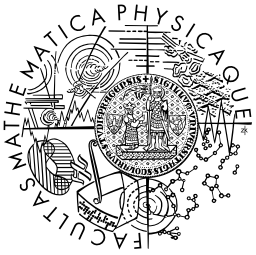

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

František Havránek

Multilineární zobrazení nad celými čísly

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 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 Praze dne 19. července 2018 František Havránek

Děkuji doc. Mgr. et Mgr. Janu Žemličkovi, Ph.D. za věcné připomínky, vstřícnost, ochotu a trpělivost při vedení této práce.

Název práce: Multilineární zobrazení nad celými čísly

Autor: František Havránek

Katedra: Katedra algebry

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

Abstrakt: Cílem práce je popsat schéma [CLT15], které je založené na Diffie-Hellmanovu schématu a využívá multilineární zobrazení nad celými čísly. Toto schéma umožňuje dohodu společného šifrovacího klíče mezi několika účastníky. Schéma úrovně κ (využívající κ-lineární zobrazení) umožňuje dohodu mezi $\kappa + 1$ účastníky. Práce zavádí základní pojmy, popisuje potřebnou teorii, jejímž základem je Čínská věta o zbytcích, a dále přípravu a použití schématu. Také je dokázána korektnost schématu a diskutovány související požadavky na základní parametry.

Klíčová slova: multilineární zobrazení, zobrazení nad celými čísly, dohoda na klíči, Diffie-Hellman, Čínská věta o zbytcích

Title: Multilinear Maps Over the Integers

Author: František Havránek

Department: Department of Algebra

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

Abstract: The thesis aims to describe the [CLT15] scheme, which is based on the Diffie-Hellman scheme and uses multilinear maps over integers. This scheme enables an exchange of a key among several participants. The level κ scheme (using a κ-linear map) enables the exchange of a key among $\kappa + 1$ participants. The thesis introduces the basic terms, describes the needed theory, the base of which is the Chinese Remainder Theorem, and also the preparation and usage of the scheme. The correctness of the scheme is proved as well and the related requirements on the basic parameters are discussed.

Keywords: multilinear map, map over integers, key exchange, Diffie-Hellman, Chinese Remainder Theorem

Obsah

Úvod

Komunikace je jedním ze základních kamenů našeho života. Komunikujeme se svým okolím prakticky neustále, přestože si to kolikrát ani neuvědomujeme. Často nám ale záleží na tom, aby se informace, kterou posíláme, dostala pouze k tomu, komu je určena. Při osobním setkání to není problém. Co když ale potřebujeme komunikovat na dálku? A navíc máme k dispozici pouze nezabezpečený komunikační kanál. V takovém případě nám nezbývá, než zprávy šifrovat.

V našem případě navíc potřebujeme, aby komunikace probíhala mezi více účasníky současně. To znamená, že když některý z účastníků zveřejní šifrovanou zprávu, nejen že nikdo jiný ji není schopen rozluštit, ale zároveň ji vždy může každý z účastníků úspěšně dešifrovat. K takovému účelu ovšem potřebujeme společný šifrovací klíč.

S možností, jak dohodnout bezpečný klíč během nezabezpečené komunikace, přišli v roce 2013 Jean-Sébastien Coron, Tancrède Lepoint a Mehdi Tibouchi. Rozhodli se k tomuto účelu využít multilineární zobrazení nad celými čísly, jejichž možné využití v kryptografii se v současné době teprve zkoumá. Své schéma zveřejnili v [CLT13].

Netrvalo ovšem dlouho a v roce 2015 Jung Hee Cheon společně s dalšími spolupracovníky dokázal bezpečnost schématu prolomit. Použitý útok byl zveřejněn v [CHL$^+$15].

Ještě v roce 2015 ale také J.-S. Coron, T. Lepoint a M. Tibouchi zveřejnili schéma [CLT15], ve kterém upravují původní schéma, aby zvýšili jeho bezpečnost a zabránili útoku [CHL$^+$15] v jeho prolomení.

Cílem této práce je popsat výsledné schéma [CLT15], jeho přípravu, kterou provádí nezávislá autorita, a způsob, jakým následně účastníci schéma používají. Přestože autorita může všechny parametry připravit a zveřejnit současně před použitím schématu, je jejich popis pro přehlednost rozložen do jednotlivých kapitol a parametry jsou uváděny až v kapitolách, ve kterých se používají.

Každý účastník si nejprve připraví svůj soukromý a veřejný klíč pro průběh Diffie-Hellmanova schématu. Veřejný klíč musí pro zajištění bezpečnosti před odesláním projít znáhodněním a následnou redukcí, aby mohl být odeslán v základním tvaru. Po výměně klíčů počítá každý z účastníků finální kódové slovo, které otestuje, zda se nejedná o slovo nulové zprávy a následně může extrahovat klíč. K tomu všemu slouží předem připravené parametry generované nezávislou autoritou.

V první kapitole jsou popsány základní pojmy a teorie, která nám umožňuje provádět další výpočty, dále způsob, jakým si účastníci připravují své klíče pro průběh Diffie-Hellmanova schématu. Druhá kapitola popisuje způsob, jakým účastníci v průběhu výpočtů redukují rostoucí délku šifrované zprávy. Ve třetí kapitole najdeme, jak mají účastníci před odesláním znáhodnit svůj veřejný klíč pro Diffie-Hellmanovo schéma, a čtvrtá kapitola ukazuje, jak po zveřejnění všech veřejných klíčů jednotlivých účastníků získat společný klíč.

Práce je zaměřena hlavně na zpřehlednění základního popisu schématu a podrobný důkaz jeho funkčnosti.

1. Příprava schématu

Základními parametry pro přípravu jsou úroveň schématu κ, která je určena počtem účastníků, a bezpečnostní parametr λ, který klade nároky na velikost všech dalších parametrů, které se v rámci schématu objeví, čímž cílí na zajištění jeho dostatečné bezpečnosti.

