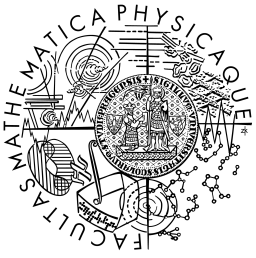

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Tomáš Rabas

Kryptografické využití multilineárních forem

Katedra algebry

Vedoucí bakalářské práce:	doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2018

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Kryptografické využití multilineárních forem

Autor: Tomáš Rabas

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: Tato práce popisuje teoretický koncept multilineárního zobrazení a jeho praktickou realizaci pomocí konstrukce Garg-Gentry-Halevi (GGH) Stupňovité kódovací schéma. V této konstrukci, která je založena na ideálových mřížích, matematicky zdůvodníme předpoklady konstrukce a vyjasníme některé algebraické nejasnosti, především invertibilitu náhodně zvoleného prvku z v okruhu R_q. Využití teoretického konceptu i její praktické realizace pak ukážeme v protokolu jednokolové Diffie-Hellman výměny klíčů mezi N účastníky.

Klíčová slova: Diffie-Hellman, ideálová mříž, GGH, multilineární zobrazení

Title: Application of Multilinear Forms in Cryptography

Author: Tomáš Rabas

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: We describe the theoretical concept of multilinear maps and its practical realization using new construction - Garg-Gentry-Halevi (GGH) Graded Encoding Scheme. In this construction, which is based on ideal lattices, we justify its assumptions and clarify some algebraic inaccuracies, especially the inversibility of the randomly chosen z from commutative ring R_q. We also present application of theoretical concept and its practical realization GGH to one-round N-way Diffie-Hellman key exchange.

Keywords: Diffie-Hellman, ideal lattice, GGH, multilinear map

Obsah

1. Multilineární zobrazení jako teoretický konstrukt

Dnes je již známo, že multilineární formy (zobrazení) mohou být v kryptografii velmi užitečný nástroj. Dan Boneh a Alice Silverberg v článku [3] popisují hned několik aplikací, které jsou velmi zajímavé. Mezi ně patří i „jednokolová výměna klíčů mezi N účastníky“, kterou se zde budeme zabývat.

Bohužel i přesto, že je popsáno mnoho článků o teoretickém využití multilineárních zobrazení, jejich praktická realizace se zdá být velmi obtížná. V poslední době se ukázalo, že k jejich konstrukci se dají využít ideálové mříže.

Ty se v poslední době stali v kryptografii velmi oblíbené, zdá se totiž, že poskytují protokoly odolné i proti kvantovým počítačům, které jsou jinak schopny efektivně řešit problém diskrétního logaritmu a problém faktorizace, na kterých je založena většina dnešních kryptografických protokolů.

V následujícím textu popíšeme jednu z konstrukcí multilineárních zobrazení založenou právě na ideálových mřížích z článku [6] a ukážeme, jak se využije v „jednokolové výměně klíčů mezi N účastníky“.

1.1 Značení, definice a seznámení s algoritmickou složitostí

Ještě předtím než vyslovíme definici multilineárního zobrazení, zavedeme zde standardní značení a definice, které budeme potřebovat.

Množinu všech konečných binárních řetězců budeme značit $\{0,1\}^*$ a množinu všech binárních řetězců délky m označíme $\{0,1\}^m$.

Deterministický algoritmus nazýváme algoritmus, který vždy ze stejných výchozích (vstupních) podmínek svým během vytvoří stejné výsledky a jehož aktuální i následující krok vykonávání algoritmu je jednoznačně definován.

Nedeterministický algoritmus je takový algoritmus, který v některých krocích může volit z několika možností dalších kroků a při stejném vstupu může dávat rozdílné výsledky.

Pravděpodobnostní algoritmus je takový algoritmus, jehož chování je podmíněno vstupními náhodnými bity a jehož výsledek i čas běhu je tedy náhodná veličina.

Pravděpodobnostní algoritmus tedy narozdíl od deterministického ve svém běhu obsahuje náhodu. To můžeme vnímat tak, že si algoritmus v každém kroku může hodit mincí, jak bude pokračovat dál(orel - 0 bit, panna - 1 bit). Jiný pohled je, že se na začátku náhodně vybere deterministický algoritmus, který se pak provede.

Pravděpodobnost jevu $\mathcal{D}$ označíme $\Pr[\mathcal{D}]$. Pro konečnou množinu S, budeme pomocí $x \leftarrow S$ definovat náhodnou veličinu x, která vybírá prvky z S rovnoměrně náhodně. (t.j. pro všechna $c \in S$ platí $\Pr[x = c] = 1/|S|$).

Pro pravděpodobnostní algoritmus $\mathcal{A}$ budeme pomocí $x \leftarrow \mathcal{A}(y)$ definovat náhodnou veličinu x, která je výstupem $\mathcal{A}$ pro vstup y. (t.j. pro všechna $c \in \{0,1\}^*$ máme $\Pr[x = c] = \Pr[\mathcal{A}(y) = c]$)

Říkáme, že funkce $f : \mathbb{Z}^+ \to \mathbb{R}^+$ je zanedbatelná, pokud pro všechna $d > 0$ a dostatečně velké t platí: $0 < f(t) < 1/t^d$.

Příklad: funkce 2^{-t} nebo $t^{-\log t}$ jsou zanedbatelné, zatímco funkce $t^{-1000000}$ není zanedbatelná.

Říkáme, že funkce $f(t)$ je *téměř jistá*, pokud $1 - f(t)$ je zanedbatelná.

Říkáme, že jev nastane *téměř jistě*, pokud jev nastane s pravděpodobností alespoň $1 - f(t)$, kde funkce $f(t)$ je zanedbatelná (odpovídající termín v angličtině je *with overwhelming probability*).

Říkáme, že jev E (závislý na parametru n) nastane *s vysokou pravděpodobností* (*with high probability - whp*), pokud pravděpodobnost, že jev E nastane, $p_n \geq 1 - C/n^\alpha$ pro nějaké C,$\alpha > 0$. Tedy platí, že $\lim_{n\to\infty} p_n \to 1$.

Problémy, které lze řešit algoritmicky, lze rozlišit na dva případy. *Rozhodovací problémy* jsou ty, kde očekáváme odpověd ANO/NE. Příklady: Zjisti, zda dané přirozené číslo je prvočíslo. Zjisti, zda daná diofantická rovnice má řešení. Zjisti, zda v daném grafu existuje hamiltonovská cesta.

Vyhledávacím problémem rozumíme problém, kdy je správných odpovědí více. Příklady: Pro dané prvočíslo najdi nějaký jeho faktor. Najdi nejkratší cestu mezi dvěma body orientovaného grafu. Vyhledávací problémy ale lze převést na sérii rozhodovacích problémů: „Je i-tý bit odpovědi 0 nebo 1?“.

Mezi známé matematické problémy v kryptografii patří...
Nechť $G = \langle g \rangle$ je grupa prvočíselného řádu r s generátorem g, x,y,$z \in 0, \ldots, r-1$
Discrete Log Problem (DLP): Dáno g, g^x, spočti x.
Computational Diffie-Hellman Problem (CDHP): Dáno g, g^x, g^y, spočti g^{xy}.
Decisional Diffie-Hellman Problem (DDHP): Dáno g,g^x,g^y,g^z, zjisti zda $xy = z$.

Algoritmus nazvěme *efektivní*, pokud má polynomiální složitost vzhledem k velikosti vstupu. Zobrazení f je efektivní, pokud algoritmus na vypočtení $f(x)$ $\forall x \in \mathrm{D}(f)$ je efektivní.

Definice 1. *Říkáme, že problém je těžký, pokud neexistuje efektivní algoritmus, který by vrátil správné řešení s větší než zanedbatelnou pravděpodobností.*

Problém, který není těžký, nazveme *lehký*.

Nechť existuje orákulum $\mathcal{O}$, které vrací správné řešení problému A. Říkáme, že problém B je *redukovatelný* na problém A, pokud existuje algoritmus P, mající k dispozici orákulum $\mathcal{O}$, řešící B v polynomiálním čase. Příklad: CDHP je redukovatelný na DLP.

Pokud je problém B redukovatelný na problém A, říkáme že B je *téměř tak těžký* jako A.

1.2 Multilineární zobrazení

Definice 2. *Říkáme, že zobrazení* $e : G_1^n \to G_2$ *je n-multilineární zobrazení, pokud splňuje následující požadavky:*

(1) G_1 *a* G_2 *jsou grupy stejného (prvočíselného) řádu* p*;*

(2) Pokud $a_1,\ldots,a_n \in \mathbb{Z}$ *a* $x_1,\ldots,x_n \in G_1$*, pak*

$$e(x_1^{a_1},\ldots,x_n^{a_n}) = e(x_1,\ldots,x_n)^{a_1\ldots a_n};$$

(3) Zobrazení e *není degenerované v následujícím smyslu: pokud* $g \in G_1$ *je generátor* G_1*, pak* $e(g,\ldots,g)$ *je generátor* G_2*.*

Pro nás zajímavá jsou samozřejmě pouze ta n-multilineární zobrazení, která splňují, že (1) grupové operace v G_1 a G_2 a zobrazení e se dají efektivně spočíst a (2) není znám žádný efektivní algoritmus na spočtení diskrétního logaritmu v G_1.

Jelikož se budeme zabývat výpočetními problémy nad grupami, fixujme explicitní reprezentaci těchto grup, a to navíc tak, abychom zajistili, že všechny grupové operace a n-multilineární zobrazení budou mít polynomiální složitost.

Definice 3. *Parametry n-multilineárního zobrazení, značíme* Γ*, jsou: popis grup* G_1 *a* G_2 *stejného prvočíselného řádu, n-multilineární zobrazení* $e : G_1^n \to G_2$ *a funkce* $\mathsf{prod}_b, \mathsf{inverse}_b, \mathsf{map}_b$ *a* test_b *pro* $b = 1,2$*, splňující:*

- *Pokud* $b = 1,2$ *a* $x,y \in G_b$*, pak* $\mathsf{prod}_b(\Gamma,x,y) = xy$ *a* $\mathsf{inverse}_b(\Gamma,x) = x^{-1}$.
- *Pokud* $x_1,\ldots,x_n \in G_1$*, pak* $\mathsf{map}(\Gamma,x_1,\ldots,x_n) = e(x_1,\ldots,x_n)$.
- *Pokud* $b = 1,2$ *a* $x \in \{0,1\}^*$*, pak* $\mathsf{test}_b(\Gamma,x) = \mathsf{yes}$ *právě, když* $x \in G_b$.

Příklad: Grupy G_1 a G_2 jsou grupy celých čísel se sčítáním modulo p,
tj. $G_1 = G_2 = (\mathbb{Z}_p, + \pmod p, - \pmod p, 0)$, $n \not\equiv 0 \ (mod\, p)$;
$e : \mathbb{Z}_p^n \to \mathbb{Z}_p$, $(x_1,\ldots,x_n) \mapsto x_1 + \ldots + x_n \pmod p$,
$x,y \in \mathbb{Z}_p$, pak $\mathsf{prod}_b(\Gamma,x,y) = x + y \pmod p$, $\quad \mathsf{inverse}_b(\Gamma,x) = -x$;
$x_1,\ldots,x_n \in \mathbb{Z}_p$, pak $\mathsf{map}(\Gamma,x_1,\ldots,x_n) = x_1 + \ldots + x_n \pmod p$;
Reprezentace v počítači: prvky grupy $\mathbb{Z}_p$ v binárním zápise, algoritmus pro sčítání je lineární (vzhledem k délce čísla p v binárním zápise), operace inverse - odečtení $p - x$ - složitost lineární
Bohužel DLP je v grupě $\mathbb{Z}_p$ triviální (kolikrát nasčítat jedničku, abych získal x?).

Definice 4. *Generátor multilineárních zobrazení, značíme* $\mathcal{G} = \mathcal{G}(t,n)$*, nazvěme pravděpodobnostní algoritmus, který má polynomiální složitost v proměnných* $t \in \mathbb{N}$ *a* $n \in \mathbb{N}$ *a výstupem je uspořádaná trojice* (Γ,g,l)*.* Γ *jsou parametry n-multilineárního zobrazení, kde (1) funkce* $\mathsf{prod}_b, \mathsf{inverse}_b, \mathsf{map}$*, a* test_b *mají polynomiální složitost vzhledem k* t *a* n*, (2)* l *je řád grup* G_1 *a* G_2 *definovaný* Γ*, a (3)* g *je nějaký generátor* G_1*.*

Poznamenjeme, že t je bezpečnostní parametr, který podmiňuje velikost grup G_1 a G_2. Velikost grupy G_1 jakožto funkce v proměnné t, musí být tak velká, aby polynomiální algoritmy na grupové operace byli „dostatečně rychlé“, superpolynomiální algoritmy (které jsou obvykle k dispozici) na spočtení diskrétního logaritmu v G_1 byly „dostatečně pomalé“ a pravděpodobnostní polynomiální algoritmy řešili diskrétní logartimus jen se zanedbatelnou pravděpodobností.

