_1 = n_1 \cdot (\lfloor \log q \rfloor + 1)$. Ako výstup procedúry položíme maticu $B \in R_q^{n_2 \times N_1}$:

$$B = A + \begin{pmatrix} Powersof2(\vec{s_1}) \\ \vec{0} \end{pmatrix}$$

$SwitchKey(B \in R_q^{n_2 \times n_1 \cdot (\lfloor \log q \rfloor + 1)}, \vec{c}_1 \in R_q^{n_1}) = B \cdot BitDecomp(\vec{c}_1)^T \in R_q^{n_2}$

Lema 11. *Nech $\vec{s}_1, \vec{c}_1 \in R_q^{n_1}$, $\vec{s}_2 \in R_q^{n_2}$, $B = SwitchKeyGen(\vec{s_1}, \vec{s_2})$ a $c_2 = SwitchKey(B, \vec{c_1})$, A je verejný kľúč k $\vec{s}_2$, $\vec{s}_2 \cdot A = 2\vec{e}_2$. Potom*

$$\langle \vec{c}_2, \vec{s}_2 \rangle \equiv 2 \langle BitDecomp(\vec{c}_1), \vec{e_2} \rangle + \langle \vec{c}_1, \vec{c}_2 \rangle \bmod q$$

Dôkaz.

$$\begin{aligned}\langle \vec{c}_2, \vec{s}_2 \rangle &= \vec{s}_2 \cdot (B \cdot BitDecomp(\vec{c}_1)^T) \\ &= (2\vec{e}_2 + Powersof2(\vec{s}_1)) \cdot BitDecomp(\vec{c}_1)^T \\ &\equiv 2\vec{e}_2 \cdot BitDecomp(\vec{c}_1)^T + \langle \vec{s}_1, \vec{c}_1 \rangle \bmod q \\ &\equiv 2 \langle BitDecomp(\vec{c}_1), \vec{e_2} \rangle + \langle \vec{c}_1, \vec{c}_2 \rangle \bmod q\end{aligned}$$

□

Takto dokážeme redukovať dimenziu šifrového textu so zachovaním korektnosti dešifrovania kým $|2\langle BitDecomp(\vec{c}_1), \vec{e_2}\rangle| + |\langle \vec{c}_2, \vec{s}_2\rangle| < q/2$ - čo sa líši od podmienky na korektnosť dešifrovania $\vec{c_1}$ nanjvýš o $|2\langle BitDecomp(\vec{c}_1), \vec{e_2}\rangle|$, čo spadá do $O(n_1 \cdot \log q \cdot B_\chi)$, keďže $BitDecomp(\vec{c}_1)$ má koeficienty z $\{0, 1\}$.

3.3 Škálovanie rozsahu

Ak by sme rozšírili súkromný kľúč zákaldnej schémy ξ o množinu súkromných kľúčov rôznych inštancií $\{\vec{s}_i \in R_q^{n+1}\}$ a verejný kľúč o množinu zodpovdajúcich matíc $\{B_i = SwitchKeyGen(\vec{s}_i, \vec{s}_{i+1})\}$, tak vieme získať čiastočne homomorfnú schému, pričom veľkosť šumu[2] pri vyhodnotení aditívneho hradla rastie lineárne a pri multiplikatívnom hradle exponenciálne: ak $\left|[\langle \vec{c}_1, \vec{s}\rangle]_q\right|, \left|[\langle \vec{c}_2, \vec{s}\rangle]_q\right| \leq k$, potom $\left|[\langle \vec{c}_1, \vec{s}\rangle + \langle \vec{c}_2, \vec{s}\rangle]_q\right| \leq 2k$ a $\left|[\langle \vec{c}_1, \vec{s}\rangle \cdot \langle \vec{c}_2, \vec{s}\rangle]_q\right| \leq k^2$.

Hlavnou myšlienkou redukcie šumu je transformácia dešifrovacej funkcie z tvaru $\left[[\langle \vec{c}, \vec{s}\rangle]_q\right]_2$ na $\left[\left[\left\langle \vec{c'}, \vec{s}\right\rangle\right]_p\right]_2$, kde $p \in \mathbb{N}$ je nový menší modulus, a $\vec{c'}$ získame škálovaním $\vec{c} \cdot (p/q)$ a správnym zaokrúhlením koeficientov. Takto sa zmenší veľosť šumu $\left|\left[\left\langle \vec{c'}, \vec{s}\right\rangle\right]_q\right| \approx \left|[\langle \vec{c}, \vec{s}\rangle]_q\right| \cdot (p/q)$. Neprekáža nám, že o rovnaký faktor sa zmenší aj modulus, a teda aj maximálna prípustná veľkosť šumu: naprkílad ak šum v šifrových textoch $\approx k$, a máme postupnosť modulov veľkostí približne $k^8, k^7, k^6 \ldots$, tak pri násobení a škálovaní šifrových textov je veľkosť šumu stále $\approx k$ a teda pomer veľkosť šumu/veľkosť modulu sa zmenšuje lineárne, len o faktor k. Ak by sme nepoužívali škálovanie, tak veľkosť šumu po násobení je postupne $\approx k^2, k^4, k^8$, teda pomer veľkosť šumu/veľkosť modulu klesá exponenciálne.

Definujeme operáciu škálovania nasledovne: Nech $\vec{x} \in \mathbb{Z}^n$, $q > p > 2$. Potom $Scale(\vec{x}, q, p)$ je vektor $\vec{x'} \in \mathbb{Z}^n$ taký, že $\vec{x} = \vec{x'} \bmod 2$ a $\left|\vec{x} - \vec{x'}\right|$ je minimálna.

Lema 12. *Nech $q > p > 2$ sú nepárne, nech $\vec{c} = (c_1, \ldots, c_n) \in R^n$, $\vec{c'} = (c'_1, \ldots, c'_n) = Scale(\vec{c}, q, p)$, nech $\vec{s} = (s_1, \ldots, s_n) \in R^n$, $l_1(\vec{s}) = \sum_{i=1}^n |s_i|$ a platí*

$$\left|[\langle \vec{c}, \vec{s}\rangle]_q\right| < q/2 - (q/p) \cdot l_1(\vec{s})$$

[2]Pod veľkosťou šumu v $\vec{c}$ rozumieme $\left|[\langle \vec{c}, \vec{s}\rangle]_q\right|$ a maximálnou veľkosťou šumu pre modulus q je $q/2$. Môže sa zdať, že toto obmedzenie na veľkosť šumum je triviálne, keďže $\forall a \in R : \left|[a]_q\right| \leq q/2$. Pre nás je ale dôležité, aby pri homomorfnom vyhodnocovaní nepretiekla veľkosť šumu cez túto hranicu, t.j. aby súčet, resp. súčin šumov pôvodných textov bol $\leq q/2$.

Potom

$$\left[\left\langle \vec{c'}, \vec{s} \right\rangle\right]_p \equiv \left[\langle \vec{c}, \vec{s} \rangle\right]_q \bmod 2$$

a

$$\left|\left[\left\langle \vec{c'}, \vec{s} \right\rangle\right]_p\right| < (p/q) \cdot \left|\left[\langle \vec{c}, \vec{s} \rangle\right]_q\right| + l_1(\vec{s})$$

Dôkaz. Zrejme $\left[\langle \vec{c}, \vec{s} \rangle\right]_q = \langle \vec{c}, \vec{s} \rangle - k \cdot q$ pre nejaké $k \in R$. Označme $e_p = \left\langle \vec{c'}, \vec{s} \right\rangle - k \cdot p$. Zrejme $[e_p]_p = \left[\left\langle \vec{c'}, \vec{s} \right\rangle\right]_q$. Taktiež platí

$$\begin{aligned}
|e_p| &= \left|-k \cdot q + \langle (p/q) \cdot \vec{c}, \vec{s} \rangle + \left\langle \vec{c'} - (p/q)\vec{c}, \vec{s} \right\rangle\right| \\
&\leq |-k \cdot q + \langle (p/q) \cdot \vec{c}, \vec{s} \rangle| + \left|\left\langle \vec{c'} - (p/q)\vec{c}, \vec{s} \right\rangle\right| \\
&\leq (p/q) \cdot |\langle \vec{c}, \vec{s} \rangle| + \sum_{i=1}^{n} |c'_i - (p/q) \cdot c_i| \cdot |s_i| \\
&\leq (p/q) \cdot |\langle \vec{c}, \vec{s} \rangle| + l_1(\vec{s}) \\
&< p/2
\end{aligned}$$

teda $e_p = [e_p]_p = \left[\left\langle \vec{c'}, \vec{s} \right\rangle\right]_p$, čím sme ukázali platnosť ohraničenia na $\left[\left\langle \vec{c'}, \vec{s} \right\rangle\right]_p$. Ďalej platí $\left[\left\langle \vec{c'}, \vec{s} \right\rangle\right]_p = e_p = \left\langle \vec{c'}, \vec{s} \right\rangle - k \cdot p \equiv \langle \vec{c}, \vec{s} \rangle - k \cdot q = \left[\langle \vec{c}, \vec{s} \rangle\right]_q \bmod 2$. □

Z tejto lemy vyplýva, že ak nový modulus je menší než predchádzajúci a $\vec{s}$ je krátky vektor, tak vieme jednoducho transformovať šifrový text so zachovaním korektnosti dešifrovania pod novým modulom, a zároveň dosiahnuť redukciu veľkosti šumu.