Připomeneme zde Čínskou větu o zbytcích a další známá algebraická tvrzení z [BS11], která budeme při výpočtech používat. Zavedeme základní pojmy pro popis schématu jako prostor zpráv nebo kód úrovně k a pojmy potřebné pro důkaz funkčnosti schématu jako třeba náhodný šum, délka šumu kódu, či velikost šumu kódového slova. Dále popíšeme, jak může nezávislá autorita kódová slova počítat a jakým způsobem s nimi mohou účastníci pracovat. V závěru kapitoly ještě ukážeme, jak tvoří účastníci soukromé a veřejné klíče pro Diffie-Hellmanovu dohodu na společném klíči.

1.1 Základní pojmy

Věta 1.1 (Čínská věta o zbytcích)**.** Nechť $p_1, \ldots, p_k \in \mathbb{N}$ jsou po dvou nesoudělná, $N = p_1 \cdot \ldots \cdot p_k$ a $z_1, \ldots, z_k \in \mathbb{Z}$. Pak existuje právě jedno $x \in \{0, \ldots, N-1\}$, pro které platí: $x \equiv z_i \pmod{p_i}$ pro každé $i \in \{1, 2, \ldots, k\}$.

V celém schématu budeme větu aplikovat na pevně zvolenou posloupnost prvočísel $p_1, \ldots, p_n$, která budou po dvou různá a tedy nesoudělná.

Poznámka. Jestliže p je prvočíslo, pak všechny aritmetické operace vyskytující se v kongruencích modulo p budeme provádět v $\mathbb{Z}_p$, tj. budeme uvažovat kongruentní hodnotu ze Z_p. Ostatní operace budou prováděny nad $\mathbb{Z}$, nebude-li uvedeno jinak. Dále pro $a, b \in \mathbb{Z}_p$ budeme používat značení $\frac{a}{b} \bmod p = a \cdot b^{-1} \bmod p$, tedy také $\frac{a}{b} \equiv a \cdot b^{-1} \pmod{p}$, a budeme nazývat čitatelem a b jmenovatelem.

Při práci s vektory budeme využívat konvenci označování složek stejnými písmeny, tedy např. $\vec{m} = (m_i)$, $\vec{r} = (r_i)$.

Definice 1.2 (bitová délka)**.** *Bitovou délku* (počet bitů) čísla $x \in \mathbb{Z}$ definujeme jako

$$\ell_2(x) = \lfloor \log_2 |x| \rfloor + 1.$$

V konstruovaném systému předpokládáme, že veškeré parametry jsou připraveny nezávislou autritou. Ta nejprve generuje řadu n po dvou různých prvočísel $g_1, \ldots, g_n$ jednotné bitové délky α a také po dvou různých prvočísel $p_1, \ldots, p_n$ jednotné bitové délky η. Budeme vyžadovat, aby délka η byla výrazně větší než délka α, přesnější požadavky budou stanoveny později. Dále nezávislá autorita položí $x_0 = \prod_{i=1}^{n} p_i$ a vygeneruje prvek $z \in \mathbb{Z}_{x_0}^*$. Všimněme si, že z je invertibilní modulo p_i pro všechna $i \in \{1, 2, \ldots, n\}$.

Tyto parametry budou nyní pevné pro celý průběh použití schématu a parametry $g_1, \ldots, g_n$, $p_1, \ldots, p_n$, x_0, z zůstávají tajné.

Definice 1.3 (prostor zpráv)**.** *Prostorem zpráv* budeme rozumět okruh na množině $R = \mathbb{Z}_{g_1} \times \ldots \times \mathbb{Z}_{g_n}$ s operacemi po složkách, tedy pro $\vec{m}, \vec{n} \in R$ a $1 \leq i \leq n$:

- $(\vec{m} + \vec{n})_i = m_i + n_i \bmod g_i$,

- $(\vec{m} \cdot \vec{n})_i = m_i \cdot n_i \bmod g_i$,
- $(-\vec{m})_i = -m_i \bmod g_i$.

Jednotkovou zprávou budeme rozumět n-tici $(1, \ldots, 1) \in R$ (tj. neutrální prvek vůči násobení) a *nulovou zprávou* budeme rozumět n-tici $(0, \ldots, 0) \in R$ (tj. neutrální prvek vůči sčítání).

Definice 1.4 (kód úrovně k)**.** Nechť $R = \prod_{i=1}^{n} \mathbb{Z}_{g_i}$ je prostor zpráv a $p_1, \ldots, p_n$, x_0, z jsou parametry schématu popsané výše. Nechť $k \in \mathbb{Z}$, $k \geq 0$, $\rho \in \mathbb{N}$. *Kódem úrovně k* zprávy $\vec{m} \in R$ nazveme množinu

$$C_\rho^k(\vec{m}) = \left\{ c \in \mathbb{Z} \;\middle|\; c \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i};\ r_i \in \mathbb{Z}, -2^\rho < r_i < 2^\rho;\ 1 \leq i \leq n \right\}.$$

Každý prvek $c_k \in C_\rho^k(\vec{m})$ pak nazveme *kódovým slovem* (úrovně k zprávy $\vec{m}$); jestliže navíc $c_k \in \mathbb{Z}_{x_0}$, nazveme c_k kódovým slovem *v základním tvaru*.

Vektoru $\vec{r}$ kódového slova budeme říkat náhodný *šum* a parametru ρ kódu budeme říkat *délka šumu* kódu.

Vidíme, že délka šumu kódu odpovídá maximální bitové délce, které může dosáhnout šum jednotlivých kódových slov daného kódu.