Definice 5. *Generátor multilineárních zobrazení $\mathcal{G}$ nazveme kryptografický generátor multilineárních zobrazení, pokud pro všechny pravděpodobnostní algoritmy $\mathcal{A}$ s polynomiální složitostí v t a pro všechna n platí, že funkce*

$$\mathsf{AdvDlog}_{\mathcal{G},\mathcal{A},n}(t) = \mathsf{Pr}\left[\mathcal{A}(\Gamma,g,g^r) = r : (\Gamma,g,l) \leftarrow \mathcal{G}(t,n), r \leftarrow \mathbb{Z}/l\mathbb{Z}\right]$$

je zanedbatelná.

Konstrukce kryptografického generátoru multilineárních zobrazení je stále otevřený problém pro $n > 2$. Pro $n = 2$ je známo řešení pomocí bilineárního párování, viz [5].

1.3 Předpoklady

MCDH předpokladem myslíme, že je těžké nalézt $e(g,\ldots,g)^{a_1\cdots a_{n+1}} \in G_2$, máme-li k dispozici $g, g^{a_1}, \ldots, g^{a_{n+1}} \in G_1$. Přesněji:

Definice 6 (Multilineární Computational Diffie-Hellman (MCDH) předpoklad)**.** *Říkáme, že generátor multilineárních zobrazení $\mathcal{G}$ splňuje Multilineární Computational Diffie-Hellman (MCDH) předpoklad, pokud pro všechny pravděpodobnostní algoritmy $\mathcal{A}$ s polynomiální složitostí vzhledem k t a pro všechna $n > 1$ platí, že funkce:*

$$\mathsf{AdvDHm}_{\mathcal{G},\mathcal{A},n}(t) = \mathsf{Pr}\left[\mathcal{A}(\Gamma,g,g^{a_1},\ldots,g^{a_{n+1}}) = e(g,\ldots,g)^{a_1\cdots a_{n+1}} : (\Gamma,g,l) \leftarrow \mathcal{G}(t,n), (a_1,\ldots,a_{n+1}) \leftarrow (\mathbb{Z}/l\mathbb{Z})^{n+1}\right]$$

je zanedbatelná.

MDDH předpokladem myslíme následující: máme-li dáno $g, g^{a_1}, \ldots, g^{a_{n+1}} \in G_1$ a máme náhodné $a \leftarrow (\mathbb{Z}/l\mathbb{Z})$, pak odlišit $e(g,\ldots g)^{a_1\cdots a_{n+1}} \in G_2$ od náhodného prvku $e(g,\ldots,g)^a \in G_2$ je těžké. Přesněji:

Definice 7 (Multilineární Decisional Diffie-Hellman (MDDH) předpoklad)**.** *Definujme $\mathsf{IsSame}(a,b) = 1$, pokud $a = b$, a $\mathsf{IsSame}(a,b) = 0$, pokud $a \neq b$. Pak, říkáme, že generátor multilineárních zobrazení $\mathcal{G}$ splňuje Multilineární Decisional Diffie-Hellman (MDDH) předpoklad, pokud pro všechny pravděpodobnostní algoritmy $\mathcal{A}$ s polynomiální složitostí vzhledem k t a pro všechna $n > 1$ platí, že funkce:*

$$\mathsf{AdvDDHm}_{\mathcal{G},\mathcal{A},n}(t) = \mathsf{Pr}\left[\mathcal{A}(\Gamma,g,g^{a_1},\ldots,g^{a_{n+1}}, e(g,\ldots,g)^{a_1\cdots a_{n+1}}, e(g,\ldots g)^a) = \mathsf{IsSame}(\, e(g,\ldots,g)^{a_1\cdots a_{n+1}}, e(g,\ldots,g)^a) : (\Gamma,g,l) \leftarrow \mathcal{G}(t,n), (a_1,\ldots,a_{n+1},a) \leftarrow (\mathbb{Z}/l\mathbb{Z})^{n+2}\right]$$

je zanedbatelná.

1.4 Výměna klíčů mezi N účastníky

Výměnou klíčů mezi N účastníky nazýváme protokol, kdy libovolně N účastníků může zahájit šifrovanou komunikaci přes nezabezpečený kanál. Tento protokol budeme též nazývat *Diffie-Hellman pro N účastníků* (standardní Diffie-Hellman je výměna klíčů mezi dvěmi stranami).

Možné řešení, jak protokol sestavit, je iterovat standardní výměnu klíčů Diffie-Hellman. Ve zkratce, účastníci si posílají N klíčů dokola a každý ho umocní na svůj soukromý klíč. Po posledním umocnění daná strana získá společný tajný šifrovací klíč. To nazveme jako *naivní iterovaný Diffie-Hellman pro N účastníků.* Nebudeme ho přesně definovat, ale uvedeme pouze příklad pro $N = 3$:

Naivní iterovaný Diffie-Hellman pro $N = 3$ účastníků: Alice, Bob a Cyril chtějí komunikovat přes nezabezpečený kanál.

1. Veřejně se dohodnou na parametrech $G = \langle g \rangle$.
2. Každý si vygeneruje svůj soukromí klíč a,b,c.
3. Alice spočte g^a a pošle ho Bobovi.
4. Bob spočte $(g^a)^b$ a pošle ho Cyrilovi.
5. Cyril spočte $(g^{ab})^c$ a uschová si ho jako svůj tajný šifrovací klíč.
6. Bob spočte g^b a pošle ho Cyrilovi.
7. Cyril spočte $(g^b)^c$ a pošle ho Alici.
8. Alice spočte $(g^{bc})^a$ a uschová si ho jako svůj tajný šifrovací klíč.
9. Cyril spočte g^c a pošle ho Alici.
10. Alice spočte $(g^c)^a$ a pošle ho Bobovi.
11. Bob spočte $(g^c a)^b$ a uschová si ho jako svůj tajný šifrovací klíč.

Pozorování. *Všichni účastníci získají stejný šifrovací klíč g^{abc}.*
Útočník zná g^a,g^b,g^c,g^{ab},g^{bc} a g^{ac}, ale společný šifrovací klíč g^{abc} zůstane tajný.
Tento algoritmus obsahuje N^2 mocnění v grupě G.

Naivní iterovaný Diffie-Hellman pro N účastníků lze optimalizovat vhodným pořadím metodou rozděl a panuj následovně:

Optimalizovaný iterovaný Diffie-Hellman pro N účastníků Algoritmus napišme rekurzivně: Pro zjednodušení, nechť $N = 2^k$, g je generátor G, účastníky značíme $A_1, \ldots, A_N$ a jejich soukromé klíče $\alpha_1, \ldots, \alpha_N$. Definujme:

`OptIterDiffie-Hellman`$(M,(A_1, \ldots, A_M),h)$
`{`
`if` $(M = 1)$`:`
A_1 `spočte společný tajný klíč` $S = h^{\alpha_1}$ `a uloží si ho.`

else:
Rozděl M účastníků na dvě poloviny:
$U_1 = (A_1, \ldots, A_{M/2})$ a $U_2 = (A_{M/2+1}, \ldots, A_M)$
A_i v U_1 provedou každý jedno mocnění a pošleme $h_1 = h^{\alpha_1 \cdots \alpha_{M/2}}$ k U_2.
Účastníci A_j v U_2 vykonají to samé a pošlou $h_2 = h^{\alpha_{M/2+1} \cdots \alpha_M}$ k U_1.
OptIterDiffie-Hellman($M/2$,U_1,h_2);
OptIterDiffie-Hellman($M/2$,U_2,h_1);
}
Optimalizovaný iterovaný Diffie-Hellman pro N účastníků (pokud $N = 2^k$) pak definujeme jako OptIterDiffie-Hellman(N,$(A_1, \ldots, A_N)$,g).

Pozorování. *Všichni účastníci získají společný šifrovací klíč $S = g^{\alpha_1 \cdots \alpha_N}$ a v celém protokolu se provede $N \log N$ mocnění.*

Nechť $n := N$. Pomocí n-multilineárních zobrazení lze ale vytvořit protokol, viz níže, který obsahuje jen dvě mocnění (jedno mocnění v grupě G_1 a druhé v G_2) pro každého účastníka, tedy celkově $2n$ mocnění.

Výměnu klíčů mezi n účastníky nazýváme *jednokolovou*, pokud každý z účastníků posílá ostatním svůj klíč pouze jednou.

Protokol 1. ***Jednokolová výměna klíčů mezi*** $(n+1)$***-účastníky s využitím multilineárních forem:***

Setup$(t, n+1)$**:** *Získej (Γ,g,l) z algoritmu $\mathcal{G}(t,n)$. Nechť $e : G_1^n \to G_2$ je n-multilineární zobrazení definované Γ. Pak g je generátor G_1 a l je řád G_1. Výstupem jsou veřejné parametry $\Gamma_{dh} = (\Gamma,g,l)$*

Publish(Γ_{dh}, i)**:** *Náhodně vezmi celé číslo $a_i \in [1,l-1]$. Spočti $h_i = g^{a_i} \in G_1$. Výstupem je dvojice $(pub_i,priv_i)$, kde $pub_i = h_i$ a $priv_i = a_i$. i-tý účastník pošle h_i všem ostatním účastníkům a uschová si své tajemství a_i.*

KeyGen$(\Gamma_{dh}, j, priv_j, \{pub_i\}_{i \neq j})$**:** *Nechť $priv_j = a_j$ a $pub_i = h_i$. j-tý účastník spočte společný klíč S následovně:*

$$S = e(h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_{n+1})^{a_j} \in G_2.$$

Tento klíč S je výstupem.

Pozorování. *Pro všechna $j \in (1, \ldots, n+1)$ platí, že*

$$S = e(h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_{n+1})^{a_j} = e(g^{a_1}, \ldots, g^{a_{j-1}}, g^{a_{j+1}}, \ldots, g^{a_{n+1}})^{a_j} = (e(g, \ldots, g)^{a_1 \cdots a_{j-1} a_{j+1} \cdots a_{n+1}})^{a_j} = e(g, \ldots, g)^{a_1 a_2 \cdots a_{n+1}},$$

tedy všech $n+1$ účastníků získá stejný šifrovací klíč S.

Schéma považujeme za *bezpečné*, pokud pro každý pravděpodobnostní algoritmus $\mathcal{A}$ s polynomiální složitostí je následující funkce:

$$\mathsf{AdvDH}_{\mathcal{A},n}(t) = \mathsf{Pr}[\mathcal{A}(\Gamma_{dh}, \mathrm{pub}_1, \ldots, \mathrm{pub}_n) = S : \Gamma_{dh} \leftarrow \mathsf{Setup}(t,n), (\mathrm{pub}_i, \mathrm{priv}_i) \leftarrow \mathsf{Publish}(\Gamma,i), S \leftarrow \mathsf{KeyGen}(\Gamma,1,\mathrm{priv}_1, \{\mathrm{pub}_i\}_{i \neq 1})]$$

zanedbatelná v proměnné t.

Tvrzení 1. *Nechť $\mathcal{G}$ je generátor multilineárních zobrazení. Pokud $\mathcal{G}$ splňuje MCDH předpoklad, pak je protokol 1 bezpečná jednokolová výměna klíčů mezi $n+1$ účastníky pro všechna n.*

Důkaz. V průběhu protokolu může útočník odposlechnout všechny hodnoty $pub_i = g^i \quad \forall i \in (1,\ldots,n+1)$. Pokud daná grupa splňuje MCDH předpoklad, pak z def. 6 platí, že funkce

$$\mathsf{AdvDHm}_{\mathcal{G},\mathcal{A},n}(t) = \mathsf{Pr}[\mathcal{A}(\Gamma,g,g^{a_1},\ldots,g^{a_{n+1}}) = e(g,\ldots,g)^{a_1\ldots a_{n+1}} : (\Gamma,g,l) \leftarrow \mathcal{G}(t,n), (a_1,\ldots,a_{n+1}) \leftarrow (\mathbb{Z}/l\mathbb{Z})^{n+1}]$$

je zanedbatelná pro všechny pravděpodobnostní algoritmy $\mathcal{A}$ a tedy naše schéma je bezpečné. ($S = e(g,\ldots,g)^{a_1 a_2 \cdots a_{n+1}}$) □

Pro reálné použití S jakožto klíče symetrické šifry, je třeba dokázat, že S lze konvertovat do binárního stringu určité délky nerozlišitelného od náhodného řetězce stejné délky. To ale vyžaduje silnější předpoklad než MCDH předpoklad. V druhé části ukážeme konstrukci, která při splnění MDDH předpokladu skutečně náhodný string vrací téměř jistě).