3.4 Plne homomorfná schéma

Na základe uvedených procedúr dokážeme zostaviť stupňovito plne homomorfnú schému $\Psi = \{\xi^d \mid d \in \mathbb{N}\}$.

Generovanie kľúčov:

1. Zvolíme postupnosť modulov $q_0 > \ldots > q_d \in \mathbb{N}$ tak, že q_i má $(d - i + 1) \cdot \mu$ bitov, kde $\mu \in \mathbb{N}$ je parameter, ktorý špecifikujeme pri analýze schémy. $\mathcal{P}_{\xi^d} = R_2$.

2. Pre $0 \leq i \leq d$ vygenerujeme $KeyGen(1^\lambda) \rightarrow (\mathcal{C}_i = R_{q_i}^{n_i}, A_i \in R_{q_i}^{n_i \times N_i}, \vec{s}_i \in R_{q_i}^{n_i})$

3. Pre $0 \leq i \leq d-1$ označíme $\vec{s'}_i = \vec{s}_i \otimes \vec{s}_i$, $\vec{s''}_i = BitDecomp(\vec{s'}_i)$ a $B_i = SwitchKeyGen(\vec{s''}_i, \vec{s}_{i+1})$.

4. Položíme $\mathcal{C}_{\xi^d} = \{(\vec{c}, i) \mid 0 \leq i \leq d, \vec{c} \in \mathcal{C}_i\}$, $sk = (\vec{s}_0, \ldots, \vec{s}_d)$ a $pk = (A_0, \ldots, A_d, B_0, \ldots B_{d-1})$.

5. $KeyGen_{\xi^d}(1^\lambda) \rightarrow (\mathcal{P}_{\xi^d}, \mathcal{C}_{\xi^d}, pk, sk)$

Šifrovanie: $E_{\xi^d}(pk, m) = (E_\xi(A_0, m), 0)$
Dešifrovanie: $D_{\xi^d}(sk, (\vec{c}, i)) = D_\xi(\vec{s}_i, \vec{c})$

3.4.1 Homomorfné vyhodnocovanie

Pre jednoduchosť sa budeme zaoberať len obvodmi s hradlami s 2 vstupmi. Obvod O nad $\mathcal{P}_{\xi^d} = R_2$ budeme vyhodnocovať tak, že na vstupy dáme zašifrované podoby príslušných otvorených textov, a jednotlivé hradlá budeme emulovať pomocou operácií $Add_{\xi^d}, Mult_{\xi^d} : \mathcal{C}_{\xi^d} \times \mathcal{C}_{\xi^d} \rightarrow \mathcal{C}_{\xi^d}^{long} = \{(\vec{c}, i) \mid \vec{c} \in R_{q_i}^{\binom{n_i+1}{2}}, 0 \leq i \leq d-1\}$. Najprv ale popíšeme operácie $Recrypt_{\xi^d} : \mathcal{C}_{\xi^d}^{long} \rightarrow \mathcal{C}_{\xi^d}$ a $Expand_{\xi^d} : \mathcal{C}_{\xi^d} \rightarrow \mathcal{C}_{\xi^d}^{long}$.

Recrypt:

Táto operácia transformuje šifrový text pod $\vec{s'}_i$ a modulom q_i na šifrový text pod $\vec{s}_{i+1}$ a modulom q_{i+1}. Pomocou nej budeme emulovať hradlá vyhodnocovaného obvodu.

1. vstup: $(\vec{c}, i)$
2. $\vec{c}_1 = Powersof2(\vec{c})$
3. $\vec{c}_2 = Scale(\vec{c}_1, q_i, q_{i+1})$
4. $\vec{c}_3 = SwitchKey(B_i, \vec{c}_2)$
5. $Recrypt_{\xi^d}(\vec{c}, i) = (\vec{c}_3, i+1)$.

Expand:

Na vstupe $(\vec{c}, i)$ táto operácia expanduje vektor $\vec{c} \in R_{q_i}^{n_i}$ na vektor $\vec{c}_1 \in R_{q_i}^{n_i \times N_i}$ tak, že $\langle \vec{c}, \vec{s}_i \rangle = \left\langle \vec{c}_1, \vec{s'}_i \right\rangle$. Je zrejmé, že ak $\vec{c} = (c_1, \ldots, c_{n_i})$, tak $\vec{c}_1 = (c_1, \ldots, c_{n_i}, 0, \ldots, 0)$ vyhovuje požiadavke.

Sčitovanie:

1. Vstup:$(\vec{c}_1, i), (\vec{c}_2, j)$. Ak $i > j$, tak pomocou operácií $Expand_{\xi^d}$ a $Recrypt_\xi$ vieme transformovať $(\vec{c}_2, j)$ tak, aby $i = j$. Uvažujme teda $i = j$.
2. $\vec{c'} = \vec{c}_1 + \vec{c}_2$
3. $\vec{c} = Expand_{\xi^d}(\vec{c}_3, i)$
4. $Add_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, j)) = Recrypt_{\xi^d}(\vec{c}_4, i)$

Násobenie: $Mult_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, j))$

1. Vstup: $(\vec{c}_1, i), (\vec{c}_2, j)$, opäť predpokladáme, že $i = j$.
2. Označíme $\vec{c} \in R_{q_i}^{n_i \times N_i}$ vektor koeficientov lineárnej funkcie $L^{long}_{\vec{c}_1, \vec{c}_2}$ popísanej v časti 3.2.
3. $Mult_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, j)) = Recrypt_{\xi^d}(\vec{c}, i)$

3.4.2 Korektnosť

Chceme ukázať, že vieme zvoliť parametre schémy tak, aby všetky obvody hĺbky nanajvýš d patrili medzi prípustné obvody schémy ξ^d, a teda že schéma Ψ je stupňovito plne homomorfná. Menovite, potrebujeme špecifikovať hodnotu μ, dimenzie vektorov n_i a rozdelenie χ.

Z bezpečnostných požiadaviek vyplynie, že potrebujeme $n_i \in \Omega(\lambda \cdot \log(q_i/B_\chi))$, a B_χ aspoň sublineárne od n_i. Teda môžme položiť $B_\chi = n_0$, $n_i = \lambda \cdot \log q_i$. Ostáva teda určiť μ.

Najprv určíme univerzálnu hranicu $L \in \mathbb{N}$, takú, že všetky "validné" [3] šifrové texty $(\vec{c}, i)$ budú mať veľkosť šumu menšiu než L, t.j. $\left|[\langle \vec{c}, \vec{s}_i \rangle]_{q_i}\right| < L$.

Aby toto obmedzenie platilo pre výstupy E_{ξ^d}, potrebujeme podľa lemy 9 $L \in \Omega(\lambda^2 \cdot \log^3 q_0)$. Keďže operácia sčítanie zväčšuje veľkosť šumu v porovnaní s násobením zanedbateľne, sústredíme sa na operáciu $Mult_{\xi^d}$. Ak veľkosť šumu vstupov je $< L$, potom $\left|\left[\left\langle \vec{c}, \vec{s'}_i \right\rangle\right]_{q_i}\right| < L^2$.

V procedúre $Recrypt_{\xi^d}$ expanzia šifrového textu podľa lemy 10 nemení veľkosť šumu, teda $\left|\left[\left\langle \vec{c}_1, \vec{s''}_i \right\rangle\right]_{q_i}\right| < L^2$. Škálovanie podľa lemy 12 zmenší veľkosť šumu

[3] t.j. získané ako výstup E_{ξ^d} alebo vyhodnotením obvodu s hĺbkou menšou než d

$\left|\left[\left\langle \vec{c}_2, \vec{s''}_i \right\rangle\right]_{q_{i+1}}\right| < (q_{i+1}/q_i) \cdot L^2 + \gamma_{scale},\ \gamma_{scale} \in O(\lambda^2 \cdot \log^2 q_0)$. Zámena kľúča podľa lemy 11 zmení veľkosť šumu o aditívny term $\gamma_{swap} \in O(\lambda^2 \cdot \log^3 q_0)$ na $\left|[\langle \vec{c}_3, \vec{s}_{i+1} \rangle]_{q_{i+1}}\right| < (q_{i+1}/q_i) \cdot L^2 + \gamma_{scale} + \gamma_{swap}$.