Pro celý chod schématu jsou pro délku šumu pevně určeny 2 význačné hodnoty. *Základní délka šumu* ρ_0 udává hodnotu používanou při výpočtu kódových slov nezávislou autoritou, zatímco *maximální délka šumu* ρ_f stanovuje hranici, kterou délka šumu kódu nesmí přesáhnout při průběžných výpočtech v rámci chodu schématu. Délka šumu kódových slov se tak v průběhu schématu může pohybovat v rozmezí $\rho \in [\rho_0, \rho_f]$.

Funkčnost schématu vyžaduje, aby bylo každé kódové slovo c jednoznačně spjato se zprávu, které odpovídá. Proto jestliže pro každé $i \in \{1, 2, \ldots, n\}$ platí $c \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i}$ a $m_i < g_i$, pak potřebujeme dostat

$$|r_i \cdot g_i + m_i| < \frac{p_i}{2}.$$

Jelikož pro $\rho \in [\rho_0, \rho_f]$ máme $r_i \in (2^{-\rho}, 2^\rho)$, nemůžeme dostat $0 \leq r_i g_i + m_i < p_i$. Můžeme odhadnout

$$|r_i \cdot g_i + m_i| < (2^{\rho_f} + 1) \cdot g_i < \frac{p_i}{2},$$

k tomu máme $g_i < 2^\alpha$, $2^{\eta-1} < p_i$. Dohromady nám tedy stačí $2^\alpha < \frac{2^{\eta-1}}{2^{\rho_f+2}}$, takže náš požadavek splníme podmínkou:

$$\alpha < \eta - \rho_f - 3.$$

Definice 1.5 (velikost šumu kódového slova)**.** Nechť $k \in \mathbb{Z}$, $0 \leq k \leq \kappa$. Nechť c_k je kódové slovo úrovně k zprávy $\vec{m}$, takže $c_k \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i}$ pro všechna $i \in \{1, 2, \ldots, n\}$. Velikost šumu označíme

$$\rho(c_k) = \max_{i \in \{1,2,\ldots,n\}} |r_i|.$$

Jelikož při použití je vždy zřejmé, s jakou zprávou $\vec{m}$ pracujeme, nebudeme ji explicitně značit.

Jako velikost šumu kódového slova budeme uvažovat skutečnou velikost této hodnoty, nikoli pouze její bitovou délku, jako je tomu u délky šumu kódu, abychom mohli v důkazech přehledně pracovat s přesnějšími hodnotami. Také to znamená, že

$$C_\rho^k(\vec{m}) = \left\{ c \in \mathbb{Z} \;\middle|\; c \text{ je kódové slovo úrovně } k \text{ zprávy } \vec{m}, \rho(c) < 2^\rho \right\}.$$

Nyní popíšeme, jakým způsobem lze počítat kódová slova. Vzhledem k tomu, že potřebné parametry jsou tajné, je nezávislá autorita jediným, kdo může kódová slova počítat.

Nejprve připomeneme dobře známá algebraická tvrzení z [BS11], která budeme využívat.

Tvrzení 1.6 (Eukleides)**.** Nechť n, p jsou nesoudělná přirozená čísla. Potom $\exists! t \in \mathbb{Z}_p$, pro které platí

$$t \cdot n \equiv 1 \pmod{p}.$$

Tvrzení 1.7 (Bézoutovy koeficienty)**.** Nechť n, p jsou nesoudělná přirozená čísla, $t \in \mathbb{Z}_p$ a platí $t \cdot n \equiv 1 \pmod{p}$. Potom $\exists! u \in \mathbb{Z}$, pro které platí

$$t \cdot n + u \cdot p = 1,$$

a není-li $n = p = 1$, pak platí také $|t| \leq \frac{p}{2}$, $|u| \leq \frac{n}{2}$.

Tvrzení 1.8 (Lagrange)**.** Nechť $p_1, \ldots, p_n$ jsou po dvou různá prvočísla a nechť $u_1, \ldots, u_n \in \mathbb{Z}$. Pro každé $i \in \{1, \ldots, n\}$ položme

$$N_i = \frac{\prod_{j=1}^n p_j}{p_i},$$

a jelikož N_i a p_i jsou nesoudělná, díky 1.6 najdeme $t_i \in \mathbb{N}$ splňující $t_i \cdot N_i \equiv 1 \pmod{p_i}$. Potom

$$\sum_{i=1}^n t_i N_i \cdot u_i \equiv u_i \pmod{p_i}$$

pro každé $i \in \{1, \ldots, n\}$.

Tvrzení 1.8 lze pro $u_i = \frac{r_i \cdot g_i + m_i}{z^k} \mod p_i$ použít k výpočtu kódových slov nezávislou autoritou. Jelikož výpočty budou probíhat pro různé zprávy $\vec{m} \in R$ a různé šumy $\vec{r}$ a všechny ostatní parametry zůstávají pevné (pro každé nezáporné $k \leq \kappa$), můžeme výpočet dále optimalizovat, což zachycuje následující důsledek.

Důsledek 1.9 (výpočet kódu)**.** Nechť $p_1, \ldots, p_n$, $g_1, \ldots, g_n$ jsou po dvou různá prvočísla a nechť $m_i \in \mathbb{Z}_{g_i}$ pro každé $i \in \{1, \ldots, n\}$. Položme $x_0 = \prod_{i=1}^n p_i$ a uvažujme $z \in \mathbb{Z}_{x_0}^*$, $0 \leq k \leq \kappa$ a celá čísla $r_1, \ldots, r_n \in (-2^{\rho_0}, 2^{\rho_0})$.

Pro každé $i \in \{1, \ldots, n\}$ položme $N_i = \frac{x_0}{p_i}$, a jelikož N_i, p_i a z jsou vzájemně nesoudělná čísla, najdeme $t_i' \in \mathbb{N}$ splňující $t_i' \cdot z^k N_i \equiv 1 \pmod{p_i}$. Potom

$$\sum_{i=1}^n t_i' N_i \cdot (r_i \cdot g_i + m_i) \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i}$$

pro všechna $i \in \{1, \ldots, n\}$.