2. Kandidát multilineárního zobrazení z ideálových mříží - GGH (Garg, Gentry, Halevi)

Článek [6], který popisuje GGH, v popisu konstrukce vybere náhodně tajný prvek $\mathbf{z}$ z jistého okruhu R_q (který definujeme později) a tímto prvkem pak v tomto okruhu dělí. Nijak bohužel už nevysvětluje, zda $\mathbf{z}$ vybíráme z množiny invertibilních prvků okruhu R_q, nebo zda náhodně zvolený (nenulový) prvek v tomto okruhu být invertibilní musí (tj. R_q je těleso).
V rámci této práce jsme se proto zaměřili na prozkoumání předpokladů konstukce, především tedy invertibilitu prvku $\mathbf{z}$, a v této kapitole uvedeme tyto výsledky:

Ukážeme, že okruh R_q v konstrukci GGH není oborem integrity, a tedy je třeba brát prvek $\mathbf{z}$ z množiny invertibilních prvků R_q.

Dále matematicky zdůvodníme, že neinvertibilních prvků je relativně velmi málo a tedy pravděpodobnost, že náhodně zvolené $\mathbf{z}$ bude invertibilní, je velmi blízko jedné.

Bodová mříž

Bodová mříž $L \subset \mathbb{R}^n$, zkráceně mříž nebo mřížka, je aditivní diskrétní podgrupa $\mathbb{R}^n$. Každá (netriviální) mřížka má bázi: báze mřížky plné hodnosti je množina n lineárně nezávislých bodů $\mathbf{b}_1, \ldots, \mathbf{b}_n \in L$ takových, že $L = \{\sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z}\, \forall i\}$. Pokud uspořádáme vektory $\mathbf{b}_i$ do sloupců matice $B \in \mathbb{R}^{n \times n}$, pak můžeme psát $L = \{B\mathbf{z} : \mathbf{z} \in \mathbb{Z}^n\}$. Nechť $L \subset \mathbb{R}^n$ je mřížka, pak duální mřížkou L^* rozumíme všechny body v lineárním obalu L (lineární obal značíme span(L)), které jsou ortogonální k L modulo jedna, přesněji $L^* = \{\mathbf{y} \in \text{span}(L) : \forall\, \mathbf{x} \in L, \langle x,y \rangle \in \mathbb{Z}\}$. Pokud bodová mříž $L \subset \mathbb{Z}^n$, pak L je $\mathbb{Z}$-modul.

Okruhy z konstrukce GGH

Pro n mocninu dvojky (to potřebujeme, aby x^n+1 byl invertibilní - jak dokážeme v další kapitole) uvažujme okruh

$$R = \mathbb{Z}[X]/(x^n + 1),$$

a ztotožněme prvek $u \in R$ s vektorem koeficientů celočíselného polynomu stupně $(n-1)$, který reprezentuje u. Tímto způsobem ztotožníme R s celočíselnou mřížkou $\mathbb{Z}^n$. Dále pro prvočíslo q uvažujme okruh

$$R_q = R/q = \mathbb{Z}_q[X]/(x^n + 1).$$

Sčítání v těchto okruzích probíhá po složkách a násobení jako polynomiální násobení modulo polynom x^n+1. V některých případech budeme uvažovat algebraické číselné těleso $\mathbb{K} = \mathbb{Q}[X]/(x^n + 1)$, jehož prvky obdobně ztotožňujeme s vektory v $\mathbb{Q}^n$. Pak můžeme R chápat jako podokruh $\mathbb{K}$, případně mříž R chápat jako podgrupu $\mathbb{K}$ (s operací sčítání).

2.1 Ireducibilita $x^{2^k}+1$ v $\mathbb{Z}[X]$

V této části ukážeme, že polynom $x^{2^k}+1$, $k \in \mathbb{N}$ je ireducibilní jako polynom v $\mathbb{Z}[X]$ i $\mathbb{Q}[X]$, a tedy okruh $R = \mathbb{Z}[X]/(x^{2^k}+1)$ je oborem integrity a okruh $\mathbb{K} = \mathbb{Q}[X]/(x^{2^k}+1)$ je těleso.
Formulujme znění Eisensteinova kritéria, které budeme potřebovat:

Eisensteinovo kritérium Nechť $f(x)$ je polynom stupně n s koeficienty z oboru celých čísel, tedy $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, a nechť p je prvočíslo takové, že $p \nmid a_n$, $p \mid a_i \; \forall i < n$ a $p^2 \nmid a_0$, pak $f(x)$ je ireducibilní v oboru $\mathbb{Q}[X]$.

Tvrzení 2. *x^n+1 je ireducibilní v $\mathbb{Q}[X]$ právě tehdy, když $n = 2^k$ pro $k \in \mathbb{N}$*

Důkaz. Platí: $f(x)$ je ireducibilní $\Leftrightarrow$ $f(x+1)$ je ireducibilní
($\phi : x \to x+a \; ; \; a \in \mathbb{Z}$ je automorfismus okruhu $\mathbb{Q}[X]$).

" $\Leftarrow$ " obměnou implikace, nechť $d|n$, d liché, tj. $n = d.s$, pak

$$x^n + 1 \;=\; x^{d.s} + 1 \;=\; (x^s+1).(x^{(d-1)s} - x^{(d-2)s} + \ldots - x^{(d-d+1).s} + 1)$$

" $\Rightarrow$ " přímo, nechť $f(x) = x^{2^k}+1$, pak aplikujeme Eisensteinovo kritérium na $f(x+1)$:

$$f(x+1) = (x+1)^{2^k} + 1 = x^{2^k} + 2^k x^{2^k-1} + \binom{2^k}{2} x^{2^k-2} + \ldots + \binom{2^k}{1} x + 1 + 1$$

tj. $a_n = 1$, $a_{n-1} = 2^k$, $a_{n-2} = \binom{2^k}{2}$, $\ldots$, $a_1 = 2^k$, $a_0 = 2$. Pro $p = 2$ pak platí, že $2 \nmid a_n$, $2 \mid a_i \; \forall i < n$ a $2^2 \nmid a_0$. Z Eisensteinova kritéria tedy plyne, že $f(x+1)$ je ireducibilní v $\mathbb{Q}[X]$ a tedy i $f(x)$ je ireducibilní, což jsme chtěli dokázat. □

Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom, pak definujeme obsah polynomu f jako $\mathrm{c}(f) = \mathrm{NSD}(a_0, \ldots, a_n)$ a primitivní část polynomu f jako $\mathrm{pp}(f) = f/\mathrm{c}(f)$. Pokud platí $f = \mathrm{pp}(f)$, pak říkáme, že f je primitivní polynom.

Tvrzení 3. *Buď $\mathbf{R}$ gaussovský obor, $\mathbf{Q}$ jeho podílové těleso a f,g primitivní polynomy z $\mathbf{R}[X]$, pak*

1. *$f \mid g$ v $\mathbf{R}[X]$ právě tehdy, když $f \mid g$ v $\mathbf{Q}[X]$;*
2. *f je ireducibilní v $\mathbf{R}[X]$ právě tehdy, když f je ireducibilní v $\mathbf{Q}[X]$;*
3. *$NSD_{\mathbf{R}[X]}(f,g)$ existuje a je roven primitivnímu polynomu $h \in \mathbf{R}[X]$ splňujícímu $h = NSD_{\mathbf{Q}[X]}(f,g)$.*

Důkaz. Viz [7, Tvrzení 1]. □

Důsledek 4. *$x^{2^k}+1$ pro $k \in \mathbb{N}$ je ireducibilní polynom v $\mathbb{Z}[X]$.*

Důkaz. Nechť $n = 2^k$. Podle tvrzení 2 je $x^n+1 \in \mathbb{Z}[X]$ ireducibilní v $\mathbb{Q}[X]$, zřejmě je primitivní v $\mathbb{Z}[X]$ a $\mathbb{Q}$ je podílové těleso $\mathbb{Z}$. Z tvrzení 3 části 2 tedy plyne, že x^n+1 je ireducibilní polynom v $\mathbb{Z}[X]$ □

Důsledek 5. $\mathbb{Z}[X]/(x^{2^k}+1)$ *pro* $k \in \mathbb{N}$ *je obor integrity.*

Důkaz. Nechť $n = 2^k$. Z důsledku 4 víme, že $x^n+1 \in \mathbb{Z}[X]$ je ireducibilní polynom v okruhu $\mathbb{Z}[X]$ a tedy (x^n+1) je prvoideál v $\mathbb{Z}[X]$.
Platí: R je okruh a I jeho prvoideál právě tehdy, když R/I je obor integrity.
Tedy $\mathbb{Z}[X]/(x^n+1)$ je obor integrity. □

Platí: R je okruh a I jeho maximální ideál právě tehdy, když R/I je těleso.
Tedy $x^n+1 \in \mathbb{Q}[X]$, kde $n = 2^k$, $k \in \mathbb{N}$ je ireducibilní polynom v okruhu $\mathbb{Q}[X]$ a (x^n+1) je maximální ideál v $\mathbb{Q}[X]$, tedy $\mathbb{Q}[X]/(x^n+1)$ je těleso, přičemž platí, že jeho podokruh, který je obor integrity, je $\mathbb{Z}[X]/(x^n+1)$.

2.2 Ideálová mříž

Nechť $n = 2^k$, $k \in \mathbb{N}$. Pro prvek $\mathbf{g} \in R = \mathbb{Z}[X]/(x^n+1)$, nechť $\langle \mathbf{g} \rangle$ je hlavní ideál v R generovaný $\mathbf{g}$ (alternativně, podmřížka $\mathbb{Z}^n$ odpovídající tomuto ideálu), přesněji $\langle \mathbf{g} \rangle = \{\mathbf{g} \cdot \mathbf{u} \,:\, \mathbf{u} \in R\}$. Definujme:

$$R_g := R/\langle \mathbf{g} \rangle = {}^{\mathbb{Z}[X]/(x^n+1)}\!/_{\langle \mathbf{g} \rangle} \simeq \mathbb{Z}[X]/(x^n+1,g),$$

kde $g \in \mathbb{Z}[X]$ je ten, pro který $[g]_{(x^n+1)} = \mathbf{g} \in R$.
Budeme $\langle \mathbf{g} \rangle$ nazývat ideálová mříž, abychom zdůraznili možnou dvojí interpretaci, jako ideál a jako bodová mříž. $B(\mathbf{g})$ bude značit bázi ideálové mříže $\langle \mathbf{g} \rangle$ tvořenou vektory $\{\mathbf{g}, x\mathbf{g}, x^2\mathbf{g}, \ldots, x^{n-1}\mathbf{g}\}$.

Pozorování. $B(\mathbf{g})$ *je báze* $\langle \mathbf{g} \rangle$.

Důkaz. Jsou vektory z $B(\mathbf{g})$ lineárně nezávislé?

$$\text{Nechť} \quad \exists\, a_i \;:\; \sum_{i=0}^{n-1} a_i X^i \mathbf{g} \equiv 0 \;\text{ v }\; \mathbb{Z}[X]/(x^n+1) \quad ,$$

$$\text{pak} \quad x^n+1 \;\Big|\; \sum_{i=0}^{n-1} a_i X^i \mathbf{g} \;=\; \mathbf{g} \cdot \sum_{i=0}^{n-1} a_i X^i \;\text{ v }\; \mathbb{Z}[X] \quad .$$

Protože dle důsledku 4 (a předpokladu $n = 2^k$) je polynom x^n+1 ireducibilní v $\mathbb{Z}[X]$, tak vidíme, že x^n+1 dělí $\mathbf{g}$ nebo $\sum_{i=0}^{n-1} a_i X^i$. Platí, že $\deg(\mathbf{g}) < n$ a $\mathbf{g} \neq 0$, tedy x^n+1 nedělí $\mathbf{g}$, ale dělí $\sum_{i=0}^{n-1} a_i X^i$. Protože $\deg(\sum_{i=0}^{n-1} a_i X^i) < n$, tak $\sum_{i=0}^{n-1} a_i X^i = 0$ a a_i jsou tedy všechny rovny nule.

Vektory z $B(\mathbf{g})=\{\mathbf{g}, x\mathbf{g}, x^2\mathbf{g}, \ldots x^{n-1}\mathbf{g}\}$ zřejmě generují $\langle \mathbf{g} \rangle$. Pokud totiž $\mathbf{f} \cdot \mathbf{g} \in \langle \mathbf{g} \rangle$, kde $\mathbf{f} \in \mathbb{Z}[X]/(x^n+1)$, pak můžeme psát $\mathbf{f} = \mathbf{q}(x^n+1) + \sum_{i=0}^{n-1} a_i x^i$, a tedy $\mathbf{f} \cdot \mathbf{g} = \mathbf{g}\mathbf{q}(x^n+1) + \sum_{i=0}^{n-1} a_i \mathbf{g} x^i \equiv_{(x^n+1)} \sum_{i=0}^{n-1} a_i \mathbf{g} x^i$.

□

Příklad: Nechť $n = 3$, tj. $R = \mathbb{Z}[X]/(x^3+1)$, a zvolme $\mathbf{g} = (1+x)$ dělitele $(1+x^3)$. Pak vektory $B(\mathbf{g}) = \{(1,1,0), (0,1,1), (-1,0,1)\}$ jsou lineárně závislé.