Teda aby naše ohraničenie na veľkosť šumu platilo, potrebujeme $(0 \leq i \leq d-1)$

$$(q_{i+1}/q_i) \cdot L^2 + \gamma_{scale} + \gamma_{swap} \leq L$$

Aby táto podmienka platila, stačí zvoliť parametre tak, aby súčasne platilo:

$L \geq 2 \cdot (\gamma_{scale} + \gamma_{swap})$

$(q_i/q_{i+1}) \geq 2 \cdot L$

Jednou z možností je zvoliť $L = \lambda^a \cdot d^b$ pre dosť veľké $a, b \in \mathbb{N}$ a $q_i \approx 2^{(d-i+1)\cdot\omega(\log\lambda\cdot\log d)}$. Potom platia predchádzajúce podmienky, ako aj $L \in \Omega(\lambda^2 \cdot \log^3 q_0)$.

Teraz môžme vysloviť lemy o korektnosti operácií $Recrypt_{\xi^d}$, Add_{ξ^d} a $Mult_{\xi^d}$:

Lema 13. *Ak* $\left|\left[\left\langle \vec{c}, \vec{s'}_i \right\rangle\right]_{q_i}\right| < L$, $0 \leq i \leq d-1$, *potom*

$$\left|\left[\left\langle Recrypt_{\xi^d}(\vec{c}, i), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}}\right| < L$$
$$\left[\left\langle Recrypt_{\xi^d}(\vec{c}, i), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}} \equiv \left[\left\langle \vec{c}, \vec{s'}_i \right\rangle\right]_{q_i} \bmod 2$$

Dôkaz. Vyplýva z liem 10, 11 a 12. □

Lema 14. *Ak* $\left|[\langle \vec{c}_1, \vec{s}_i \rangle]_{q_i}\right| < L$ *a* $\left|[\langle \vec{c}_2, \vec{s}_i \rangle]_{q_i}\right| < L$, *potom*

$$\left|\left[\left\langle Add_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, i)), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}}\right| < L$$
$$\left[\left\langle Add_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, i)), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}} \equiv [\langle \vec{c}_1, \vec{s}_i \rangle]_{q_i} + [\langle \vec{c}_2, \vec{s}_i \rangle]_{q_i} \bmod 2$$

Dôkaz. $\vec{c'} = \vec{c}_1 + \vec{c}_2$, teda

$$\begin{aligned}\left[\left\langle \vec{c'}, \vec{s}_i \right\rangle\right]_{q_i} &= [\langle \vec{c}_1, \vec{s}_i \rangle + \langle \vec{c}_2, \vec{s}_i \rangle]_{q_i} \\ &= [\langle \vec{c}_1, \vec{s}_i \rangle]_{q_i} + [\langle \vec{c}_2, \vec{s}_i \rangle]_{q_i}\end{aligned}$$

Z lemy 13 vyplýva, že $\left[\left\langle Add_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, i)), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}} \equiv \left[\left\langle \vec{c'}, \vec{s}_i \right\rangle\right]_{q_i} \bmod 2$. □

Lema 15. *Ak* $\left|[\langle \vec{c}_1, \vec{s}_i \rangle]_{q_i}\right| < L$ *a* $\left|[\langle \vec{c}_2, \vec{s}_i \rangle]_{q_i}\right| < L$, *potom*

$$\left|\left[\left\langle Mult_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, i)), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}}\right| < L$$
$$\left[\left\langle Add_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, i)), \vec{s}_{i+1} \right\rangle\right]_{q_{i+1}} \equiv [\langle \vec{c}_1, \vec{s}_i \rangle]_{q_i} \cdot [\langle \vec{c}_2, \vec{s}_i \rangle]_{q_i} \bmod 2$$

Dôkaz. Z definície funkcie $L^{long}_{\vec{c}_1,\vec{c}_2}$ vyplýva, že $[\langle \vec{c}_1, \vec{s}_i\rangle]_{q_i} \cdot [\langle \vec{c}_2, \vec{s}_i\rangle]_{q_i} = \left[\left\langle \vec{c}, \vec{s'}_i \right\rangle\right]_{q_i}$. Z lemy 13 vyplýva, že $\left[\left\langle Mult_{\xi^d}((\vec{c}_1, i), (\vec{c}_2, i)), \vec{s}_{i+1}\right\rangle\right]_{q_{i+1}} \equiv \left[\left\langle \vec{c}, \vec{s'}_i \right\rangle\right]_{q_i} \bmod 2$. □

3.5 Bezpečnosť schémy

Bezpečnosť základnej schémy ξ je posavená na tzv. LWE (learning with errors) probléme:

Definícia 13. *Nech $n \in \mathbb{N}$ je dimenzia, $q \in \mathbb{N}, q \geq 2$ je modulus, a χ je rozdelenie nad $\mathbb{Z}$ a $\vec{s'} \in \mathbb{Z}_q^n$ je rovnomerne náhodný tajný vektor. Potom $LWE_{n,q,\chi}$ problém je nasledovný: Zvolíme bit $b \in \{0, 1\}$. Ak $b = 0$, tak rovnomerne náhodne zvolíme $(\vec{v}, r) \in \mathbb{Z}_q^{n+1}$. Inak rovnomerne náhodne zvolíme $\vec{v} \in \mathbb{Z}_q^n$, zvolíme $e \in \mathbb{Z}$ podľa rozdelenia χ a položíme $r = \left\langle \vec{v}, \vec{s'} \right\rangle + e \bmod q$. Úlohou je na základe $(\vec{v}, r)$ určiť b.*

$LWE_{n,q,\chi}$ predpoklad je že $LWE_{n,q,\chi}$ problém je ťažký.

Analýzou tohto problému sa nebudeme podrobnejšie zaoberať. Bolo ukázané, že napríklad pre gaussovo rozdelenie χ a isté moduly q $LWE_{n,q,\chi}$ predpoklad platí, ak isté problémy v mriežkach sú ťažké.

Presnejšie, pre rozdelenie χ také, že pravdepodobnosť výberu prvku $|a| > B_\chi$ je zanedbateľná vzhľadom na n, B_χ je sublineárne od n a $n \in \Omega(\lambda \cdot \log(q/B_\chi))$, je časová zložitosť algoritmu riešiaceho $LWE_{n,q,\chi}$ problém aspoň 2^λ.

Taktiež bolo ukázané, že ak je $LWE_{n,q,\chi}$ problém ťažký pre $\vec{s}$ rovnomerne náhodne zvolený z R_q^n, tak je rovnako ťažký aj pre $\vec{s}$ volené na základe rozdelenia χ.

V schéme ξ má šifrový text tvar $(r, \vec{v})$, kde $\vec{v}$ je súčet nejakej podmnožiny stĺpcov matice A_0 a $r = \left\langle -\vec{v}, \vec{s'} \right\rangle + 2e + m$, kde e je súčet podmnožiny koeficientov $\vec{e}$. Na základe $LWE_{n,q,\xi}$ predpokladu môžme usúdiť, že r v uvedenom tvare je výpočtovo neodlíšiteľné od náhodného r.

Bezpečnosť schémy Ψ možno ukázať podobným spôsobom ako v časti 1.6.3.

3.6 Zložitosť schémy

Súkromný kľúč schémy ξ^d je $(\vec{s}_0, \ldots, \vec{s}_d) \in R_{q_0}^{n_0} \times \ldots \times R_{q_d}^{n_d}$, teda jeho veľkosť je $O(d \cdot n_0 \cdot \log q_0) = \widetilde{O}(d^3 \cdot \lambda)$. Keďže koeficienty $\vec{s}_i$ sú volené na základe rozdelenia χ s ohraničením B_χ, môžme si jednotlivé koeficienty pamätať na $O(B_\chi) = O(n_0)$ bitoch, čím redukujeme veľkosť súkromného kľúča na $\widetilde{O}(d^2 \cdot \lambda)$.