Důkaz:

Z nesoudělnosti čísel N_i, p_i a z pro každé $i \in \{1, 2, \ldots, n\}$ získáváme t_i a t_i', že $t_i \cdot N_i \equiv 1 \pmod{p_i}$ a $t_i' \cdot z^k N_i \equiv 1 \pmod{p_i}$. Odtud dostáváme

$$t_i \cdot N_i \equiv t_i' \cdot z^k N_i \pmod{p_i}.$$

A pokud navíc pro každé $i \in \{1, 2, \ldots, n\}$ položíme $u_i = \frac{r_i \cdot g_i + m_i}{z^k} \mod p_i$, pak z předchozího tvrzení dostáváme

$$\begin{aligned} \sum_{i=1}^{n} t_i N_i \cdot \frac{r_i \cdot g_i + m_i}{z^k} &\equiv \frac{r_i \cdot g_i + m_i}{z^k} && \pmod{p_i} \\ \equiv \sum_{i=1}^{n} t_i' z^k N_i \cdot \frac{r_i \cdot g_i + m_i}{z^k} &\equiv \sum_{i=1}^{n} t_i' N_i \cdot (r_i \cdot g_i + m_i) && \pmod{p_i}. \end{aligned}$$

□

Jelikož nezávislá autorita má k dispozici hodnotu x_0, může navíc snadno převést kódová slova do základního tvaru.

1.2 Operace s kódy

Jelikož schéma vychází z Diffie-Hellmanova protokolu, je potřeba ukázat, že účastníci mohou provádět aritmertické operace (sčítání, odčítání, násobení) mezi kódovými slovy a získat tak opět platné kódové slovo. Operace mezi kódovými slovy budeme používat v dalších výpočtech. V článcích [CLT13] a [CLT15] se o operacích mluví velmi stručně, zde popíšeme jednotlivé operace podrobně.

Sečtením dvou kódových slov stejné úrovně dostaneme kódové slovo součtu zpráv odpovídající úrovně, pouze s šumem vyšší bitové délky.

Tvrzení 1.10 (sčítání kódů)**.** Nechť $\vec{m}, \vec{n} \in R$; $\rho_1 \geq \rho_2 > 0$, $k \geq 0$, pak

$$C^k_{\rho_1}(\vec{m}) + C^k_{\rho_2}(\vec{n}) \subset C^k_{\rho_1+1}(\vec{m} + \vec{n})$$

Důkaz:

Zvolme $c_1 \in C^k_{\rho_1}(\vec{m})$ a $c_2 \in C^k_{\rho_2}(\vec{n})$. Pak pro každé $i \in \{1, 2, \ldots, n\}$ platí, že $c_1 \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i}$ a $c_2 \equiv \frac{s_i \cdot g_i + n_i}{z^k} \pmod{p_i}$ pro nějaká celá čísla $r_i \in (-2^{\rho_1}, 2^{\rho_1})$, $s_i \in (-2^{\rho_2}, 2^{\rho_2})$.

$$c_1 + c_2 \equiv \frac{r_i \cdot g_i + m_i}{z^k} + \frac{s_i \cdot g_i + n_i}{z^k} \equiv \frac{r_i g_i + s_i g_i + m_i + n_i}{z^k} \pmod{p_i}$$

Sčítání zpráv provádíme v prostoru zpráv R. Když $\vec{m} + \vec{n}$ po složkách vydělíme se zbytkem hodnotami g_i, tj. napíšeme ve tvaru $m_i + n_i = a_i \cdot g_i + b_i$; $a_i, b_i \in \mathbb{Z}$, $0 \leq b_i < g_i$, vidíme, že $b_i = m_i + n_i$ v $\mathbb{Z}_{g_i}$ a $a_i \in \{0, 1\}$. Takže pokud položíme $t_i = r_i + s_i + a_i$, dostáváme

$$\frac{r_i g_i + s_i g_i + m_i + n_i}{z^k} \equiv \frac{r_i g_i + s_i g_i + a_i g_i + b_i}{z^k} \equiv \frac{(r_i + s_i + a_i) \cdot g_i + b_i}{z^k} \equiv \frac{t_i \cdot g_i + b_i}{z^k} \pmod{p_i}$$

pro každé $i \in \{1, 2, \ldots, n\}$.

Jelikož pro všechna $i \in \{1, 2, \ldots, n\}$ platí $|r_i| < 2^{\rho_1}$, $|s_i| < 2^{\rho_1}$ a $|a_i| \leq 1$, platí také $|r_i + s_i + a_i| < 2 \cdot 2^{\rho_1}$, a tedy $c_1 + c_2 \in C^k_{\rho_1+1}(\vec{m} + \vec{n})$. □

Opačné kódové slovo je kódovým slovem opačné zprávy stejné úrovně. Odečtením dvou kódových slov stejné úrovně tedy dostaneme kódové slovo rozdílu zpráv odpovídající úrovně, pouze s šumem vyšší bitové délky.

Tvrzení 1.11 (opačný kód)**.** Nechť $\vec{m} \in R$; $\rho > 0$, $k \geq 0$, pak

$$-C_\rho^k(\vec{m}) = C_\rho^k(-\vec{m})$$

Důkaz:

Zvolme $c \in C^k(\vec{m})$. Pro každé $i \in \{1, 2, \ldots, n\}$ platí pro nějaké $r_i \in \mathbb{Z}$:

$$c \equiv \tfrac{r_i \cdot g_i + m_i}{z^k} \iff -c \equiv -\tfrac{r_i \cdot g_i + m_i}{z^k} \equiv \tfrac{-r_i \cdot g_i - m_i}{z^k} \equiv \tfrac{(-r_i) \cdot g_i + (-m_i)}{z^k} \pmod{p_i}$$

Tedy $c \in C_\rho^k(\vec{m})$ právě tehdy, když $-c \in C_\rho^k(-\vec{m})$. □

Vynásobením dvou kódových slov dostaneme kódové slovo součinu zpráv úrovně odpovídající součtu původních úrovní, pouze s šumem vyšší bitové délky.