Příklad: Nechť $R = \mathbb{Z}[X]/(x^4+1)$, tj. platí, že $x^4 \equiv -1$. Dále nechť $g = x^3+5x^2+3x+2$. Pak

$$\begin{aligned} Xg &= x^4+5x^3+3x^2+2x \equiv 5x^3+3x^2+2x-1 \\ X^2g &= x^5+5x^4+3x^3+2x^2 \equiv 3x^3+2x^2-x-5 \\ X^3g &= x^6+5x^5+3x^4+2x^3 \equiv 2x^3-x^2-5x-3 \end{aligned}$$

$B(\mathbf{g}) = \{(1,5,3,2),(5,3,2,-1),(3,2,-1,-5),(2,-1,-5,-3)\}$ je báze $\langle \mathbf{g} \rangle \subset \mathbb{Z}^4$ a libovolný prvek $a = (a_1,a_2,a_3,a_4) \in \langle \mathbf{g} \rangle$ lze napsat jako lineární kombinace bázových vektorů z $B(\mathbf{g})$ nad celými čísly, tj. $\exists\, z = (z_1,z_2,z_3,z_4) \in \mathbb{Z}^4$ takový, že

$$z1 \cdot \begin{pmatrix} 1 \\ 5 \\ 3 \\ 2 \end{pmatrix} + z_2 \cdot \begin{pmatrix} 5 \\ 3 \\ 2 \\ -1 \end{pmatrix} + z_3 \cdot \begin{pmatrix} 3 \\ 2 \\ -1 \\ -5 \end{pmatrix} + z_4 \cdot \begin{pmatrix} 2 \\ -1 \\ -5 \\ -3 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

Tvrzení 6. *Nechť $\mathbf{u} \in R$ je libovolný, pak existuje právě jeden prvek $\mathbf{u}' \in R$ takový, že $\mathbf{u} - \mathbf{u}' \in \langle \mathbf{g} \rangle$ a*

$$\mathbf{u}' = \sum_{i=0}^{n-1} \alpha_i X^i \mathbf{g}, \text{ kde všechny } \alpha_i \text{ leží v intervalu } \left[-\frac{1}{2}, \frac{1}{2}\right).$$

Důkaz. Uvažujme $\mathbf{h} \in R$ jako prvek $\mathbb{Z}^n$, resp. $\mathbb{Q}^n$. Víme, že $B(\mathbf{g})$ je báze mříže $\mathbb{Z}^n$, tedy je to i báze vektorového prostoru $\mathbb{Q}^n$. Vezměme $\{\mathbf{h}\}_{B(\mathbf{g})}$ - souřadnice prvku $\mathbf{h}$ v $\mathbb{Q}^n$ vzhledem k bázi $B(\mathbf{g})$. Označme $\mathbf{u}' = \{\mathbf{h}\}_{B(\mathbf{g})} - [\{\mathbf{h}\}_{B(\mathbf{g})}]$, kde $[\cdot]$ značí celou část, tedy $\mathbf{u}' = (\alpha_0, \ldots, \alpha_n)$, kde $\alpha_i \in \left[-\frac{1}{2}, \frac{1}{2}\right)$. Pak prvek $\mathbf{u}' = \sum_{i=0}^{n-1} \alpha_i X^i \mathbf{g}$ je ten, který hledáme. □

Pozorování. *Platí, že $\mathbf{u} + \langle \mathbf{g} \rangle = \mathbf{u}' + \langle \mathbf{g} \rangle$ a $\|\mathbf{u}'\| < n \cdot \|\mathbf{g}\|$.*

Příklad: Nechť $R = \mathbb{Z}[X]/(x^4+1)$, $\mathbf{g} = (1,1,1,1)$. Pak označme
$b_1 = \mathbf{g}$, $b_2 = X\mathbf{g}$, $b_3 = X^2\mathbf{g}$, $b_4 = X^3\mathbf{g}$, a tedy
$B(\mathbf{g}) = \{b_1,b_2,b_3,b_4\} = \{(1,1,1,1),(1,1,1,-1),(1,1,-1,-1),(1,-1,-1,-1)\}$ je báze $\langle \mathbf{g} \rangle$.
Pro náš příklad zkonstruujeme bázi $B'(\mathbf{g}) = \{b_1', b_2', b_3', b_4'\}$, kde

$$\begin{aligned} b_1' &= b_1 = (1,1,1,1) & b_3' &= b_3 - b_2 = (0,0,-2,0) \\ b_2' &= b_2 - b_1 = (0,0,0,-2) & b_4' &= b_4 - b_3 = (0,-2,0,0) \end{aligned}$$

tj. $B'(\mathbf{g}) = \{(1,1,1,1), (0,0,0,-2), (0,0,-2,0), (0,-2,0,0)\}$.
Zvolme $\mathbf{u} = (5,2,1,4) \in R$, pak redukce $\mathbf{u}$ modulo $B'(\mathbf{g})$ je

$$\mathbf{u}' = 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + (-\frac{1}{2}) \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \end{pmatrix} + (-\frac{1}{2}) \cdot \begin{pmatrix} 0 \\ -2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \notin \langle \mathbf{g} \rangle$$

a $\mathbf{u} - \mathbf{u}' = (5,2,1,4) - (0,1,0,1) = (5,1,1,3) \in \langle \mathbf{g} \rangle$, neboť $\exists\, z = (z_1, z_2, z_3, z_4) \in \mathbb{Z}^4$ takové, že $z_1.b_1' + z_2.b_2' + z_3.b_3' + z_4.b_4' = \mathbf{u} - \mathbf{u}'$. Konkrétně $z = (5,1,2,2)$:

$$5 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ -2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \\ 1 \\ 3 \end{pmatrix}$$

Platí následující tvrzení:

Tvrzení 7. *Nechť $\mathcal{I} = \langle \mathbf{g} \rangle$ je nenulový prvoideál, pak $R/\mathcal{I}$ je konečný obor.*

Důkaz. R i $\mathcal{I}$ jsou volné $\mathbb{Z}$-moduly hodnosti 2^k. Podle [4, I.6.3] existuje $\mathbb{Z}$-báze R, $\{e_i\}_{i=1}^{2^k}$ a celá čísla $\{r_i\}_i$ taková, že $\{e_i \cdot r_i\}_i$ je $\mathbb{Z}$-báze $\mathcal{I}$. Žádné r_i není nulové, protože kdyby bylo, pak by $\mathcal{I}$ nemělo hodnost 2^k. Z lemmatu [4, I.6.4] plyne, že $R/I \cong \oplus e_i\mathbb{Z}/e_i r_i\mathbb{Z} \cong \oplus \mathbb{Z}_{r_i}$. Všechny $\mathbb{Z}_{r_i}$ jsou ale konečné, a tedy izomorfní $R/\mathcal{I}$ je také konečný. □

Konečný obor integrity je nutně těleso. Zobrazení ρ dané násobením nenulovým prvkem, je totiž na konečném oboru integrity bijekce a tedy pro libovolný nenulový prvek a existuje jeho inverz $\rho^{-1}(a)$, tedy $R/\mathcal{I}$ je konečné těleso.
Okruh $R/\mathcal{I}$ je těleso řádu p^r pro nějaké prvočíslo p a $r \in \mathbb{N}$. Článek [6, 5.2] navrhuje, aby při použití konstrukce GGH pro jednokolovou výměnu klíčů mezi N účastníky byl $\mathbf{g}$ volen tak, aby řád $R/\mathcal{I}$ byl velké prvočíslo.

2.3 Reducibilita $x^{2^k} + 1$ v $\mathbb{Z}_q[X]$

V této části ukážeme, že $x^{2^k} + 1$ není ireducibilní v $\mathbb{Z}_q[X]$ a tedy
$R_q = \mathbb{Z}_q[X]/(x^{2^k} + 1)$ není obor integrity, viz důsledek 11 na konci.

Příklad: V $\mathbb{Z}_{11}[X]$ se polynom $x^n + 1$, kde $n = 2^4$ rozkládá na součin polynomů $x^{16} + 1 = (x^8 + 3x^4 + 10) \cdot (x^8 + 8x^4 + 10)$. Pak ale okruh $\mathbb{Z}_{11}[X]/(x^{16} + 1)$ není obor integrity (svědkem jsou nenulové polynomy $x^8 + 3x^4 + 10$ a $x^8 + 8x^4 + 10$, jejichž součin je v tomto okruhu nulový), a tedy není ani těleso.

Další příklady jsou rozklad $x^{256} + 1$ v okruhu $\mathbb{Z}_{9973}[X]$:

$$x^{256} + 1 \;=\; (x^{128} + 2798) \cdot (x^{128} + 7175)$$

nebo rozklad polynomu $x^8 + 1$ v okruhu $\mathbb{Z}_{17}[X]$:

$$x^8 + 1 \;=\; (x+3)(x+5)(x+6)(x+7)(x+10)(x+11)(x+12)(x+14).$$

Lemma 8. *Nechť q je prvočíslo, $n = 2^k$, pak nekonstantní polynomy v okruhu $\mathbb{Z}_q[X]/(x^n + 1)$ jsou invertibilní právě tehdy, když jsou nesoudělné s $(x^n + 1)$.*

Důkaz. Zprava doleva: pokud máme prvek $f(x)$ nesoudělný s $x^n + 1$ v $\mathbb{Z}_q[X]$, pak jeho inverz nalezneme pomocí rozšířeného Euklidova algoritmu (jsme v euklidovském oboru), ze kterého získáme Bézoutovu rovnost. Konkrétně

$$1 = \mathrm{NSD}_{\mathbb{Z}_q[X]}(f(x), x^n + 1) \;=\; a(x)f(x) + b(x)(x^n + 1),$$

tj. máme $1 \equiv a(x)f(x) \bmod (x^n + 1)$, a tedy $a(x)$ je inverzní prvek k $f(x)$ v $\mathbb{Z}_q[X]/(x^n + 1)$.

Zleva doprava: nechť $f(x)$ je invertibilní, tj. existuje $a(x)$ takové, že

$$f(x)a(x) \equiv 1 \bmod (x^n + 1).$$

Pak musí existovat $b(x)$ takový, že $a(x)f(x) - 1 = b(x)(x^n + 1)$. Pak rovnost $a(x)f(x) - b(x)(x^n + 1) = 1$ implikuje, že $\mathrm{NSD}_{\mathbb{Z}_q[X]}(f(x), x^n + 1)$ dělí 1, tj. $f(x)$ je nesoudělné s $(x^n + 1)$. □

Cyklotomické polynomy a okruh R_q

Nechť $m := 2^{k+1}$. Grupa jednotek v $\mathbb{Z}_m$ je $\mathbb{Z}_m^* = \{1,3,5,7,\ldots,2^{k+1}-1\}$, tj. $n := \varphi(m) = |\mathbb{Z}_m^*| = 2^k$; m-tou primitivní odmocninu z jedné značíme ζ_m, m-tý cyklotomický polynom je její minimální polynom nad $\mathbb{Q}$ a značíme ho $\Phi_m(x)$. Platí, že $\Phi_m(x) \mid x^m - 1$ a koeficienty $\Phi_m(x)$ jsou celá čísla, tj. $\Phi_m(x) \in \mathbb{Z}[X]$. $\Phi_m(x) = \prod_{k\in\mathbb{Z}_m^*}(x - \zeta_m^k) \in \mathbb{Z}[X]$ a tedy stupeň $\Phi_m(x)$ je $\varphi(m) = 2^k$. $\Phi_m(x)$ je ireducibilní v okruhu $\mathbb{Q}[X]$ i $\mathbb{Z}[X]$.

Víme tedy, že $\Phi_m(x) = \Phi_{2n}(x)$ je ireducibilní stupně $\varphi(m) = n$ a dělí $x^m - 1$. Zřejmě platí $x^m - 1 = (x^n - 1)(x^n + 1)$, tedy $(x^n + 1)$ je jediný ireducibilní dělitel $x^m + 1$ stupně n, a tedy $\Phi_m(x) = x^n + 1$. Poznamenjeme, že $2n$-té primitivní odmocniny z jedné jsou n-té primitivní odmocniny z mínus jedné.