Verejný kľúč sa skladá z $(A_0, \ldots, A_d, B_0, \ldots B_{d-1})$, kde $A_i \in R_{q_i}^{n_i \times N_i}$ a $B_i \in R_{q_{i+1}}^{n_{i+1} \times n_i \cdot \lceil \log q_{i+1} \rceil}$, teda jeho veľkosť je $O(d \cdot n_0^2 \cdot \log^2 q_0) = \widetilde{O}(d^4 \cdot \lambda)$.

Veľkosť šifrového textu je $O(n_0 \cdot \log q_0) = \widetilde{O}(d^2 \cdot \lambda)$.

Homomorfné vyhodnotenie jedného hradla sa skladá z operácií Add_{ξ^d} resp. $Mult_{\xi^d}$, $Powersof2$, $Scale$ a $SwitchKey$. Sčítanie dvoch šifrových textov vieme realizovať v čase $O(n_0 \cdot \log q_0) = \widetilde{O}(d^2 \cdot \lambda)$, násobenie v čase $O(n_0^2 \cdot \log q_0) = \widetilde{O}(d^3 \cdot \lambda^2)$.

Vstupom do funkcie $Powersof2$ je expandovaný $\vec{c} \in R_{q_i}^{\binom{n_i+1}{2}}$. Ak označíme $\vec{c} = (c_1, \ldots, c_{\binom{n_i+1}{2}})$, tak potrebujeme zrátať $2^k \cdot c_j, 0 \leq k \leq \lceil \log q_i \rceil$, čo vieme v čase $O(n_i^2 \cdot \log^2 q_i)$. Vieme ale, že jednotlivé koeficienty $\vec{s_i}$ sú ohraničené B_χ, teda koeficienty $\vec{s'}_i$ ohraničené B_χ^2. To nám umožní zmenšiť dĺžku $BitDecomp(\vec{s'}_i)$ z $O(n_0^2 \cdot \log d_0)$ na $O(n_0^2 \cdot \log n_0)$, a teda zanedbať pri výpočte $Powersof2$ koeficienty pre $k \geq 2 \log n_0$ a teda redukovať časovú zložitosť na $O(n_0^2 \cdot \log d_0) = \widetilde{O}(d^3 \cdot \lambda^2)$.

Vstupom do funkcie $Scale$ je $\vec{c} \in R_{q_i}^{\binom{n_i+1}{2} \cdot \lceil 2 \log B_\chi \rceil}$ ak používame optimalizovanú $Powersof2$. Potrebujeme jednotlivé koeficienty prenásobiť $(q_{i+1}/q_i) \approx 2^{\omega(\log \lambda \cdot \log d)}$, čo vieme v čase $\widetilde{O}(d^3 \cdot \lambda^2)$.

Napokon potrebujeme vyhodnotiť funkciu $SwitchKey$, ktorá má vstup $\vec{c} \in R_{q_i}^{\binom{n_i+1}{2} \cdot \lceil 2 \log B_\chi \rceil}$, t.j. vynásobiť $B_i \cdot \vec{c}^T$, čo vieme v čase $\widetilde{O}(d^5 \cdot \lambda^3)$.

Teda celková zložitosť homomorfného vyhodnotenia jedného hradla obvodu je $\widetilde{O}(d^5 \cdot \lambda^3)$.

3.7 Optimalizácie

3.7.1 RLWE

Jedným z problémov doteraz prezentovanej schémy bol kvadratický nárast počtu koeficientov šifrového textu pri homomorfnom násobení. Tento problém vieme odstrániť, ak pozmeníme okruh nad ktorým budeme pracovať: nahradíme celé čísla polynómami, a bezpečnosť postavíme na (pravdepodobne silnejšom) predpoklade:

Definícia 14. *Nech $f(x) = x^k + 1, k = 2^l$ je polynóm, $T = \mathbb{Z}[x]/(f(x))$, χ je rozdelenie nad $\mathbb{Z}$, $q \geq 2$ je modulus a $s \in T$ je rovnomerne náhodne zvolený tajný prvok. Potom $RLWE_{k,q,\chi}$ problém je nasledovný: Zvolíme bit $b \in \{0, 1\}$. Ak $b = 0$ tak rovnomerne náhodne zvolíme $(v, r) \in T_q^2$. Inak rovnomerne náhodne zvolíme $v \in T_q = T/qT$, zvolíme $e \in T_q$ s koeficientami podľa rozdelenia χ a položíme $r = v \cdot s + e$. Úlohou je na základe (v, r) určiť b. $RLWE_{k,q,\chi}$ predpoklad je, že $RLWE_{k,q,\chi}$ problém je ťažký.*

Bolo ukázané, že RLWE predpoklad platí pre $k \in \Omega(\lambda \cdot \log(q/B_\chi))$, ak isté problémy v ideálnych mriežkach sú ťažké – na rozdiel od LWE predpokladu, ktorý vyžadoval ťažké problémy vo všeobecných mriežkach. Na $RLWE_{k,q,\chi}$ predpoklade je postavená bepečnosť nasledovnej schémy ξ_{RLWE}, ktorá je v podstane analogická k schéme ξ.

Generovanie kľúčov:

1. na základe bezpečnostného parametra zvolíme stupeň $k = 2^l$, modulus $q \geq 2$, rozdelenie χ nad $\mathbb{Z}$ s ohraničením B_χ a n = 1.

2. Položíme $T = \mathbb{Z}[x]/(x^k + 1)$, označíme T_q množinu polynómov z T s koeficientami v $(-q/2, q/2\rangle$, operácia $[a]_q$ bude transformovať koeficienty $a \in T$ do $(-q/2, q/2\rangle$. Položíme $\mathcal{P}_{\xi_{RLWE}} = T_2$, $\mathcal{C}_{\xi_{RLWE}} = T_q$.

3. Zvolíme $s_0 \in T_q$, pričom jednotlivé koeficienty polynómu volíme na základe χ. Za súkromný kľúč položíme $\vec{s} = (1, s_0) \in T_q^2$.

4. Položíme $N = \lceil 3 \cdot \log q \rceil$, rovnomerne náhodne zvolíme maticu $A_0 \in T_q^{1\times N}$ a vektor $\vec{e} \in T_q^N$ na základe rozdelenia χ. Položíme $\vec{b} = s_0 \cdot A_0 + 2\vec{e}$. Za verejný kľúč zvolíme maticu $A \in T_q^{2\times N}$

$$A = \begin{pmatrix} \vec{b} \\ -A_0 \end{pmatrix}$$

5. $KeyGen_{\xi_{RLWE}} = (\mathcal{P}_{\xi_{RLWE}}, \mathcal{C}_{\xi_{RLWE}}, A, \vec{s})$

Šifrovanie:

1. Pre $m \in T_2$ položíme $\vec{m} = (m, 0) \in T_q^2$a rovnomerne náhodne zvolíme $\vec{r} \in T_2^N$

2. $E_{\xi_{RLWE}}(A, m) = \vec{m} + \vec{r} \cdot A^T$.

Dešifrovanie: $D_{\xi_{RLWE}}(\vec{s}, \vec{c}) = \left[[\langle \vec{c}, \vec{s} \rangle]_q \right]_2$

Stupňovito plne homomorfnú schému Ψ_{RLWE} skonštruujeme analogicky k Ψ. Keďže teraz sa pri násobení nezväčšuje počet koeficientov $L^{long}_{\vec{c_1},\vec{c_2}}$ kvadraticky, dosiahneme podstatne lepšiu zložitosť homomorfného vyhodnocovania. Konkrétne časová zložitosť homorfného vyhodnotenia jedného hradla bude $\widetilde{O}(d^3 \cdot \lambda)$.

3.7.2 Batching

Ak potrebujeme viackrát vyhodnotiť rovnaký obvod na rôznych vstupoch – označme vektory vstupov $\vec{m}_1, \ldots, \vec{m}_l$ – tak batching nám umožní skomprimovať viaceré zodpovedajúce si otvorené texty do jedného, čím získame vektor $\vec{m}$, ktorého komponenty potom môžme zašifrovať, homomorne vyhodnotiť, dešifrovať a následne dekomprimovať na výsledky operácií pre jednotlivé pôvodné vstupy, pričom asymptotická zložitosť homomorfného vyhodnotenia obvodu na "komprimovaných" šifrových textoch sa nezmení.