Tvrzení 1.12 (násobení kódů)**.** Nechť $\vec{m}, \vec{n} \in R$; $\rho_1 \geq \rho_2 \geq 2$, $k, l \geq 0$, $\alpha = \ell_2(g_i)$; $i \in \{1, 2, \ldots, n\}$, pak

$$C_{\rho_1}^k(\vec{m}) \cdot C_{\rho_2}^l(\vec{n}) \subset C_{\rho_1+\rho_2+\alpha+1}^{k+l}(\vec{m} \cdot \vec{n})$$

a pro libovolné $c_1 \in C_{\rho_1}^k(\vec{m})$ a $c_2 \in C_{\rho_2}^l(\vec{n})$ platí

$$\rho(c_1 \cdot c_2) < 2^{\rho_1+\rho_2+\alpha} + 2^{\rho_1+\alpha+2}.$$

Důkaz:

Zvolme $c_1 \in C_{\rho_1}^k(\vec{m})$ a $c_2 \in C_{\rho_2}^l(\vec{n})$. Pak pro každé $i \in \{1, 2, \ldots, n\}$ platí, že $c_1 \equiv \tfrac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i}$ a $c_2 \equiv \tfrac{s_i \cdot g_i + n_i}{z^l} \pmod{p_i}$ pro nějaká celá čísla $r_i \in (-2^{\rho_1}, 2^{\rho_1})$, $s_i \in (-2^{\rho_2}, 2^{\rho_2})$.

$$\begin{aligned} c_1 \cdot c_2 &\equiv \tfrac{r_i \cdot g_i + m_i}{z^k} \cdot \tfrac{s_i \cdot g_i + n_i}{z^l} && \pmod{p_i} \\ &\equiv \tfrac{r_i s_i g_i^2 + m_i s_i g_i + n_i r_i g_i + m_i n_i}{z^{k+l}} && \pmod{p_i} \\ &\equiv \tfrac{(r_i s_i g_i + m_i s_i + n_i r_i) \cdot g_i + m_i n_i}{z^{k+l}} && \pmod{p_i} \end{aligned}$$

Násobení provádíme v prostoru zpráv R po složkách, tedy $(\vec{m} \cdot \vec{n})_i = m_i \cdot n_i$. Když $\vec{m} \cdot \vec{n}$ po složkách vydělíme se zbytkem hodnotami g_i, tj. napíšeme ve tvaru $m_i \cdot n_i = a_i \cdot g_i + b_i$; $a_i, b_i \in \mathbb{Z}$, $0 \leq b_i < g_i$, vidíme, že $b_i = m_i \cdot n_i$ v $\mathbb{Z}_{g_i}$ a $a_i = \left\lfloor \tfrac{m_i \cdot n_i}{g_i} \right\rfloor$. Takže pokud položíme $t_i = r_i s_i g_i + m_i s_i + n_i r_i + a_i$, dostáváme

$$\tfrac{(r_i s_i g_i + m_i s_i + n_i r_i) \cdot g_i + m_i n_i}{z^{k+l}} \equiv \tfrac{(r_i s_i g_i + m_i s_i + n_i r_i + a_i) \cdot g_i + b_i}{z^{k+l}} \equiv \tfrac{t_i \cdot g_i + b_i}{z^{k+l}} \pmod{p_i}$$

pro každé $i \in \{1, 2, \ldots, n\}$.

Jelikož pro všechna $i \in \{1, 2, \ldots, n\}$ platí $|r_i| < 2^{\rho_1}$, $|s_i| < 2^{\rho_2} \leq 2^{\rho_1}$, dále $|a_i| < \left\lfloor \tfrac{g_i \cdot g_i}{g_i} \right\rfloor \leq g_i < 2^\alpha$, platí i $|r_i s_i g_i| < 2^{\rho_1+\rho_2+\alpha}$, $|m_i s_i| < 2^{\alpha+\rho_2}$, $|n_i r_i| < 2^{\alpha+\rho_1}$.

$$\begin{aligned} & |n_i r_i + m_i s_i| && < 2^{\rho_1+\alpha} + 2^{\rho_2+\alpha} \leq 2^{\rho_1+\alpha+1} \\ \implies \quad & |n_i r_i + m_i s_i + a_i| && < 2^{\rho_1+\alpha+1} + 2^\alpha < 2^{\rho_1+\alpha+2} \\ \implies \quad & |r_i s_i g_i + m_i s_i + n_i r_i + a_i| && < 2^{\rho_1+\rho_2+\alpha} + 2^{\rho_1+\alpha+2} \end{aligned}$$

A protože $2^{\rho_1+\rho_2+\alpha} + 2^{\rho_1+\alpha+2} \leq 2^{\rho_1+\rho_2+\alpha+1}$, platí také $c_1 \cdot c_2 \in C_{\rho_1+\rho_2+\alpha+1}^{k+l}(\vec{m} + \vec{n})$. □

Během výpočtů budeme chtít sčítat současně více kódových slov se stejnou velikostí šumu. Pro takový součet můžeme určit přesnější odhad výsledné velikosti šumu.