Rozšíření tělesa $\mathbb{Q}$ o m-tou primitivní odmocninu z jedné tedy je

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}[X]/\Phi_m(x) = \mathbb{Q}[X]/(x^{2^k} + 1).$$

$\mathbb{Q}(\zeta_m)$ je tedy tělesové rozšíření $\mathbb{Q}$ stupně 2^k a jeho báze coby vektorového prostoru nad $\mathbb{Q}$ je $1,\zeta_m,\zeta_m^2,\ldots,\zeta_m^{2^k-1}$.
Říkáme, že prvek z $\mathbb{Q}(\zeta_m)$ je celistvý nad $\mathbb{Z}$, pokud je kořenem monického polynomu s celočíselnými koeficienty. Například ζ_m je celistvý, protože je kořenem polynomu $x^m - 1$. Okruhem celistvých čísel tělesa $\mathbb{Q}(\zeta_m)$, tj. množina všech celistvých prvků z $\mathbb{Q}(\zeta_m)$ je

$$\mathcal{O} := \mathbb{Z}[\zeta_m] = \mathbb{Z}[X]/\Phi_m(x) = \mathbb{Z}[X]/(x^{2^k} + 1).$$

Platí, že každý okruh celistvých čísel, tedy i $\mathcal{O}$, je dedekindův obor a volný $\mathbb{Z}$-modul.
Dedekindův obor je takový obor integrity, kde se každý vlastní ideál rozkládá na prvoideály, a to až na přerovnání jednoznačně. Volný modul je modul, který má bázi, tj. lineárně nezávislou množinu prvků, která jej generuje. Báze $\mathcal{O}$ je $1,\zeta_m,\zeta_m^2,\ldots,\zeta_m^{2^k-1}$.

Tvrzení 9. *Nechť q je prvočíslo a NSD(m,q) = 1. Pak cyklotomický polynom $\Phi_m(x)$ je ireducibilní nad $\mathbb{F}_q$ právě tehdy, když q mod m je generátor $\mathbb{Z}_m^*$.*

Důkaz. Nechť ζ je m-tá primitivní odmocnina z jedné a $\mathbb{F}[\zeta] = \mathbb{F}_{q^k}$,
tj. $\mathbb{F}_{q^k}$ je nejmenší tělesové rozšíření $\mathbb{F}_q$, kde leží ζ.
Prvek ζ leží v tělese $\mathbb{F}_{q^k}$, tedy platí $\zeta^{q^k-1} = 1$ (řád multiplikativní grupy $\mathbb{F}_{q^k}$ je $q^k - 1$), což je ekvivalentní $m \mid q^k - 1$, neboli $q^k \equiv 1 \pmod m$. Z minimality tělesového rozšíření, plyne, že k je nejmenší takové, že $q^k \equiv 1 \pmod m$.
Pak z teorie o konečných tělesech víme, že minimální polynom ζ nad $\mathbb{F}_q$ je

$$m(x) = (x - \zeta)(x - \zeta^q)(x - \zeta^{q^2})\cdots(x - \zeta^{q^{k-1}}).$$

Označme množinu kořenů polynomu $m(x)$:

$$\mathcal{M}_{m(x)} = \{\zeta,\zeta^q,\zeta^{q^2},\ldots,\zeta^{q^{k-1}}\}.$$

Platí, že $m(x) \mid \Phi_m(x)$ (připomeňme, že $\Phi_m(x)$ sice je minimální polynom ζ ale nad $\mathbb{Z}$, tedy nad konečným tělesem se může rozkládat).
$\Phi_m(x) = \prod_{k \in \mathbb{Z}_m^*}(x - \zeta^k)$, tj. kořeny $\Phi_m(x)$ jsou

$$\mathcal{M}_{\Phi_m(x)} = \{\zeta^a \,:\, 1 \leq a < m\,, \mathrm{NSD}(m,a) = 1\} = \{\zeta^a \,:\, a \in \mathbb{Z}_m^*\}.$$

$\Phi_m(x)$ je tedy ireducibilní v $\mathbb{F}_q$ právě tehdy, když jsou množiny kořenů $m(x)$ a $\Phi_m(x)$ stejné. A $\mathcal{M}_{\Phi_m(x)} = \mathcal{M}_{m(x)}$ právě tehdy, když q generuje $\mathbb{Z}_m^*$.

□

Dokonce platí následující tvrzení:

Tvrzení 10. *$\Phi_m(x)$ se rozkládá na $\varphi(m)/d$ různých monických ireducibilních polynomů téhož stupně d, kde d je nejmenší přirozené číslo takové, že*

$$q^d \equiv 1 \ mod\ m.$$

Důkaz. Viz [8, věta 5.3, strana 20]. □

Nechť $a \in \mathbb{Z}, \mathrm{NSD}(a,m) = 1$. Říkáme, že a je *primitivní kořen modulo m*, pokud řád a je $\varphi(m)$ v $\mathbb{Z}_m^*$, ekvivalentně a je generátor grupy $\mathbb{Z}_m^*$ (a tedy $\mathbb{Z}_m^*$ je cyklická).

Nechť $n = 2^k, m = 2n$. Z tvrzení 9 plyne, že $\mathbb{Z}_q[X]/\Phi_m(x) = \mathbb{Z}_q[X]/(x^n + 1)$ je těleso (a tedy všechny nenulové prvky jsou invertibilní) pokud prvočíslo q mod m je generátor $\mathbb{Z}_m^*$, neboli q je primitivní kořen modulo m

Z teorie čísel víme, že platí, primitivní kořen modulo m existuje (ekvivalentně $\mathbb{Z}_m^*$ je cyklická) právě tehdy, když m je tvaru $2, 4, p^\ell, 2p^\ell$, kde p je liché prvočíslo, $\ell \in \mathbb{N}$. Pro zajímavost toto dokázal Gauss.

V naší konstrukci ale potřebujeme $m = 2^{k+1}$ pro $k > 1$, tedy snaha aby $R_q = \mathbb{Z}_q[X]/\Phi_m(x) = \mathbb{Z}_q[X]/(x^n + 1)$ bylo těleso je marná pro libovolné q a dokázali jsme tedy následující:

Důsledek 11. *Nechť $n = 2^k$, $1 < k \in \mathbb{N}$ a q je prvočíslo, pak:*
Okruh $R_q = \mathbb{Z}_q[X]/(x^n + 1)$ není obor integrity.

Příklad:
$n = 2, m = 4, q = 3, d = 2 = \varphi(m)$:
$\mathbb{Z}_m^* = \{1,3\} = \{3 \bmod 4, 3^2 \bmod 4\}$, tedy $\mathbb{Z}_3[X]/\Phi_4(x) = \mathbb{Z}_3[X]/(x^2 + 1)$ je těleso, tedy $x^2 + 1$ je ireducibilní v $\mathbb{Z}_3[X]$.

$n = 4, m = 8, q = 3, d = 2 \neq \varphi(m)$: $\mathbb{Z}_m^* = \{1,3,5,7\}$ není generované q, neboť $3^2 \equiv 1 \pmod 8$. Tedy $\mathbb{Z}_3[X]/\Phi_8(x) = \mathbb{Z}_3[X]/(x^4 + 1)$ není těleso, a tedy $x^4 + 1$ není ireducibilní v $\mathbb{Z}_3[X]$.

$$\left(x^4 + 1 \equiv (x^2 + x + 2)(x^2 + 2x + 2) \bmod 3\right).$$

$n = 4, m = 8, q = 17, d = 1 \neq \varphi(m)$: $\mathbb{Z}_m^* = \{1,3,5,7\}$ není generované q, neboť $17^1 \equiv 1 \pmod 8$. Tedy $\mathbb{Z}_{17}[X]/\Phi_8(x) = \mathbb{Z}_{17}[X]/(x^4 + 1)$ není těleso, a tedy $x^4 + 1$ není ireducibilní v $\mathbb{Z}_{17}[X]$.

$$\left(x^4 + 1 \equiv (x + 2)(x + 8)(x + 9)(x + 15) \bmod 17\right)$$

2.4 Invertibilní prvky v R_q

V této části se budeme věnovat poměru invertibilních prvků v R_q vůči všem prvkům, tj. pravděpodobnosti, že rovnoměrně náhodně zvolený prvek $\mathbf{z}$ v R_q bude invertibilní.

Nechť $n = 2^k$, $k \in \mathbb{N}$, $m = 2n$. Pak

$$\Phi_m(x) = x^n + 1 \equiv f_1 \cdot \ldots \cdot f_{n/d} \; ; \; \deg(f_i) = d \; \forall \, i$$

je rozklad (jako v tvrzení 10 výše) na různé monické ireducibilní polynomy v $\mathbb{Z}_q[X]$ kde $q > 2$ je prvočíslo a d je nejmenší takové, že $q^d \equiv 1$.

Tvrzení 12 (Čínská věta o zbytcích)**.** *Buď* $\mathbf{R}$ *obor integrity hlavních ideálů,* $m_1, \ldots, m_n$ *jeho po dvou nesoudělné prvky a označme* $M = m_1 \cdot \ldots \cdot m_n$*. Pak*

$$\mathbf{R}/M \simeq \mathbf{R}/m_1 \times \ldots \times \mathbf{R}/m_n \; .$$

$\mathbb{Z}_q[X]$ je obor integrity hlavních ideálů a $f_1 \cdot \ldots \cdot f_{n/d}$ jsou po dvou různé ireducibilní polynomy, tedy nesoudělné.
Z tvrzení 12 tedy máme okruhový izomorfismus

$$\mathbb{Z}_q[X]/(x^n + 1) \simeq \mathbb{Z}_q[X]/f_1 \times \ldots \times \mathbb{Z}_q[X]/f_{n/d} \; ,$$

kde na pravé straně je součin těles. Pak invertibilní prvky na levé straně odpovídají invertibilním prvkům na pravé straně a to jsou právě ty prvky, které jsou nenulové v každé složce. Podíl invertibilních prvků ku všem prvkům je tedy právě $(\frac{q^d-1}{q^d})^{n/d} = (1 - \frac{1}{q^d})^{n/d}$. Můžeme se dále ptát, jaké jsou pro nás nepříznivé volby prvočísel?

V případě, že $q = s2^{k+1} + 1$; $s \in \mathbb{N}$, tedy $q^1 \equiv 1 \pmod{m}$, kde jako obvykle $n = 2^k$ a $m = 2n$. $\Phi_m(x) = x^n + 1$ se pak rozkládá na součin n lineárních členů. Podíl invertibilních prvků v tomto nejhorším případě bude $(1 - 1/q)^n$.

Číslo tvaru $N = s \cdot 2^r + 1$, kde $s \in \mathbb{N}$ je liché a $2^r > s$, se nazývá Prothovo číslo. Pokud je Protohovo číslo prvočíslem, pak se nazývá Prothovým prvočíslem. Největším dosud nalezeným Prothovým prvočíslem je $10223 \cdot 2^{31172165} + 1$. To je také největší prvočíslo, které není Mersenovo.

Mersenovo prvočíslo je prvočíslo tvaru $q = 2^p - 1$ kde p je prvočíslo. Sedm největších dosud nalezených prvočísel jsou právě tohoto tvaru. Dosud úplně největší je $2^{77232917} - 1$, nalezené na přelomu let 2017/2018. Pokud v naší konstrukci bude $m = 2^p$ a $n = m/2$, pak se polynom $x^n + 1$ bude v $\mathbb{Z}_q$ rozkládat na $n/2$ faktorů a podíl invertibilních prvků v okruhu $\mathbb{Z}_q[X]/(x^n + 1)$ tedy bude $\left(1 - \dfrac{1}{q^2}\right)^{n/2}$.

Naštěstí počet prvočísel, kdy podíl invertibilních prvků bude nejnepříznivější tj. počet Prothových prvočísel, vůči všem prvočíslům bude pravděpodobně málo.

Podívejme se na asymptotické chování podílu invertibilních prvků se zvyšujícím se n pro ten nejnepříznivější případ, kdy podíl invertibilních prvků je roven

$(1-1/q)^n$. Budeme značit $f(n) = \omega(g(n))$, pokud $\forall k > 0 \ \exists n_0 \ \forall n > n_0 \ |f(n)| \geq k \cdot |g(n)|$. V konstrukci GGH je požadováno, aby $q = n^{\omega(1)}$ (jako v [6, Lemma 4]), tj. q je super-polynomiální vzhledem k n. Platí tedy, že $\lim_{n\to\infty} n^c/q(n) = 0$ pro libovolné c. Dále počítejme:

$$\lim_{n\to\infty} \left(1 - \frac{1}{q(n)}\right)^n = \lim_{n\to\infty} \exp\left[n \ln\left(1 - \frac{1}{q(n)}\right)\right] = (+) \quad ;$$

$$\lim_{n\to\infty} \frac{\ln\left(1 + \left(-\frac{1}{q(n)}\right)\right)}{\left(-\frac{1}{q(n)}\right)} \cdot (-1) \cdot \frac{n}{q(n)} = 1 \cdot (-1) \cdot 0 = 0 \quad \text{, tedy}$$

z věty o složené funkci, spojitosti funkce exp a známé limity

$$\lim_{x\to 0} \frac{\ln(1+x)}{x} = 1 \qquad \text{platí, že } (+) = 1$$

Vidíme, že podíl invertibilních prvků $z \leftarrow \mathbb{Z}_q[x]/(x^n + 1)$ se blíží k jedné se zvyšujícím se n. Jak ale skutečně vypadá podíl pro nějaké konečné n?