Budeme demonštrovať na schéme Ψ_{RLWE}. V doterajšej konštrukcii sme pre jednoduchosť mali $\mathcal{P}_{\Psi_{RLWE}} = T_2 = T/(2)$. Ak zvolíme prvočíslo $p > 2d$, potom môžme pracovať s $\mathcal{P}_{\Psi_{RLWE}} = T_p = T/(p)$. Budeme musieť pozmeniť dešifrovaciu funkciu na $\left[[\langle \vec{c}, \vec{s} \rangle]_q\right]_p$, pri generovaní verejného kľúča ξ_{RLWE} položiť $\vec{b} = s_0 \cdot A_0 + p\vec{e}$ namiesto $s_0 \cdot A_0 + 2\vec{e}$ a podobne pozmeniť $SwitchKeyGen$ a $Scale$. Taktiež sa nám zväčšia hodnoty γ_{scale} a γ_{swap}, ale pokiaľ je $p \in poly(\lambda)$, na asymptotickej zložitosti schémy to nič nezmení.

Pri vyhodnocovaných obvodoch sa môžme obmedziť na boolovské obvody zložené z XOR hradiel, ktoré vieme simulovať v ľubovoľnom okruhu: $a, b \in \{0, 1\} \subset T_p$, $XOR(a, b) = a + b - 2ab$.

Kompresiu šifrových textov docielime tak, že skonštruujeme ideály $P_1, \ldots, P_l \subseteq T$, vyjadríme šifrové texty jednotlivých sád vstupov $\vec{m}_i$ ako prvky v $T_{P_i} = T/P_i$. Ideály skonštruujeme tak, aby existoval izomorfizmus medzi T_p a kartézskym súčinom $T_{P_1} \times \ldots \times T_{P_l}$, pomocou ktorého budeme "komprimovať" a "dekomprimovať" otvorené texty.

Ak $a \in \mathbb{Z}_p$ je primitívny $2d$-ty koreň jednotky v $\mathbb{Z}_p$, tak označíme $a_i = a^{2i-1}$ a platí

$$x^d + 1 = \prod_{i=1}^{d} (x - a_i) \bmod p$$

Položíme $P_i = (p, x - a_i)$. Platí $(p) = \prod_{i=1}^{d} P_i$. Navyše sú P_i navzájom nesúdeliteľné - t.j. $i \neq j : P_i + P_j = T$, teda podľa čínskej zvyškovej vety T_p je izomorfné s $T_{P_1} \times \ldots \times T_{P_l}$.

3.7.3 Bootstrapping

Aj keď na konštrukciu stupňovitej FHE nepotrebujeme bootstrapovať, bootstrapping môže byť optimalizáciou s dvoch dôvodov:

- v doterajšej schéme Ψ, resp. Ψ_{RLWE} závisí čas vyhodnotenia jedného hradla od celkovej hĺbky vyhodnocovaného obvodu, čo pri veľkých obvodoch môže zavážiť.
- bootstrapping nám umožní vytvoriť plne homomorfnú schému, ak budeme predpokladať KDM-bezpečnosť schémy Ψ.

Budeme sa na našu stupňovitú FHE schému Ψ pozerať ako na čiastočne homomorfnú schému, z ktorej spôsobom prezentovaným v prvej kapitole pomocou bootstrappingu skonštruujeme stupňovitú FHE Υ_Ψ, resp. $\Upsilon_{\Psi_{RLWE}}$. Skúsime analyzovať zložitosť dešifrovacej funkcie Ψ:

$$\left[[\langle \vec{c}, \vec{s} \rangle]_q\right]_2$$

Nech $\vec{c} = (c_1, \ldots, c_n) \in R_q^n$ a $\vec{s} = (s_1, \ldots, s_n) \in R_q^n$. Pri rátaní skalárneho súčinu spočítame najprv pre $1 \leq i \leq n$: $c_i \cdot s_i$, čo je súčin dvoch $\lceil \log q \rceil$-bitových čísel, ktorý vieme transformovať na súčet $\lceil \log q \rceil$ $2\lceil \log q \rceil$-bitových čísel jednoduchým shiftovaním bitov. Teda $\langle \vec{c}, \vec{s} \rangle$ vieme vyjadriť ako súčet $n \cdot \lceil \log q \rceil$ $2\lceil \log q \rceil$-bitových čísel. Pomocou "3 za 2" algoritmu obvodom s hĺbkou $O(\log(n \cdot \log q))$ a veľkosťou $O(n \cdot \log^2 q)$ vieme získať dve $O(\log q + \log n)$-bitové čísla s požadovaným súčtom. Tie vieme sčítať obvodom hĺbky $O(\log\log n + \log\log q)$ a veľkosťou $O(\log n + \log q)$.

Tento súčet potrebujeme redukovať modulo q, čo je operácia rovnakej zložitosti ako delenie, a to vieme rátať obvodom hĺbky $O(\log\log q)$ a veľkosti $polylog(q)$. Záverečné modulo 2 znamená len useknutie bitov.

Teda celkový obvod má hĺbku $O(\log n + \log\log q) = \widetilde{O}(\log \lambda)$ a veľkosť $O(n \cdot \log^l q), l \in \mathbb{N}$, teda $\widetilde{O}(\lambda)$.

V prípade Ψ_{RLWE} môžeme simulovať $\mathbb{Z}_2$ pomocou T_2. Ak $\vec{c} = (c_1, c_2) \in T_q^2$ a $\vec{s} = (s_1, s_2) \in T_q^2$, tak $\langle \vec{c}, \vec{s} \rangle = c_1 s_1 + c_2 s_2$. Súčin dvoch polynómov k-teho stupňa s $\lceil \log q \rceil$-bitovými koeficientami vieme rátať pomocou FFT násobenia polynómov obvodom veľkosti $O(k \cdot \log k \cdot \log q)$ a hĺbky $O(\log k \cdot \log\log k \cdot \log\log q)$, teda platia rovnaké odhady ako pre Ψ.

Keďže na homomofné vyhodnotenie jedného hradla potrebujeme $\widetilde{O}(\lambda^3 \cdot d^5)$ v Ψ, resp. $\widetilde{O}(\lambda \cdot d^3)$ v Ψ_{RLWE} tak celková časová zložitosť homomorfného vyhodnotenia jedného hradla v schéme získanej bootstrapovaním je $\widetilde{O}(\lambda^4)$ pre Υ_Ψ a $\widetilde{O}(\lambda^2)$ pre $\Upsilon_{\Psi_{RLWE}}$.

3.7.4 Bootstrapping batching

Keďže homomorfné vyhodnocovanie dešifrovacej funkcie vykonávame na každom hradle obvodu, zdá sa, že je to ideálny priestor pre uplatnenie batchingu. Problém

je v tom, že v časti 3.7.2 sme neuvažovali nad pokračovaním výpočtu po ukončení batch procedúry – zatiaľ nevieme ako transformovať šifrový text "komprimovaného" otvoreného textu z T_p na šifrové texty jeho zložiek z T_{P_i}. Taktiež nevieme uskutočniť opačnú procedúru – t.j. transformovať šifrové texty jednotlivých zložiek do jedného "komprimovaného" šifrového textu. Ak by sme mali spôsob, ako efektívne realizovať izomorfizmus medzi T_p a $T_{P_1} \times \ldots \times T_{P_l}$ homomorfne, na šifrových textoch, tak môžme značne urýchliť bootstrapovanie viacerých šifrových textov súčasne.

Brakerski, Gentry a Vaikuntanathan [BGV11, časť 5.3] popisujú ako realizovať dané procedúry, čím dosahujú časovú zložitosť (pre dostatočne veľké obvody) homomorfného vyhodnocovania $\widetilde{O}(\lambda)$. Keďže konštrukcia je pomerne náročná, neuvádzame ju tu.

Záver

Predstavili sme prvotnú Gentryho schému nad ideálnymi mriežkami, prezentovali sme analýzu jej zložitosti a uviedli sme výsledky existujúcej implementácie. Videli sme, že výkon tejto schémy nie je dostatočný na praktické použitie.

Potom sme prezentovali iný prístup k homomorfnému vyhodnocovaniu použitý v chimérickej schéme založený na kombinácii čiastočne homomorfnej schémy a multiplikatívne homomorfnej schémy. Videli sme, že aj keď myšlienka konštrukcie je zaujímavá, nepriniesla asymptotické zlepšenie zložitosti.

V tretej kapitole sme prezentovali schému využívajúcu metódu škálovania rozsahu na redukciu šumu v šifrovom texte, ktorá v kombinácii s bootstrapingom umožnila zložitosť homomorfného vyhodnocovania kvázi lineárnu od bezpečnostného parametra.

Pre obmedzenie rozsahom sme nespomenuli ďalšie plne homomorfné schémy, napríklad FHE nad celými číslami [vDGHV10] ktorá je zaujímavá svojou jednoduchosťou.