Tvrzení 1.13 (sčítání slov se stejnou velikostí šumu)**.** Nechť $c_k^{(1)}, c_k^{(2)}, \ldots, c_k^{(n)}$ jsou kódová slova stejné úrovně a $\rho\left(c_k^{(i)}\right) < 2^\rho$ pro každé $i \in \{1, 2, \ldots, n\}$. Pak

$$\rho\left(\sum_{j=1}^{n} c_k^{(j)}\right) < n \cdot 2^\rho.$$

Důkaz:

Pro každé $j \in \{1, \ldots, n\}$ platí $\rho\left(c_k^{(j)}\right) \leq 2^\rho - 1$. Podle tvrzení o sčítání kódových slov 1.10 získáme v každé složce $\sum_{j=1}^{n} c_k^{(j)}$ šum $\sum_{j=1}^{n} r_{j_i} + \sum_{j=1}^{n-1} a_j$, kde $\left|r_{j_i}\right| \leq 2^\rho - 1$, $j \in \{1, 2, \ldots, n\}$ a $a_j \in \{0, 1\}$, $j \in \{1, 2, \ldots, n-1\}$; pro každé $i \in \{1, 2, \ldots, n\}$. Odtud získáváme

$$\rho\left(\sum_{j=1}^{n} c_k^{(j)}\right) \leq \sum_{j=1}^{n} \left|r_{j_i}\right| + \sum_{j=1}^{n-1} a_j \leq n \cdot (2^\rho - 1) + (n-1) < n \cdot 2^\rho$$

pro každé $i \in \{1, 2, \ldots, n\}$. □

1.3 Soukromý klíč

Jako soukromé klíče pro dohodu na společném šifrovacím klíči slouží účastníkům kódová slova úrovně 0. Kvůli nedostatku veřejných parametrů nemohou tato kódová slova konstruovat sami, využívají k tomu nezávislou autoritou vytvořená kódová slova, ze kterých skládají svá vlastní.

Nezávislá autorita generuje parametr $\ell \in \mathbb{N}$, z bezpečnostních důvodů požadujeme $\ell \geq n \cdot \alpha + 2\lambda$ [CLT15, Lemma 1], a následně vytvoří ℓ různých náhodných zpráv $\vec{a_j} \in R$, $j \in M = \{1, \ldots, \ell\}$. Tyto zprávy zůstávají zcela tajné.

Dále nezávislá autorita ke každému z vektorů $\vec{a_j}$ vytvoří podle dusledku 1.9 kódové slovo x'_j úrovně 0, tedy $x'_j \in C^0_{\rho_0}(a_j)$, takže pro každé $i \in \{1, 2, \ldots, n\}$ platí

$$x'_j \equiv r_{j_i} \cdot g_i + a_{j_i} \pmod{p_i}.$$

Množinu takových kódových slov označíme $X_0 = \{x'_j; 1 \leq j \leq \ell\}$. Tu poskytne nezávislá autorita účastníkům.

Každý z účastníků si zvolí $M' \subset M$ a vytvoří své kódové slovo úrovně 0 jako

$$c_0 = \sum_{j \in M'} x'_j.$$

Kódové slovo c_0 si každý účastník ponechá a použije ho při dohodě jako svůj soukromý klíč.

Definice 1.14 (počáteční zpráva)**.** Výše popsané kódové slovo c_0 budeme dále označovat jako *soukromé kódové slovo* účastníka a *počáteční zprávou* účastníka nazveme takové $\vec{m} \in R$, pro které platí

$$c_0 \in C^0_{\rho_f}(\vec{m}).$$

Tvrzení 1.15. Pro soukromé kódové slovo c_0 zprávy $\vec{m}$ každého z účastníků platí:

$$c_0 \in C^0_{\lceil \log_2 \ell \rceil + \rho_0}(\vec{m}).$$

Důkaz:

Nechť $M' \subset \{1, \ldots, \ell\}$ a $c_0 = \sum_{j \in M'} x'_j$ je soukromé kódové slovo. Jelikož podle tvrzení 1.13 platí $\rho\left(\sum_{j=1}^{\ell} x'_j\right) < \ell \cdot 2^{\rho_0}$, zjevně také

$$\rho(c_0) < \ell \cdot 2^{\rho_0} \leq 2^{\lceil \log_2 \ell \rceil + \rho_0}.$$

□

Počáteční zpráva $\vec{m}$ odpovídající soukromému slovu účastníka c_0 je tedy lineární kombinací vektorů $\vec{a_j}$ a platí $\vec{m} = \sum_{j \in M'} a_j$. Vzhledem k tomu, že zprávy $\vec{a_j}$ jsou tajné, počáteční zprávy zůstávají utajeny i samotným účastníkům, kteří vytvářejí rovnou soukromá kódová slova, s nimiž dále pracují.

1.4 Veřejný klíč

Tato kapitola popisuje způsob, jakým mohou účastníci ze svého soukromého kódového slova úrovně 0 vytvořit kódové slovo úrovně 1, které slouží jako základ pro vytvoření veřejného klíče pro dohodu na společném šifrovacím klíči. Před zveřejněním je ještě třeba provést znáhodnění, to je popsáno v kapitole 3.

Nezávislá autorita pro průběh schématu připraví pevné kódové slovo úrovně 1 jednotkové zprávy. Budeme ho značit y. Nezávislá autorita ho opět spočte pomocí důsledku 1.9, takže $y \in C^1_{\rho_0}(1)$, takže pro každé $i \in \{1, 2, \ldots, n\}$ platí

$$y \equiv \frac{r_i \cdot g_i + 1}{z} \pmod{p_i}$$

Kódové slovo y nezávislá autorita poskytne účastníkům, kteří s jeho pomocí vytvoří ze svého soukromého kódového slova c_0 úrovně 0 kódové slovo c_1 úrovně 1:

$$c_1 = c_0 \cdot y$$

Tvrzení 1.16. Pro kódové slovo c_1 zprávy $\vec{m}$ každého z účastníků platí:

$$c_1 \in C^1_{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1}(\vec{m}).$$

Důkaz:

Z tvrzení 1.15 víme, že $\rho(c_0) < \ell \cdot 2^{\rho_0}$. Dále víme, že $\rho(y) < 2^{\rho_0}$. Podle tvrzení o násobení kódových slov 1.12 dostáváme

$$\rho(c_1) < 2^{2\rho_0 + \alpha} + 2^{\rho_0 + \alpha + 2} < \ell \cdot 2^{2\rho_0 + \alpha + 1} \leq 2^{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1}.$$

□

2. Redukce kódového slova

Horní mez kódování x_0 patří mezi tajné parametry. Účastníci schématu tedy nemohou k výpočtům použít okruh $\mathbb{Z}_{x_0}$ a mohou počítat pouze nad $\mathbb{Z}$. Pro správné fungování schématu je ale nutné, aby účastníci dokázali nalézt kódová slova v základním tvaru. K tomuto účelu slouží následující postup redukce bitové délky kódových slov za pomoci kódových slov nulové zprávy. Sečteme-li kódové slovo zprávy $\vec{m}$ s kódovým slovem nulové zprávy, výsledné kódové slovo zůstává v kódu zprávy $\vec{m}$.