Podle článku [2], který se zabývá efektivní implementací tohoto a odvozených schématů, používá mimo další (viz [2, strana 4]) tyto parametry: $\lambda = 52$, $\kappa = 6$, $n = 2^{15} = 32768$, $q \approx 2^{2117}$. Podíl invertibilních prvků vůči všem prvkům, neboli pravděpodobnost, že náhodně zvolený prvek je invertibilní, se bude i v tom nejnepříznivějším případě, tj. když q bude Prothovo prvočíslo, rovnat $\left(1 - \frac{1}{2^{2117}}\right)^{2^{15}} \doteq 0,\overbrace{999\ldots9}^{632\times}82822928\ldots$, což je velmi blízko jedné.

2.5 Další pojmy důležité pro GGH

Gaussova funkce (Gausián) Pro $\sigma > 0$ definujme *kulovitou (sférickou) Gaussovu funkci* na $\mathbb{R}^n$ s parametrem σ jako $\rho_\sigma(\mathbf{x}) = \exp(-\pi\|x\|^2/\sigma^2)$ pro každé $\mathbf{x} \in \mathbb{R}^n$. To zobecníme na elipsoidní Gaussovu funkci následovně:
Pro matici $S \in \mathbb{R}^{m\times n}$ hodnosti n definujeme *elipsoidní Gaussovu funkci* na $\mathbb{R}^n$ s parametrem S jako $\rho_S(\mathbf{x}) = \exp(-\pi\mathbf{x}^T(S^TS)^{-1}\mathbf{x}) \ \ \forall \mathbf{x} \in \mathbb{R}^n$. Zřejmě tato funkce závisí na $\Sigma = S^TS$ a ne na konkrétní volbě S. Je také zřejmé, že kulovitý případ lze zpětně dostat volbou $S = \sigma I_n$, kde I_n je jednotková matice $n \times n$.

Elipsoidní diskrétní Gaussova distribuce (rozdělení) nad mříží L s parametrem S je $\forall \mathbf{x} \in L, D_{L,S}(x) = \rho_S(\mathbf{x})/\rho_S(L)$, kde $\rho_S(L)$ značí $\sum_{\mathbf{x}\in L} \rho_S(\mathbf{x})$. Jinými slovy pravděpodobnost $D_{L,S}(\mathbf{x})$ je přímo úměrná $\rho_S(\mathbf{x})$ a jmenovatel je normalizační faktor.
Kulovitá (sférická) diskrétní Gaussova distribuce (rozdělení) nad mříží L s parametrem σ je definována obdobně: $\forall \mathbf{x} \in L, D_{L,\sigma}(x) = \rho_\sigma(\mathbf{x})/\rho_\sigma(L)$, kde $\rho_\sigma(L)$ značí $\sum_{\mathbf{x}\in L} \rho_\sigma(\mathbf{x})$.

Napíšeme-li $\mathbf{v} \leftarrow D_{\mathbb{Z}^m,\sigma}$, znamená to, že prvek $v \in \mathbb{Z}^m$ je výstupem náhodné veličiny s distribucí $D_{\mathbb{Z}^m,\sigma}$.

Nechť máme mřížku L a $0 < \epsilon \in \mathbb{R}$, pak definujme *vyhlazovací (smoothing) parametr* $\eta_\epsilon(L)$ jako nejmenší s takové, že $\rho_{1/s}(L^* \setminus \{0\}) \leq \epsilon$.

Intuitivně, pro dostatečně malé ϵ je $\eta_\epsilon(L)$ větší než základní buňka mříže L.

Největší a nejmenší singulární číslo matice plné hodnosti $X \in \mathbb{R}^{m\times n}$ lze charakterizovat popořadě jako $\sigma_1(X) = \sup(U_X)$ a $\sigma_n(X) = \inf(U_X)$, kde
$U_X = \{\|X\mathbf{u}\| : \mathbf{u} \in \mathbb{R}^n, \|\mathbf{u}\| = 1\}$, $\|\cdot\|$ je eukleidovská norma.

Lze ukázat, že velikost vektorů z $D_{L,S}$ je „zhruba omezena“ největším singulárním číslem matice S, přesněji:

Lemma 13. *Pro bodovou mříž L hodnosti n, konstantu $0 < \epsilon < 1$ a matici S takovou, že $\sigma_n(S) \geq \eta_\epsilon(L)$, platí, že* $\Pr_{\mathbf{v}\leftarrow\mathcal{D}_{L,S}}(\|\mathbf{v}\| \geq \sigma_1(S)\sqrt{n}) \leq \frac{1+\epsilon}{1-\epsilon}\cdot 2^{-n}$.

Důkaz. Viz [1, lemma 3]. □

Toto lemma tedy říká, že (při splnění předpokladu na nejmenší singulární číslo matice S) velikost prvku $\mathbf{v}$ z Gausiánu $\mathbf{v} \leftarrow D_{L,S}$ je téměř jistě menší než součin největšího vlastního čísla a odmocniny z n, tj. téměř jistě $\|\mathbf{v}\| < \sigma_1(S)\sqrt{n}$.

Suma diskrétních gausiánů Práce [1] popisuje proces, který začíná vybráním m bodů v mříži L nezávisle na sobě z diskrétního Gausiánu $\mathbf{x}_i \leftarrow D_{L,S}$, které fixujeme. Sestavíme z nich matici X typu $m \times n$,
$X = (\mathbf{x}_1|\mathbf{x}_2|\ldots|\mathbf{x}_m)^T$ a pak uvažujeme rozdělení $\mathcal{E}_{X,\sigma}$, indukované výběrem celočíselného vektoru $\mathbf{v}$ z diskrétního kulovitého Gausiánu nad $\mathbb{Z}^m$ s parametrem σ a výstupem $\mathbf{y} = X^T\mathbf{v}$, $\mathcal{E}_{X,\sigma} \stackrel{def}{=} \{X^T\mathbf{v} \ : \ \mathbf{v} \leftarrow D_{\mathbb{Z}^m,\sigma}\}$. [1] dokázal, že s vysokou pravděpodobností je X vybráno tak, že distribuce $\mathcal{E}_{X,\sigma}$ je statisticky blízká elipsoidnímu Gausiánu $D_{L,\sigma X}$, a navíc že singulární čísla X jsou zhruba velikosti $\sigma\sqrt{m}$.
To využijeme v protokolu v proceduře $\mathsf{enc}_1(\mathsf{params},\mathbf{d})$ níže.

V popisu protokolu dále budeme značit:
$f(n) = O(g(n))$, pokud $\exists k > 0 \ \ \exists n_0 \ \ \forall n > n_0 \ \ |f(n)| \leq k \cdot g(n)$,
$f(n) = \tilde{O}(g(n))$, pokud $\exists k \ f(n) = O\left(g(n)\cdot \log^k g(n)\right)$ a
$f(n) = \mathrm{poly}(n)$, pokud $\exists k \ f(n) = O(n^k)$

3. Popis konstrukce GGH

Připomeňme definici 2 multilineárního zobrazení a formulujme ji znovu v aditivním značení.

Definice 8. *Říkáme, že zobrazení $e : G_1^\kappa \to G_2$ je κ-multilineární zobrazení, pokud splňuje následující požadavky:*

1. *G_1 a G_2 jsou grupy stejného (prvočíselného) řádu;*
2. *Pokud $\alpha_1, \ldots, \alpha_\kappa \in \mathbb{Z}$ a $x_1, \ldots, x_\kappa \in G_1$ pak*

$$e(\alpha_1 \cdot x_1, \ldots, \alpha_\kappa \cdot x_\kappa) = \alpha_1 \cdots \alpha_\kappa \cdot e(x_1, \ldots, x_\kappa)$$

3. *Zobrazení e není degenerované v následujícím smyslu: pokud $g \in G_1$ je generátor G_1, pak $e(g, \ldots, g)$ je generátor G_2.*

Naše konstrukce jako grupy G_1, G_2 chápe $R/\mathcal{I}$, který je pro nenulový prvoideál $\mathcal{I}$ tělesem řádu p^r, a využívá následující multilineární zobrazení aditivních abelovských grup tělesa $R/\mathcal{I}$:

$$([\mathbf{d}_1]_\mathcal{I} \times \ldots \times [\mathbf{d}_\kappa]_\mathcal{I}) \to [\mathbf{d}_1 \cdot \ldots \cdot \mathbf{d}_\kappa]_\mathcal{I}$$

Toto zobrazení dává konstrukci žádanou multilinearitu, kterou ale konstrukce využívá jakýmsi způsobem skrytě. V konstrukci jsou totiž prvky okruhu $R/\mathcal{I}$ kódovány pomocí dělení prvkem $\mathbf{z}$ v okruhu R_q. Pro jistou podmnožinu prvků (indukovaná omezením velikostí prvků) se multilinearita zachovává. Při kódování navíc využijeme proces „randomizace“, díky kterému stejný prvek okruhu může být zakódován mnoha způsoby a zároveň požadujeme, aby z žádného zakódování nebylo možné bez znalosti tajných parametrů získat zpět původní prvek. To dává konstrukci potřebné kryptografické vlastnosti. Většina výpočtů v konstrukci tedy probíhá v okruhu R_q a multilinearitu okruhu $R/\mathcal{I}$ využívá jen pro dané podmnožiny prvků.
Konstrukce bude rozlišovat různé stupně kódování, podle mocniny jmenovatele $\mathbf{z}$, a proto se konstrukci říká stupňovité kódovací schéma (Graded Encoding Scheme).
Naše konstrukce, jak vyplyne z jejího popisu dále, bude splňovat následující:
Nechť params jsou vhodné parametry, $\mathsf{enc}_i(\mathsf{params}, \cdot)$ je procedura definovaná dále a $\alpha, \mathbf{d}_1, \ldots, \mathbf{d}_\kappa$ jsou dostatečně malé prvky R (zakódování stupně nula), pak

$$\begin{aligned}
\alpha \cdot \mathsf{enc}_1(\mathsf{params}, \mathbf{d_1}) &= \mathsf{enc}_1(\mathsf{params}, \alpha \cdot \mathbf{d_1}), \\
\mathsf{enc}_1(\mathsf{params}, \mathbf{d_1}) \cdot \ldots \cdot \mathsf{enc}_1(\mathsf{params}, \mathbf{d}_\kappa) &= \mathsf{enc}_\kappa(\mathsf{params}, \mathbf{d_1} \cdot \ldots \cdot \mathbf{d}_\kappa), \\
\mathsf{enc}_1(\mathsf{params}, \mathbf{d_1}) + \ldots + \mathsf{enc}_1(\mathsf{params}, \mathbf{d}_\kappa) &= \mathsf{enc}_1(\mathsf{params}, \mathbf{d_1} + \ldots + \mathbf{d}_\kappa).
\end{aligned}$$

3.1 Stupňovité kódovací schéma

Tato konstrukce je parametrizována bezpečnostním parametrem λ a vyžaduje parametr multi-linearity $\kappa \leq \text{poly}(\lambda)$. V závislosti na těchto parametrech volíme cyklotomický okruh $R = \mathbb{Z}[X]/(x^n+1)$ (kde $n = 2^k$ je dostatečně velké k zajištění

bezpečnosti), modulus q který definuje $R_q = R/qR$ (kde q je dostatečně velké prvočíslo), a další parametr m. Parametry by měli splňovat: $n = \tilde{O}(\kappa\lambda^2)$, $q \approx 2^{n/\lambda}$ a $m = O(n^2)$, tedy q je super-polynomiální vzhledem k n a $n = \text{poly}(\lambda)$.

V této konstrukci jsou kódovány prvky faktorokruhu

$$R_g = R/\mathcal{I} \simeq \mathbb{Z}[X]/(x^n + 1, g) \quad \text{, kde } [g]_{(x^n+1)} = \mathbf{g},$$

kde $\mathcal{I}$ je prvoideál $\mathcal{I} = \langle \mathbf{g} \rangle \subset R$, generovaný malým vektorem $\mathbf{g}$. Malý v našem kontextu znamená, že jeho velikost $\|\cdot\|$ je patřičně omezena, v našem schématu obvykle $< q^{1/8}$, pokud neřekneme jinak. Jmenovitě jsou kódovány faktortřídy $\mathbf{e} + \mathcal{I}$ pro nějaký vektor $\mathbf{e}$. Generátor $\mathbf{g}$ ideálu $\mathcal{I}$ je utajen, stejně jako je třeba utajit jakýkoli jiný „dobrý“ popis ideálu $\mathcal{I}$. Dále se volí tajný prvek $\mathbf{z}$, který je zvolen uniformně náhodně v R_q (a proto nemusí být malý). Kvůli konstrukci potřebujeme aby byl invertibilní, tedy otestujeme, viz důkaz lemmatu 8 pomocí euklidova rozšířeného algoritmu, zda je invertibilní. Pokud ne, náhodně zvolíme další.