Taktiež sme sa nevenovali najnovším publikáciám v tejto oblasti: V máji 2012 publikovali Gentry, Halevi a Smart [GHS12] schému, kde pomocou efektívneho batchovania dosiahli len polylogaritmický nárast časovej zložitosti pri homomorfnom vyhodnocovaní.

Literatúra

[BGV11] Zvika Brakerski, Craigh Gentry, and Vinod Vaikuntanathan. Fully homomorphic encryption without bootstrapping. *Cryptology ePrint Archive*, 2011.
`http://eprint.iacr.org/2011/277.pdf`.

[BL96] Dan Boneh and Richard Lipton. Searching for elements in black box fields and applications. In *In Advances in Cryptology-Crypto'96, LNCS1109*, pages 283–297. Springer-Verlag, 1996.
`http://eprint.iacr.org/2011/471.pdf`.

[Chu11] Gu Chunsheng. Cryptanalysis of the smart-vercauteren and gentry-halevi's fully homomorphic encryption. *Cryptology ePrint Archive*, 2011.
`http://eprint.iacr.org/2011/328.pdf`.

[Gen09a] Craig Gentry. *A Fully Homomorphic Encryption Scheme*. PhD thesis, Standford University, 2009.
`http://crypto.stanford.edu/craig`.

[Gen09b] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, STOC '09, pages 169–178. ACM, 2009.
`http://eprint.iacr.org/2010/520.pdf`.

[GH11a] Craig Gentry and Shai Halevi. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. *Imagine*, 5, 2011.
`http://eprint.iacr.org/2011/279.pdf`.

[GH11b] Craig Gentry and Shai Halevi. Implementing gentry's fully-homomorphic encryption scheme. In *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer*

Science, pages 129–148. Springer, 2011.
`http://eprint.iacr.org/2010/520.pdf`.

[GHS12] Craig Gentry, Shai Halevi, and NigelP. Smart. Fully homomorphic encryption with polylog overhead. In *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 465–482. 2012.
`http://eprint.iacr.org/2011/566.pdf`.

[LMSV12] Jake Loftus, Alexander May, Nigel Smart, and Frederik Vercauteren. On cca-secure somewhat homomorphic encryption. In *Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 55–72. Springer, 2012.
`http://eprint.iacr.org/2011/328.pdf`.

[Mic99] Daniele Micciancio. Lattices in cryptography and cryptanalysis, lecture notes, 1999.
`http://cseweb.ucsd.edu/~daniele/CSE207C/`.

[Mic10] Daniele Micciancio. Lattices algorithms and applications, lecture notes, 2010.
`http://cseweb.ucsd.edu/classes/wi10/cse206a/`.

[OYKU10] Naoki Ogura, Go Yamamoto, Tetsutaro Kobayashi, and Shigenori Uchiyama. An improvement of key generation algorithm for gentry's homomorphic encryption scheme. In *Advances in Information and Computer Security*, volume 6434 of *Lecture Notes in Computer Science*, pages 70–83. Springer, 2010.

[Sch11] Patrick Schmidt. Fully homomorphic encryption: Overview and cryptanalysis. diploma thesis, Technische Universität Darmstadt, 2011.

[SS10] Damien Stehlé and Ron Steinfeld. Faster fully homomorphic encryption. In *Advances in Cryptology - ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 377–394. Springer, 2010.
`http://eprint.iacr.org/2010/520.pdf`.

[SV10] N. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*,

pages 420–443. Springer, 2010.
`http://eprint.iacr.org/2009/571.pdf`.

[vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer, 2010.
`http://eprint.iacr.org/2009/616.pdf`.

[VDJ10] Marten Van Dijk and Ari Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. In *Proceedings of the 5th USENIX conference on Hot topics in security*, HotSec'10, pages 1–8. USENIX Association, 2010.

Príloha

1.1 Mriežky

Definícia 15. *Nech* $B = \{\vec{b_1}, \ldots, \vec{b_n}\}$ *sú lineárne nezávislé vektory vektorového priestoru* $\mathbb{R}^m$*. Potom množinu*

$$\mathcal{L}(B) = \{a_1\vec{b_1} + \ldots + a_n\vec{b_n} \mid a_i \in \mathbb{Z}\}$$

nazývame mriežka generovaná bázou B*.*

Bázu mriežky B môžme reprezentovať maticou $n \times m$, kde riadky sú jednotlivé bázové vektory.

$$B = \begin{pmatrix} \vec{b_1} \\ \vec{b_2} \\ \ldots \\ \vec{b_n} \end{pmatrix}$$

Pod veľkosťou bázy budeme rozumieť dĺžku najdlhšieho bázového vektora a označovať $|B| = \min\{|\vec{b}| \mid \vec{b} \in B\}$.

Nie je ťažké vidieť, že daná mriežka môže mať viacero (dokonca nekonečne veľa) báz. Napr. v $\mathbb{R}^2$

$$\mathcal{L}(\{(0,2),(2,0)\}) = \mathcal{L}(\{(2,4),(2,0)\})$$

Ak počet bázových vektorov je rovnaký ako dimenzia vektorového priestoru, teda $m = n$, hovoríme že generovaná mriežka je plnej dimenzie. V ďalšom sa budeme zaoberať len takými mriežkami.

Definujeme determinant mriežky ako absolútnu hodnotu determinantu bázy. Na to potrebujeme ukázať, že táto hodnota nezávisí od voľby bázy

Veta 12. *Nech* $B_1, B_2 \in \mathbb{R}^{n\times n}$ *sú bázy mriežky* $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ *plnej dimenzie. Potom* $det(B_1) = \pm det(B_2)$

Dôkaz. Keďže $\mathcal{L}(B_1) = \mathcal{L}(B_2)$, tak existujú $U, V \in \mathbb{Z}^{n\times n}$ také, že $B_1 = U \cdot B_2$ a $B_2 = V \cdot B_1$. Teda $det(B_1) = det(U) \cdot det(B_2)$, $det(B_2) = det(V) \cdot det(B_1)$, čo znamená že $det(U) \cdot det(V) = 1$. Keďže sú obe celočíselné, tak $det(U) = det(V) = \pm 1$. □

Definícia 16. *Nech $B \in \mathbb{R}^{n\times n}$ je regulárna štvorcová matica. Potom determinant $det(\mathcal{L}(B))$ definujeme ako $|det(B)|$.*

Definujeme akýsi normálny tvar bázy mriežky, ktorý nám bude užitočný.

Definícia 17. *Nech $B = \{b_{i,j}\} \in \mathbb{R}^{n\times n}$ a platí:*

- *B je horná trojuholníková matica: $j < i \Rightarrow b_{i,j} = 0$*
- *Pre všetky $i < j : 0 \leq b_{i,j} < b_{j,j}$, teda všetky prvky sú kladné a prvky na diagonále sú najväčšie v stĺpci.*

Potom hovoríme, že B je v Hermiteho normálnom tvare (HNF).

Veta 13. *Ak $B \in \mathbb{Q}^{n\times n}$ potom existuje $B' \in \mathbb{Q}^{n\times n}$ v HNF taká, že $\mathcal{L}(B) = \mathcal{L}(B')$. Navyše existuje polynomiálny algoritmus ktorý transformuje B na B'.*

Dôkaz. Načrtneme základnú myšlienku transformácie.

Ak riadky matice tvoria bázové vektory, potom výmena riadkov a pripočítanie celočíselného násobku riadku j k riadku i nemení generovanú mriežku.

Ak sú koeficienty matice B v $\mathbb{Z}$, vieme maticu upraviť nasledovným spôsobom: Najprv vynulujeme celý prvý stĺpec až na prvý koeficient, potom rekurzívne pokračujeme na podmatici bez prvého riadku a stĺpca. Vyulovať prvý koeficient v riadku i vieme nasledovne; kým $b_{i,1}$ je rôzne od nuly, tak ak $b_{i,1} < b_{1,1}$, potom vymeň riadky 1 a i, inak odčítaj riadok 1 od riadku i.

Dosiahnuť aby prvky na diagonále boli najväčšie v stĺpci vieme jednoducho odčítaním riadkov.

Ak sú koeficienty matice v $\mathbb{Q}$, najprv upravíme všetky na spoločného menovateľa a potom pracujeme s čitateľmi rovnako ako v celočíelnom prípade. □

Veta 14. *Ak $B, C \in \mathbb{Q}^{n\times n}$ sú v HNF a $\mathcal{L}(B) = \mathcal{L}(C)$ potom $B = C$.*

Dôkaz. Uvedieme myšlienku dôkazu.