V této kapitole popíšeme přípravy nutné pro průběh redukce, které provádí nezávislá autorita a podrobný průběh redukce prováděné účastníky. Zaměříme se na dopad na délku šumu redukovaného kódu, protože redukce se objevuje až v článku [CLT15], kde odhady délky šumu redukovaného kódu prostor nedostávají.

Tvrzení 2.1 (maximální bitová délka kódového slova)**.** Nechť c_0 je soukromé kódové slovo a $\gamma = \ell_2(x_0)$, pak

$$\ell_2(c_0 \cdot y) \leq 2\gamma + \lfloor log_2 \ell \rfloor$$

Důkaz:

Jelikož $M' \subset \{1, \ldots, \ell\}$ a $0 < x'_j < x_0 < 2^\gamma$ pro každé $1 \leq j \leq \ell$, platí

$$c_0 = \sum_{j \in M'} x'_j < \ell \cdot 2^\gamma.$$

Dále $0 < y < x_0 < 2^\gamma$, takže

$$c_0 \cdot y < \ell \cdot 2^{2\gamma},$$

a $\ell_2(\ell \cdot 2^{2\gamma}) = 2\gamma + \lfloor log_2 \ell \rfloor$. □

Nezávislá autorita nezveřejňuje kódová slova nulové zprávy úrovně 0, účastníci tedy mohou redukovat kódová slova až od úrovně 1. Z toho důvodu probíhá první redukce až po několika operacích. Jelikož při dalších výpočtech již máme možnost redukovat kódová slova po libovolné aritmetické operaci, můžeme předpokládat, že jejich bitová délka nikdy nepřesáhne $2\gamma + \lfloor log_2 \ell \rfloor$.

2.1 Příprava kódových slov nulové zprávy

Mějme $\gamma, \gamma' \in \mathbb{N}$, $\gamma = \ell_2(x_0)$, $\gamma' = 2\gamma + \lfloor \log_2 \ell \rfloor$. Nezávislá autorita vytvoří pro každou úroveň $i \in \{1, 2, \ldots, \kappa\}$ a každou bitovou délku $j \in \{\gamma, \gamma + 1, \ldots, \gamma'\}$ kód c_i^j úrovně i nulové zprávy tak, že bitová délka kódu je $\ell_2\left(c_i^j\right) = j$.

Tvrzení 2.2 (kódové slovo dané bitové délky)**.** Nechť $d_{i,j} \in C^i_{\rho_0}(0)$ je kódové slovo v základním tvaru, $q_{i,j} \in \left[\frac{2^{j-1}}{x_0}, \frac{2^j}{x_0}\right)$ je celé číslo. Nechť

$$c_i^j = d_{i,j} + q_{i,j} \cdot x_0,$$

pak $\ell_2\left(c_i^j\right) = j$.

Důkaz:

Jelikož $d_{i,j}$ je kódové slovo v základním tvaru, platí

$$0 \leq d_{i,j} < x_0.$$

Protože q_j je celé číslo, platí $q_{i,j} \leq \frac{2^j}{x_0} - 1$, takže můžeme napsat

$$\frac{2^{j-1}}{x_0} \cdot x_0 \leq q_{i,j} \cdot x_0 \leq \left(\frac{2^j}{x_0} - 1\right) \cdot x_0.$$

Dohromady dostáváme:

$$\begin{aligned} 0 + \tfrac{2^{j-1}}{x_0} \cdot x_0 &\leq d_{i,j} + q_{i,j} \cdot x_0 < x_0 + \left(\tfrac{2^j}{x_0} - 1\right) \cdot x_0 \\ \iff \qquad 2^{j-1} &\leq d_{i,j} + q_{i,j} \cdot x_0 < 2^j \end{aligned}$$

A jelikož $\ell_2(2^j) = j + 1$, vidíme, že $\ell_2(d_{i,j} + q_{i,j} \cdot x_0) = j$. □

Kódová slova $d_{i,j} \in C^i_{\rho_0}(0)$ je třeba vytvořit podle důsledku 1.9, celá čísla $q_{i,j} \in \left[\frac{2^{j-1}}{x_0}, \frac{2^j}{x_0}\right)$ lze volit libovolně. Takto pro každé $i \in \{1, 2, \ldots, \kappa\}$ a pro každé $j \in \{\gamma, \gamma + 1, \ldots, \gamma'\}$ lze spočítat $c^j_i \in C^i_{\rho_0}(0)$.

Nyní připravená kódová slova označíme $X^{(k)}_j = c^{j+\gamma}_k$ pro každé $k \in \{1, 2, \ldots, \kappa\}$ a $j \in \{0, 1, \ldots, \gamma' - \gamma\}$. Kódová slova $\left(X^{(k)}_j\right)_{j=0}^{\gamma'-\gamma}$ nulové zprávy, $k \in \{1, 2, \ldots, \kappa\}$, kde $\ell_2\left(X^{(k)}_j\right) = \ell_2(x_0) + j$, poskytne nezávislá autorita účastníkům.

2.2 Průběh redukce

Zde popíšeme algoritmus redukce, který účastníci provádí, když bitová délka kódového slova c_k dosáhne bitové délky γ, tedy hrozí, že $c_k \geq x_0$.