V konstrukci se používá následující terminologie:
Zakódování stupně nula prvku $\mathbf{e} + \mathcal{I} \in R/\mathcal{I}$ je malý vektor v této faktortřídě (ten existuje z tvrzení 6, protože $\mathbf{g}$ je malé a $\mathbf{e} + \mathcal{I} = \mathbf{e}' + \mathcal{I}$).
Zakódování stupně i prvku $\mathbf{e} + \mathcal{I}$ je vektor tvaru $\mathbf{c}/\mathbf{z}^i \in R_q$, kde $\mathbf{c} \in \mathbf{e} + \mathcal{I}$ je malý. Prvek c pak nazýváme čitatel.
Přesněji, pro $i \in \{0,1,\ldots,\kappa\}$ je množina všech možných zakódování $S_i = \{\mathbf{c}/\mathbf{z}^i \in R_q : \|\mathbf{c}\| < q^{1/8}\}$. Tedy množina všech zakódování stupně i prvku $\mathbf{e} + \mathcal{I}$ je $S_i^{(\mathbf{e}+\mathcal{I})} = \{\mathbf{c}/\mathbf{z}^i \in R_q : \mathbf{c} \in \mathbf{e} + \mathcal{I}, \|\mathbf{c}\| < q^{1/8}\}$.

Konstrukce GGH je „citlivá“ na velikost čitatelů $\|\mathbf{c}\|$. Pokud překročí určitou horní mez, protokol nemusí fungovat správně. Je nutné opatrně volit parametry tak, aby pravděpodobnost, že velikost čitatelů mez překročí, bude zanedbatelná a zároveň aby proces randomizace dostatečně „znáhodňoval“. Přesný popis a matematické zdůvodnění volby parametrů, ale přesahuje rámec této práce.

Pro celá čísla t, q budeme redukci t modulo q do intervalu $[-q/2, q/2)$ značit $[t]_q$.

V konstrukci GGH jsou definovány následující procedury:

Instance generation: $(\mathsf{params}, \mathbf{p}_{zt}) \leftarrow \mathsf{InstGen}(\lambda, \kappa)$
Vhodně zvol $n \in \mathbb{N}$ a prvočíslo q.
Vyber tajný prvek $\mathbf{g} \leftarrow D_{\mathbb{Z}^n,\sigma}$, kde $\sigma = \sqrt{\lambda n}$, $\mathcal{I} := \langle \mathbf{g} \rangle$, tak aby $\mathcal{I}$ byl prvoideál a $\|\mathbf{g}^{-1}\| < n^2$.
Uniformně náhodně vyber $\mathbf{z}$ z množiny invertibilních prvků R_q.
Nechť $\sigma' = \sigma n$.
Vyber $\mathbf{b}_i \leftarrow D_{\mathcal{I},\sigma'}$ pro $i = 1,\ldots,m$ a polož $\mathbf{x}_i = [\mathbf{b}_i/\mathbf{z}]_q$.
Vyber $\mathbf{a} \leftarrow D_{1+\mathcal{I},\sigma'}$ a polož $\mathbf{y} = [\mathbf{a}/\mathbf{z}]_q$.
Vyber $\mathbf{h} \leftarrow D_{\mathbb{Z}^n,\sqrt{q}}$ a označme zero-test parametr $\mathbf{p}_{zt} = [\mathbf{h}\mathbf{z}^\kappa/\mathbf{g}]_q$.
Náhodně vyber seed s pro strong randomness extractor.
Výstupem jsou veřejné parametry $\mathsf{params} = (n, q, \sigma, \mathbf{y}, \{\mathbf{x}_i\}_{i \le m}, s)$ a $\mathbf{p}_{zt}$.

Z lemmatu 13 plyne, že téměř jistě $\|\mathbf{g}\| < \sigma\sqrt{n} = n\sqrt{\lambda} = O(n^2)$ a $\|\mathbf{a}\|, \|\mathbf{b}_i\| <$

$\sigma'\sqrt{n} = \sigma n^{3/2} = \sqrt{\lambda} n^2 = O(n^3)$.
Dále poznamenejme, že $\mathbf{b}_i \in \mathcal{I}$ a $\mathbf{a} \in 1 + \mathcal{I}$, tedy říkáme, že $\mathbf{b}_i$ jsou zakódování prvku 0 stupně nula a $\mathbf{a}$ je zakódování prvku 1 stupně nula. Dále říkáme, že $\mathbf{x}_i = [\mathbf{b}_i/\mathbf{z}]_q$ je zakódování prvku 0 stupně jedna a $\mathbf{y} = [\mathbf{a}/\mathbf{z}]_q$ je zakódování prvku 1 stupně jedna. Též budeme nazývat $\mathbf{x}_i$ jako randomizers. Říkáme, že $\mathbf{g}$, $\mathbf{b}_i$ a $\mathbf{a}$ jsou malé, protože jejich velikost je téměř jistě omezena $n^3 < q^{1/8}$.

Sampling level-zero encodings: $\mathbf{d} \leftarrow \mathsf{samp}(\mathsf{params})$
`Vyber a vrať` $\mathbf{d} \leftarrow D_{\mathbb{Z}^n,\sigma'}$ `, kde` $\sigma' = \sigma n$

Poznamenejme, že z lemmatu 13 plyne, že téměř jistě $\|\mathbf{d}\| < \sigma n^{3/2} = \sqrt{\lambda} n^2 = O(n^3)$. Říkáme, že $\mathbf{d}$ je zakódování prvku $\mathbf{d} + \mathcal{I}$ stupně 0.
Takto generovaný prvek $\mathbf{d}_i$ bude v protokolu na konci sekce hrát roli soukromého klíče i-tého účastníka.

Encode at level 1: $\mathbf{u} \leftarrow \mathsf{enc}_1(\mathsf{params},\mathbf{d})$
`Spočti` $\mathbf{u}' := [\mathbf{dy}]_q$.
`Proces randomizace:`
`Vyber` $\mathbf{r} = (r_1, \ldots, r_m) \leftarrow D_{\mathbb{Z}^m,\sigma^*}$ `pro` $\sigma^* = 2^\lambda \cdot \|\mathbf{d}\| \cdot \|\mathbf{a}\| \cdot \sqrt{n}$ `a vrať`

$$\mathbf{u} := [\mathbf{u}' + \sum_{j=1}^{m} r_j \mathbf{x}_j]_q$$

Poznámka: V případě potřeby lze tuto proceduru zobecnit na zakódování libovolného stupně $i < \kappa$: $\mathsf{enc}_i(\mathsf{params},\mathbf{d})$.

$\mathbf{u}' = [\mathbf{dy}]_q = [\mathbf{da}/\mathbf{z}]_q$ je zakódování prvku $\mathbf{d}+\mathcal{I}$ stupně jedna, $\mathbf{x}_i = [\mathbf{b}_i/\mathbf{z}]_q$ jsou zakódování prvku nula stupně jedna a $\mathbf{u} = [\mathbf{u}' + \sum_{j=1}^m r_j \mathbf{x}_j]_q = [(\mathbf{da} + \sum_{j=1}^m r_j \mathbf{b}_j)/\mathbf{z}]_q$ je tedy (randomizované) zakódování prvku $\mathbf{d} + \mathcal{I}$ stupně jedna.

Proč byl proces randomizace potřeba? Útočník by totiž mohl se znalostí $\mathbf{u}'$ a $\mathbf{y}$ snadno spočíst $\mathbf{d}$ jednoduchým dělením v R_q, což nechceme.

To se znalostí $\mathbf{u}$ a $\mathbf{y}$ nelze. Jak jsme obecně psali výše, práce [1] dokázala, že rozdělení $\mathbf{u}$ je „skoro“ nezávislá od původního $\mathbf{u}'$. K intuitivnímu nahlédnutí proč, poznamenejme, že pokud jsou $\mathbf{b}_i$ vzaty z dostatečně širokého kulovitého Gausiánu, tak distribuce $\mathbf{Br}$, kde $\mathbf{B} = (\mathbf{b}_1|\ldots|\mathbf{b}_m)$, je blízká dostatečně širokému elipsoidnímu Gausiánu. S naší volbou σ^* je „šířka“ této distribuce mnohem větší než původního $\mathbf{da}$, a tedy rozdělení $\mathbf{da} + \sum_j r_j \mathbf{b}_j$ je skoro nezávislá na $\mathbf{da}$.

Adding and multiplying encodings: $+$, $\cdot$
Dáno $\mathbf{u}_1 = [\mathbf{c}_1/\mathbf{z}^k]_q$ a $\mathbf{u}_2 = [\mathbf{c}_2/\mathbf{z}^k]_q$, kde $k \in 1, \ldots, \kappa$, vrať $\mathbf{u}_+ = [\mathbf{u}_1 + \mathbf{u}_2]_q$.
Dáno $\mathbf{u}_1 = [\mathbf{c}_1/\mathbf{z}^{k_1}]_q$ a $\mathbf{u}_2 = [\mathbf{c}_2/\mathbf{z}^{k_2}]_q$, kde $0 \le k_1 + k_2 \le \kappa$, vrať $\mathbf{u}_* = [\mathbf{u}_1 \cdot \mathbf{u}_2]_q$.

Velmi důležitou vlastností naší konstrukce je, že za předpokladu dostatečně malé velikosti čitatelů $\mathbf{c}_1, \mathbf{c}_2$ - který nebudeme přesně formulovat - platí následující:

$\mathbf{c}_1 + \mathbf{c}_2 = [\mathbf{c}_1 + \mathbf{c}_2]_q \in R_q$ je stále malý prvek v $(\mathbf{c}_1 + \mathcal{I}) + (\mathbf{c}_2 + \mathcal{I})$ a tedy $\mathbf{u}_+ = [\mathbf{u}_1 + \mathbf{u}_2]_q = [(\mathbf{c}_1 + \mathbf{c}_2)/\mathbf{z}^k]_q$ je zakódování $(\mathbf{c}_1 + \mathcal{I}) + (\mathbf{c}_2 + \mathcal{I})$ stupně k.

$\mathbf{c}_1 \cdot \mathbf{c}_2 = [\mathbf{c}_1 \cdot \mathbf{c}_2]_q \in R_q$ je stále malý prvek $(\mathbf{c}_1 + \mathcal{I}) \cdot (\mathbf{c}_2 + \mathcal{I})$ a tedy
$\mathbf{u}_* = [\mathbf{u}_1 \cdot \mathbf{u}_2]_q = [(\mathbf{c}_1 \cdot \mathbf{c}_2)/\mathbf{z}^k]_q$ je zakódování $(\mathbf{c}_1 + \mathcal{I}) \cdot (\mathbf{c}_2 + \mathcal{I})$ stupně $k_1 + k_2$.

Zero testing: $\mathsf{isZero}(\mathsf{params}, \mathbf{p}_{zt}, \mathbf{u}) \stackrel{?}{=} 0/1$
`Výstup: 1 pokud` $\mathbf{u} = [\mathbf{c}/\mathbf{z}^{\kappa}]_q$ `je zakódování nuly, 0 jinak.`
`Vynásob` $\mathbf{u}$ `a` $\mathbf{p}_{zt}$ `v` R_q `a zkontroluj, zda výsledný prvek` $\mathbf{w} = [\mathbf{p}_{zt} \cdot \mathbf{u}]_q$ `je menší než` $q^{3/4}$`. Tedy:`

$$\mathsf{isZero}(\mathsf{params},\mathbf{p}_{zt},\mathbf{u}) = \begin{cases} 1 & \texttt{pokud } \|[\mathbf{p}_{zt}\mathbf{u}]_q\|_\infty < q^{3/4} \\ 0 & \texttt{jinak} \end{cases}$$

Pouze poznamenejme, že $\mathbf{w} = \mathbf{p}_{zt} \cdot \mathbf{u} = \dfrac{\mathbf{h}\mathbf{z}^{\kappa}}{\mathbf{g}} \cdot \dfrac{\mathbf{c}}{\mathbf{z}^{\kappa}} = \mathbf{h} \cdot \mathbf{c}/\mathbf{g}$ (operace v R_q), kde $\mathbf{c}$ je dělitelné $\mathbf{g}$, pokud $\mathbf{u}$ je zakódování nuly a téměř jistě $\|\mathbf{c}\| < q^{1/8}$, $\|\mathbf{h}\| < q^{1/2}$. Pro úplné vysvětlení korektnosti procedury odkazujeme čtenáře na [6, kapitola 4.1, strana 12].

Tuto proceduru v protokolu níže (Návrh jednokolové výměny klíčů pro N účastníků pomocí GGH) potřebovat nebudeme. Ukazuje ale další důležitou vlastnost konstrukce GGH:
Pokud dvě zakódování stupně κ, $\mathbf{u}_1$ a $\mathbf{u}_2$, odečteme a jejich rozdíl vložíme do procedury $\mathsf{isZero}(\mathsf{params}, \mathbf{p}_{zt}, \mathbf{u}_1 - \mathbf{u}_2)$, pak pokud $\mathbf{u}_1$,$\mathbf{u}_2$ jsou zakódování téhož prvku, tak jejich rozdíl $\mathbf{u}_1 - \mathbf{u}_2$ je zakódování nuly stupně κ a tedy procedura vrátí 1. Pokud $\mathbf{u}_1$ a $\mathbf{u}_2$ nebyly zakódováním stejného prvku, tak procedura vrátí 0.