Keďže $\mathcal{L}(B) = \mathcal{L}(C)$, tak každý riadok B sa dá napísať ako súčet celočíselných násobkov riadkov C a opačne. Ak $\vec{b_i} = a_1\vec{c_1} + \ldots + a_n\vec{c_n}$, zrejme $\forall j < i : a_j = 0$, inak by B nebola horná trojuholníková. Ak nás zaujíma len koeficient $b_{i,i}$ potom $\vec{c_j}$

pre $j > i$ k nemu neprispievajú, a teda $b_{i,i} = a_i \cdot c_{i,i}$. Keďže rovnako aj $c_{i,i} = a'_i \cdot bi, i$ pre $a' \in \mathbb{Z}$ nutne $b_{i,i} = c_{i,i}$.

Ak $\vec{b_i} = a_1\vec{c_1} + \ldots + a_n\vec{c_n}$ tak vieme že $a_i = 1$, $\forall j < i : a_j = 0$. Nech $j > i$, ostáva nám ukázať, že $a_j = 0$:

Indukciou. Ak pre všetky $i < k < j$ platí $a_k = 0$, potom ak by $a_j \leq -1$, tak $b_{i,j} = c_{i,j} + a_j \cdot c_{j,j} < 0$, čo je spor s kladnosťou prvkov matice B. Ak naopak $a_j \geq 1$, potom $b_{i,j} = c_{i,j} + a_j \cdot c_{j,j} \geq c_{j,j} = b_{j,j}$, čo je spor s maximálnosťou prvku na diagonále v stĺpci.

□

Predchádzajúce dve vety hovoria o tom, že každá mriežka nad racionálnymi číslami má jedinečnú bázu, ktorú dokážeme v polynomiálnom čase získať z ľubovoľnej bázy.

Definícia 18. *Nech B je báza mriežky plnej dimenzie. Potom asociovaný polootvorený rovnobežnosten s B definujeme:*

$$P(B) = \{a_1\vec{b_1} + \ldots + a_n\vec{b_n} \mid a_i \in \langle -1/2, 1/2)\}$$

Definícia 19. *Nech $L \subset \mathbb{R}^n$ je mriežka plnej dimenzie, potom pre $1 \leq i \leq n$ definujeme $\lambda_i(L)$ ako najmenšie r také, že existuje i rôznych lineárne nezávislých vektorov v mriežke L veľkosti najviac r.*

Zrejme $\lambda_1(L) = \min\{|\vec{v}| \mid \vec{v} \in L\}$.

Definícia 20. *Ak $L \subseteq R^n$ je mriežka, potom pre $\vec{t} \in \mathbb{R}^n$ definujeme $dist(L, \vec{t})$ ako* $\min\{|\vec{v} - \vec{t}| \mid \vec{v} \in L\}$.

1.1.1 Problémy nad mriežkami

Definícia 21. *Ak je daná báza B mriežky L dimenzie n, tak problém $\gamma(n)$-najkratšieho vektora ($\gamma(n)$-Shortest Vector Problem, $\gamma(n)$-SVP) spočíva v nájdení nenulového vektora $\vec{v} \in L$, ktorého pre veľkosť je $|\vec{v}| \leq \gamma(n) \cdot \lambda_1(L)$*

Definícia 22. *Ak je daná báza B mriežky L dimenzie n, tak problém $\gamma(n)$-najkratších nezávislých vektorov ($\gamma(n)$-Shortest Indepentent Vector Problem, $\gamma(n)$-SIVP) spočíva v nájdení lineárne nezávislých vektorov $\vec{v}_1, \ldots, \vec{v}_n \in L$, pre veľkosť ktorých platí $\forall i : |\vec{v}_i| \leq \gamma(n) \cdot \lambda_n(L)$*

Definícia 23. *Ak je daná báza B mriežky L dimenzie n a vektor $\vec{t} \in \mathbb{R}^n$, tak problém $\gamma(n)$-najbližšieho vektora ($\gamma(n)$-Closest Vector Problem, $\gamma(n)$-CVP) spočíva v nájdení vektora $\vec{v} \in L$, ktorého vzdialenosť od $\vec{t}$ je $|\vec{v} - \vec{t}| \leq \gamma(n) \cdot dist(L, \vec{t})$*

Definícia 24. *Problém $\gamma(n)$-najkratšieho vektora v obmedzenej vzdialenosti ($\gamma(n)$-Bounded Distance Decoding Problem, $\gamma(n)$-BDDP) je rovnaký ako $\gamma(n)$-CVP s dodatočnou informáciou: $dist(L, \vec{t}) \cdot (\gamma(n) + 1) < \lambda_1(L)$.*

Dodatočná informácia v $\gamma(n)$-BDDP nám hovorí, že $\vec{t}$ je tak blízko mriežky, že existuje len jedno riešenie $\vec{v} \in L$, pre ktoré $|\vec{v} - \vec{t}| = dist(L, \vec{t}) < \lambda_1(L)/(\gamma(n) + 1)$. Pre všetky $\vec{u} \in L, \vec{u} \neq \vec{v}$ totiž z trojuholníkovej nerovnosti $|\vec{u} - \vec{t}| \geq |\vec{u} - \vec{v}| - |\vec{v} - \vec{t}| > \lambda_1(L) - \lambda_1(L)/(\gamma(n) + 1) = \gamma(n) \cdot \lambda_1(L)/(\gamma(n) + 1) > \gamma(n) \cdot dist(L, \vec{t})$.

Známe algotimy riešiace tieto problémy pre malé $\gamma(n)$ sú varianty LLL algoritmu, prípadne algoritmu hľadania najbližšej roviny (Babai's nearest plane algorithm). Pre $\gamma(n) = 2^{f(n)}$, $f : \mathbb{N} \to \mathbb{N}$, je dobrým odhadom časovej zložitosti týchto algoritmov $O(2^{n/f(n)})$ [Gen09b].

1.1.2 Ideálne mriežky

Definícia 25. *Nech R je okruh, $h : R \to \mathbb{Z}^n$ je izomorfizmus vzhľadom na sčítavanie. Potom mriežku $L \subseteq Z^n$ nazveme ideálna, ak $L = h(I)$ pre nejaký ideál $I \subseteq R$.*

Nech $R = \mathbb{Z}[x]/(f)$ pre nejaký ireducibilný monický polynóm $f \in \mathbb{Z}[x]$ stupňa n. Ďalej nech $S = \{g \bmod f \mid g \in \mathbb{Z}[x]\}$ je množina štadardných reprezentantov tried rozkladu, izomorfizmus $h_1 : R \to S$ zobrazuje triedu rozkladu na jej reprezentanta a izomorfizmus $h_2 : S \to \mathbb{Z}^n$ zobrazujúci polynóm na vektor koeficientov, teda

$$h_1(A) = g \bmod f, A \in R, g \in A$$

$$h_2(g_{n-1}x^{n-1} + \ldots + g_1 x + g_0) = (g_{n-1}, \ldots, g_0)$$

Potom izomorfizmus $h : R \to \mathbb{Z}^n$ definujeme $h(A) = h_2(h_1(A))$. V ďalšom texte budeme používať takto definované R a h.

Pre zjednodušenie notácie budeme interpretovať prvky R jednak ako polynómy (určené h_1) dvak ako vektory v $\mathbb{Z}^n$ (určené h), teda napríklad zápis $\vec{v} \cdot x^k$ interpretujeme ako $h^{-1}(\vec{v}) \cdot h_1^{-1}(x^k)$, pre $\vec{v} \in \mathbb{Z}^n$.