Extraction: $S \leftarrow \mathsf{ext}(\mathsf{params},\mathbf{p}_{zt},\mathbf{u})$
$\mathtt{Tmp} = [\mathbf{u} \cdot \mathbf{p}_{zt}]_q$
$\mathtt{Tmp} = (\beta_1, \ldots, \beta_n)$, `kde` $\beta_i \in \mathbb{Z}_q$
$(\gamma_1 \| \ldots \| \gamma_n) =$ `MSBs(Tmp), kde` γ_i `je` $(\log q)/4 - \lambda$ `nejvýznamnějších bitů` β_i. `(MSBs ... Most Significant Bits)`
$S =$ `EXTRACT`$_s((\gamma_1 \| \ldots \| \gamma_n))$, `kde EXTRACT je strong randomness extractor a` s `jeho seed.`
`Tedy:`

$$\mathtt{ext}(\mathsf{params},\mathbf{p}_{zt},\mathbf{u}) = \mathtt{EXTRACT}_s(\mathtt{MSBs}([\mathbf{u} \cdot \mathbf{p}_{zt}]_q))$$

Tímto získáme „kanonickou“ a „náhodnou“ reprezentaci prvku $\mathbf{e} + \mathcal{I} \ni \mathbf{c}$ z jeho zakódování $\mathbf{u} = [\mathbf{c}/\mathbf{z}^{\kappa}]_q$ stupně κ.
Totiž platí, že výstup MSBs$([\mathbf{u} \cdot \mathbf{p}_{zt}]_q)$, kde $\mathbf{u}$ je zakódování prvku $\mathbf{e} + \mathcal{I}$ stupně κ, je stejný pro všechny volby čitatele $\mathbf{c} \in \mathbf{e} + \mathcal{I}$ a naopak pro zakódování různých prvků $\mathbf{e} + \mathcal{I}$ dává MSBs$(\cdot)$ různé výsledky.
Pokud $\mathbf{u}_1$ a $\mathbf{u}_2$ jsou zakódování téhož prvku, pak viz výše platí:

$$\|\mathbf{p}_{zt}\mathbf{u}_1 - \mathbf{p}_{zt}\mathbf{u}_2\| = \|\mathbf{p}_{zt}(\mathbf{u}_1 - \mathbf{u}_2)\| < q^{3/4},$$

a z toho předpokládáme, že $\mathbf{p}_{zt}\mathbf{u}_1$ a $\mathbf{p}_{zt}\mathbf{u}_2$ se shodují na jejich $(\log q)/4 - \lambda$ nejvýznamnějších bitech. Pro úplné vysvětlení korektnosti procedury odkazujeme čtenáře na [6, kapitola 4.1, strana 13].

3.2 Jednokolová výměna klíčů mezi N účastníky pomocí GGH

GCDH/GDDH předpoklad

Zde uvedeme analogii k obecným předpokladům z první části pro naše schéma. Uvažujme následující proces:

1. $(\mathbf{y},\{\mathbf{x}_i\}_i, \mathbf{p}_{zt}) \leftarrow \mathsf{InstGen}(\lambda, \kappa)$
2. For $i = 0, \ldots, \kappa$
3. Vyber $\mathbf{e}_i, \mathbf{f} \leftarrow D_{\mathbb{Z}^n,\sigma}$
4. Spočti $\mathbf{u}_i = \left[\mathbf{e}_i\mathbf{y} + \sum_j r_{ij}\mathbf{x}_j\right]_q$ kde $r_{ij} \leftarrow D_{\mathbb{Z}^m,\sigma^*}$
5. Spočti $\mathbf{u}^* = [\prod_{i=1}^{\kappa} \mathbf{u}_i]_q$
6. Spočti $\mathbf{v} = [\mathbf{e}_0 \cdot \mathbf{u}^*]_q$
7. Spočti $\mathbf{v}' = [\mathbf{f} \cdot \mathbf{u}^*]_q$

Pak *Graded MCDH problém (GCDH)* je úloha nalezení zakódování prvku $\prod_i \mathbf{e}_i + \mathcal{I}$ stupně κ, tj. $\mathbf{v}$, při známém vstupu $((\mathbf{y},\{\mathbf{x}_i\}_i,\mathbf{p}_{zt}),\mathbf{u}_0,\ldots,\mathbf{u}_\kappa)$ a
Graded MDDH problém (GDDH) je úloha rozlišit $\mathbf{v}$ a $\mathbf{v}'$, přesněji rozlišit rozdělení
$\mathcal{D}_{GDDH} = \{(\mathbf{y},\{\mathbf{x}_i\}_i,\mathbf{p}_{zt}),\mathbf{u}_0,\ldots,\mathbf{u}_\kappa,\mathbf{v}\}$ a
$\mathcal{D}_{RAND} = \{(\mathbf{y},\{\mathbf{x}_i\}_i,\mathbf{p}_{zt}),\mathbf{u}_0,\ldots,\mathbf{u}_\kappa,\mathbf{v}'\}$.

V protokolu níže budeme předpokládat, že problém GDDH (a tedy i GCDH) je těžký. Článek [6] se kryptoanalýze těchto předpokladů věnuje ve dvou rozsáhlých sekcích, i přesto ale sám konstatuje, že je třeba provést ještě další výzkum v této oblasti a tedy zatím není vůbec jisté, zda tyto předpoklady skutečně splněné jsou.

Konstrukce protokolu

Poznamenejme, že jde o aplikování naší konstrukce do obecného protokolu 1 definovaného v první kapitole, ovšem za silnějšího GDDH předpokladu (v původním protokolu jsme vyžadovali pouze MCDH předpoklad). $\kappa = N - 1$.

$\mathsf{Setup}(\lambda, N)$ Tato procedura pouze spustí proceduru $\mathsf{InstGen}$ a z ní získá veřejné parametry $(\mathsf{params}, \mathbf{p}_{zt}) \leftarrow \mathsf{InstGen}(\lambda, N-1)$, které vrátí jako výstup.
Poznamenejme, že $\mathbf{p}_{zt}$ je zero-test parametr pro zakódování stupně $N - 1$.

$\mathsf{Publish}(\mathsf{params},\mathbf{p}_{zt},i)$ Každý účastník i si vybere prvek kódování stupně nula $\mathbf{d}_i \leftarrow \mathsf{samp}(\mathsf{params})$ jako svůj tajný klíč a zveřejní jeho zakódování stupně jedna jako svůj veřejný klíč, tj. $\mathbf{w}_i \leftarrow \mathsf{enc}_1(\mathsf{params},\mathbf{d})$.

$\mathsf{KeyGen}(\mathsf{params},\mathbf{p}_{zt},j,\mathbf{d}_j,\{\mathbf{w}_i\}_{i\neq j})$ Každý účastník j vynásobí jeho tajný klíč $\mathbf{d}_j$ s veřejnými klíči ostatních účastníků $\{\mathbf{w}_i\}_{i\neq j}$, t.j. $\mathbf{v}_j \leftarrow \mathbf{d}_j \cdot \prod_{i\neq j} \mathbf{w}_i$, a získá tak zakódování stupně $N-1$ prvku $\prod_i \mathbf{d}_i + \mathcal{I} \in R/\mathcal{I}$ (zde se využívá multilinearita naší konstrukce). Z toho pak vyextrahuje společný tajný klíč $s_j \leftarrow \mathsf{ext}(\mathsf{params},\mathbf{p}_{zt},\mathbf{v}_j)$.

V článku [6, kapitola 5.2, tvrzení 2] je dokázáno, že za GDDH předpokladu je protokol bezpečný v tom smyslu, že útočník se znalostí všech veřejných klíčů $\mathbf{w}_i$ nedokáže rozlišit společný klíč s od náhodného prvku.

Závěr

V první kapitole naší práce jsme se seznámili s teoretickým konstruktem multilineárního zobrazení. Jako odůvodnění tohoto konceptu jsme uvedli příklad protokolu Jednokolová výměna klíčů mezi N účastníky, neboli Diffie-Hellman pro N účastníků. Tento protokol má při použití multilineárního zobrazení výrazně nižší počet operací - asymptoticky došlo ke zlepšení z $N \log N$ na $2N$.
V druhé a třetí kapitole jsme zpracovali návrh konstrukce GGH [6] založeného na ideálových mříží, u kterého jsme vyjasnili některé algebraické nejasnosti. Tato konstrukce díky svým multilineárním vlastnostem nabízí vhodného kandidáta, kterého, jak jsme ukázali na konci třetí části, lze použít pro Jednokolovou výměnu klíčů mezi N účastníky.

Tato konstrukce pracuje s několika netriviálními okruhy R, $R/\mathcal{I}$ a R_q. Studiu některých vlastností těchto okruhů a seznámení s pojmy bodová a ideálová mříž jsme se věnovali v kapitole druhé. Ukázali jsme, že okruh $R = \mathbb{Z}[X]/(x^n + 1)$ je oborem integrity právě tehdy, když $n = 2^k$, a ztotožnili ho s celočíselnou mřížkou $\mathbb{Z}^n$. Dále jsme se věnovali okruhu $R/\mathcal{I}$. Ukázali jsme, že $B(\mathbf{g})$ je za předpokladu ireducibility $x^n + 1$ báze ideálové mříže $\langle \mathbf{g} \rangle = \mathcal{I}$, uvedli jsme konkrétní příklady jak okruh $R/\mathcal{I}$ a báze $B(\mathbf{g})$ vypadá (a kdy $B(\mathbf{g})$ naopak není báze) a vysvětlili, proč $R/\mathcal{I}$ může mít prvočíselný řád. Dále jsme o okruhu R_q, po připomenutí teorie konečných těles a důkazu jednoho tvrzení, dokázali, že nemůže být oborem integrity, a tedy náhodně zvolený prvek v něm nemusí být invertibilní. Proto jsme se poté věnovali počtu invertibilních prvků v R_q a z čínské věty o zbytcích jsme ukázali, že i v pro nás nejnepříznivějším případě, tedy když q je Prothovo prvočíslo, je počet invertibilních prvků v okruhu R_q dostatek. Na konci druhé kapitoly jsme pak zavedli několik pojmů (diskrétní Gausián) a uvedli jejich vlastnosti, které jsou v konstrukci GGH potřeba.

V kapitole třetí jsme pak popsali celou konstrukci GGH, ukázali její velmi zajímavé multilineární vlastnosti plynoucí z využití okruhu $R/\mathcal{I}$ a vysvětlili proces kódování a randomizace, která probíhá v okruhu R_q a ze které plyne bezpečnost celé konstrukce. Na konci třetí kapitoly jsme pak ukázali využití konstrukce GGH a z jednotlivých procedur jsme sestrojili protokol Jednokolové výměny klíčů mezi N účastníky.

Kdybychom v definici multilineárního zobrazení nevyžadovali prvočíselný řád grup a třetí podmínku nedegenerovanosti bychom pozměnili například tak, že pokud prvek g má řád ℓ, pak $e(g, \ldots, g)$ má řád ℓ, tak pak bychom v naší konstrukci mohli podmínku, aby $\mathcal{I}$ byl prvoideál (a tedy $R/\mathcal{I}$ bylo těleso), vynechat a navrhujeme k dalšímu studiu domněnku, že by protokol i přesto zůstal bezpečný.

Seznam použité literatury

[1] Shweta Agrawal, Craig Gentry, Shai Halevi, and Amit Sahai. Discrete gaussian leftover hash lemma over infinite domains. Cryptology ePrint Archive, Report 2012/714, 2012. https://eprint.iacr.org/2012/714.

[2] Martin R. Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois. Implementing candidate graded encoding schemes from ideal lattices. Cryptology ePrint Archive, Report 2014/928, 2014. https://eprint.iacr.org/2014/928.

[3] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. *IACR Cryptology ePrint Archive*, 2002:80, 2002.

[4] Ales Drapal. Komutativni okruhy. http://www.karlin.mff.cuni.cz/~zemlicka/-11-12/komalg.pdf. Online; accessed 6.7.2018.

[5] Andreas Enge. Bilinear pairings on elliptic curves. *L'Enseignement Mathématique*, 61(2):211–243, 2015.

[6] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. Cryptology ePrint Archive, Report 2012/610, 2012. https://eprint.iacr.org/2012/610.

[7] David Stanovsky. Gaussova veta. http://www.karlin.mff.cuni.cz/~stanovsk/-vyuka/archiv/1213algebra/algebra_gauss.pdf. Online; accessed 5.7.2018.

[8] Jiri Tuma. Konecna telesa. http://www.karlin.mff.cuni.cz/~barto/student/-SkriptaKonTelPuvodni.pdf. Online; accessed 5.7.2018.