Definícia 26. *Nech $\vec{v} \in R$. Potom $B_{\vec{v}} = \{\vec{v_i} = \vec{v} \cdot x^i \mid 0 \leq i < n\}$ nazývame rotačná báza mriežky $\mathcal{L}(B_{\vec{v}})$ prislúchajúca k $\vec{v}$.*

Veta 15. *Nech $\vec{v} \in R$, $I = (\vec{v})$ je hlavný ideál. Potom rotačná báza prislúchajúca k $\vec{v}$ je bázou mriežky $h(I)$.*

Dôkaz. $\mathcal{L}(B_{\vec{v}}) \subseteq h(I)$: Ak $\vec{u} \in \mathcal{L}(B_{\vec{v}})$, potom

$$\begin{aligned}\vec{u} &= a_0\vec{v_1} + \ldots + a_{n-1}\vec{v_{n-1}} \\ &= a_0\vec{v}x^0 + \ldots + a_{n-1}\vec{v}x^{n-1} \\ &= \vec{v} \cdot (a_0x^0 + \ldots + a_{n-1}x^{n-1}) \in h(I)\end{aligned}$$

$h(I) \subseteq \mathcal{L}(B_{\vec{v}})$: Ak $\vec{u} \in h(I)$, potom

$$\begin{aligned}\vec{u} &= \vec{v} \cdot \vec{a} \\ &= \vec{v} \cdot (a_0x^0 + \ldots + a_{n-1}x^{n-1}) \\ &= a_0\vec{v}x^0 + \ldots + a_{n-1}\vec{v}x^{n-1} \\ &= a_0\vec{v_1} + \ldots + a_{n-1}\vec{v_{n-1}} \in \mathcal{L}(B_{\vec{v}})\end{aligned}$$

□

Zaujímavým parametrom R je nárast veľkosti vektora pri sčítaní a násobení. Ľahko vidno, že $|\vec{u} + \vec{v}| \leq |\vec{u}| + |\vec{v}|$. Zrejme $|\vec{u} \cdot \vec{v}| \leq |\vec{u}| \cdot |\vec{v}| \cdot \gamma_{Mult}(R)$ pre nejaké $\gamma_{Mult}(R)$, bude nám stačiť ak $\gamma_{Mult}(R)$ je polynoiálna od stupňa $f(x)$ n. Napríklad pre $f(x) = x^n \pm 1$ je $\gamma_{Mult}(R) = \sqrt{n}$.

Veta 16. *Ak $R = \mathbb{Z}[x]/(f(x))$ pre $f(x) = x^n \pm 1$, potom pre každé $\vec{u}, \vec{v} \in R$ platí:* $|\vec{v} \cdot \vec{u}| \leq \sqrt{n} \cdot |\vec{v}| \cdot |\vec{u}|$

Dôkaz. Dokážeme tvrdenie pre $f(x) = x^n - 1$.

Ľahko sa dá overiť, že pre ľubovoľný $\vec{y} = (y_{n-1}, \ldots, y_0) \in \mathbb{R}$ platí
$\vec{y} \cdot x = (y_{n-2}, \ldots, y_0, y_{n-1})$, teda pre koeficienty súčinu vektorov $\vec{w} = \vec{v} \cdot \vec{u}$ platí

$$w_k = \sum_{i+j=k \bmod n} v_i \cdot u_j$$

Zrejme $|\vec{v}| \cdot |\vec{u}| = \sqrt{v_{n-1}^2 + \ldots + v_0^2} \cdot \sqrt{u_{n-1}^2 + \ldots + u_0^2} \geq w_k$ pre každý koeficient w_k. Potom $|\vec{w}| = \sqrt{w_{n-1}^2 + \ldots + w_0^2} \leq \sqrt{n \cdot |\vec{v}|^2 \cdot |\vec{u}|^2} \leq \sqrt{n} \cdot |\vec{v}| \cdot |\vec{u}|$. □

Ak $I \in R$ je ideál a B_I je báza mriežky $h(I)$ plnej dimenzie, chceme definovať množinu štandardných reprezentantov tried rozkladu R/I.Pomôže nám geometrická predstava: Priestor $\mathbb{Z}^n$ rozdelíme na otvorené rovnobežnosteny $\vec{v}+P(B_I), \vec{v} \in \mathcal{L}(B_I)$. Za množinu reprezentantov by sme mohli zvoliť napríklad ľubovoľný z týchto rovnobežnostenov, vyberieme si práve $P(B_I)$.

Potom reprezentantom triedy $\vec{v} + I$ je vektor $\vec{v'}$ pre ktorý platí $\vec{v'} \in P(B_I)$ a $\exists \vec{u} \in \mathcal{L}(B) : \vec{v'} + \vec{u} = \vec{v}$. Navyše ho vieme efektívne vypočítať ako [4]

$$\vec{v'} = \vec{v} - \lceil \vec{v} \cdot B_I^{-1} \rfloor \cdot B_I$$

Definícia 27. *Nech B je báza ideálnej mriežky $\mathcal{L}(B) \subseteq R$ plnej dimenzie. Potom definujeme projekciu $p_B : R \to P(B)$ ako*

$$p_B(\vec{v}) = \vec{v} - \lceil \vec{v} \cdot B^{-1} \rfloor \cdot B$$

Budeme používať označenie $\vec{v} \bmod B = p_B(\vec{v})$, a $R \bmod B = P(B)$

Definícia 28. *Pre $r \in \mathbb{R}$ definujeme guľu v R s polomerom r ako*

$$\mathcal{B}(r) = \{\vec{v} \in R \mid |\vec{v}| \leq r\}$$

Ďalej definujeme pojmy inverznej a duálnej mriežky, ktoré budeme využívať pri dešifrovaní. Vzhľadom na to, že v okruhu R nemáme inverzné prvky, budeme využívať okruh $\mathbb{Q}[x]/f(x)$ v ktorom nenulové prvky majú inverzy, ak $f(x)$ je ireducibilný. Navyše inverzné prvky vieme efektívne rátať pomocou rozšíreného euklidovho algoritmu pre najväčšieho spoločného deliteľa polynómov.

Definícia 29. *Nech $L \subseteq R$ je ideálna mriežka. Potom duálnu mriežku k L označujeme L^* a definujeme ako*

$$L^* = \{\vec{x} \in \mathbb{R}^n \mid \forall \vec{v} \in L : \langle \vec{x}, \vec{v} \rangle \in \mathbb{Z}\}$$

Definícia 30. *Nech $L \subseteq R$ je ideálna mriežka. Potom inverznú mriežku k L označujeme L^{-1} a definujeme ako*

$$L^{-1} = \{\vec{x} \in \mathbb{Q}[x]/(f(x)) \mid \forall \vec{v} \in L : \vec{v} \cdot \vec{x} \in R\}$$

Lema 16. *Nech B je báza ideálnej mriežky plnej dimenzie L. Potom $B^* = (B^{-1})^T$ je báza L^*.*

Dôkaz. Označíme riadky B^* ako $\vec{b_1} \ldots \vec{b_n}$.

Najprv ukážeme, že bázové vektory patria do L^*: Keďže $B \cdot (B^*)^T = I$ tak $\forall i : B \cdot \vec{b_i}^T \in \mathbb{Z}^n$. Ľubovoľný vektor $\vec{v} \in L$ je súčtom celočíselných násobkov riadkov B, a teda $\forall i : \vec{b_i} \in L^*$, teda $\mathcal{L}(B^*) \subseteq L^*$.

Ak $\vec{c} \in L^*$, potom $B \cdot \vec{v}^T = (c_1, \ldots, c_n)^T \in \mathbb{Z}^n$. Keďže násobenie vektora regulárnou maticou je izomorfizmus, tak $\vec{c} = c_1\vec{b_1} + \ldots + c_n\vec{b_n}$, a teda riadky $\mathcal{L}(B^*) \supseteq L^*$. □

[4] výsledkom operácie $\lceil \vec{v} \rfloor$ je vektor s koeficientami zaokrúhlenými na najbližšie celé číslo.

Lema 17. *Nech B je rotačná báza ideálnej mriežky L plnej dimenzie prislúcahjúca k vektoru $\vec{v}$. Potom B^{-1} je rotačná báza inverznej mriežky L^{-1} prislúchajúca k vektoru $(\vec{v})^{-1}$.*

Dôkaz. Označme $\vec{w} = (\vec{v})^{-1}$ a B_w k nemu prislúchajúcu rotačnú bázu. Z definínície rotačnej bázy vyplýva $\vec{w} \cdot B = \vec{v} \cdot B_w = \vec{w} \cdot \vec{v} = \vec{1}$ a teda $B_w \cdot B = B \cdot B_w = I$, teda $B_w = B^{-1}$.

Ľubovoľný vektor $\vec{a} \in L$ je generovaný B, teda $\vec{a} = (a_1, \ldots, a_n) \cdot B, \forall i : a_i \in \mathbb{Z}$. Potom pre $0 \leq j \leq n-1$ platí: $\vec{w}x^j \cdot \vec{a} = (a_1, \ldots, a_n) \cdot \vec{w}x^j \cdot B = (a_1, \ldots, a_n) \cdot x^j \in R$, takže $\mathcal{L}(B_w) \subseteq L^{-1}$.

Pre ľubovľný vektor $\vec{c} \in L^{-1}$ platí $\vec{c} \cdot \vec{v} = (c_1, \ldots, c_n) \in R$. Keďže násobenie regulárnou maticou je izomorfizmus, tak $\vec{c} = c_1\vec{w}x^0 + \ldots + c_n\vec{w}x^{n-1}$, z čoho vyplýva $\mathcal{L}(B_w) \supseteq L^{-1}$. □