Mějme kódové slovo c_k úrovně $k \in \{1, \ldots, \kappa\}$, $\ell_2(c_k) \geq \ell_2(x_0)$. V prvním kroku najdeme kódové slovo $c^{(1)}_k$. Vybereme $X^{(k)}_j$ tak, že $j = \ell_2(c_k) - \ell_2(x_0)$. Potom $\ell_2(c_k) = \ell_2\left(X^{(k)}_j\right)$. Nyní spočítáme

$$c^{(1)}_k = \begin{cases} c_k - X^{(k)}_j, & c_k > 0; \\ c_k + X^{(k)}_j, & c_k < 0. \end{cases}$$

Tudíž $\ell_2\left(c^{(1)}_k\right) < \ell_2(c_k)$.

V dalším kroku najdeme stejným způsobem $c^{(2)}_k$, takže $\ell_2\left(c^{(2)}_k\right) < \ell_2\left(c^{(1)}_k\right)$. Tento postup opakujeme, dokud pro nějaké $i \in \mathbb{N}$ neplatí $\left|c^{(i)}_k\right| < X^{(k)}_0$. Jelikož v každém kroku se délka získaného kódového slova zmenší alespoň o 1, potřebujeme k tomu nejvýše $\gamma' - \gamma$ kroků. Nyní můžeme určit výsledné kódové slovo $c \in \mathbb{Z}_{x_0}$ jako

$$c = \begin{cases} c^{(i)}_k, & c^{(i)}_k \geq 0; \\ c^{(i)}_k + X^{(k)}_0, & c^{(i)}_k < 0. \end{cases}$$

Potom již platí $0 \leq c < X^{(k)}_0 < x_0$.

Při každé aritmetické operaci hrozí, že hodnota kódového slova přesáhne hodnotu x_0. Proto je třeba, aby redukce kódových slov probíhala pravidelně.

2.3 Délka šumu redukovaného kódu

V této části ukážeme, že nárůst velikosti šumu kódových slov vlivem redukce probíhající po násobení je zanedbatelný. Při násobení dvou kódových slov uvažujme výsledný kód z tvrzení 1.12, do něhož spadá výsledné kódové slovo. Takový odhad je pro nás postačující. Pokud následně provedeme redukci výsledného kódového slova, bude redukované kódové slovo stále spadat do kódu se stejnou délkou šumu. Z následujících tvrzení také vyplynou podmínky pro vztahy některých parametrů.

Tvrzení 2.3. Nechť $c \in C_\rho^k(\vec{m})$ je kódové slovo a $\hat{c}$ vznikne z c provedením redukce, pak

$$\rho(\hat{c}) < 2^\rho + 2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2}$$

Důkaz:

$\hat{c} = c + \sum_{j=0}^{\gamma + \lfloor \log_2 \ell \rfloor} a_j X_j^{(1)}$, kde $a_j \in \{-1, 0, 1\}$; $0 \leq j \leq \gamma + \lfloor \log_2 \ell \rfloor$. Za předpokladu, že $\log_2 \ell < \gamma$ z tvrzení 1.13 získáváme

$$\rho\left(\sum_{j=0}^{\gamma + \lfloor \log_2 \ell \rfloor} X_j^{(1)}\right) < (\gamma + \lfloor \log_2 \ell \rfloor + 1) \cdot 2^{\rho_0} < 2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2}.$$

□

Poznámka. Z předchozího tvrzení dostáváme podmínku

$$\log_2 \ell < \gamma.$$

Tvrzení 2.4. Nechť $c_k \in C_{\rho_1}^k(\vec{m})$, $c_l \in C_{\rho_2}^l(\vec{n})$; $k + l \leq \kappa$, $\rho_1 \geq \rho_2 > 3$, $\lfloor \log_2 \gamma \rfloor < \rho_1 + \rho_2 - \rho_0 + \alpha - 3$. Nechť $\hat{c}$ je kódové slovo vzniklé redukcí součinu $c_k \cdot c_l$. Pak

$$\hat{c} \in C_{\rho_1 + \rho_2 + \alpha + 1}^{k+l}(\vec{m} \cdot \vec{n})$$

Důkaz:

Podle tvrzení o násobení kódových slov 1.12 dostáváme odhad velikosti šumu $\rho(c_k \cdot c_l) < 2^{\rho_1 + \rho_2 + \alpha} + 2^{\rho_1 + \alpha + 2}$. Podle tvrzení 2.3 máme

$$\rho(\hat{c}) < 2^{\rho_1 + \rho_2 + \alpha} + 2^{\rho_1 + \alpha + 2} + 2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2}.$$

Z předpokladů získáváme platnost dvou nerovností:

$$2^{\rho_1 + \alpha + 2} < 2^{\rho_1 + \rho_2 + \alpha - 1},$$

$$2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2} < 2^{\rho_1 + \rho_2 + \alpha - 1}.$$

Z toho plyne

$$2^{\rho_1 + \alpha + 2} + 2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2} < 2^{\rho_1 + \rho_2 + \alpha}$$

a odtud dostáváme, že

$$2^{\rho_1 + \rho_2 + \alpha} + 2^{\rho_1 + \alpha + 2} + 2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2} < 2^{\rho_1 + \rho_2 + \alpha + 1}.$$

□

Vzhledem k tomu, že podle tvrzení 1.12 máme $c_k \cdot c_l \in C^{k+l}_{\rho_1+\rho_2+\alpha+1}(\vec{m} \cdot \vec{n})$, vidíme, že za daných podmínek redukce nezvyšuje délku šumu výsledného kódu. Každý účastník tedy může při násobení kódových slov ostatních účastníků provést redukci po každém vynásobení, čímž podle tvrzení 2.1, a protože součin dvou kódových slov v základním tvaru nepřevyšuje $2x_0 < 2^{2\gamma}$, udržuje kódová slova uvnitř $[0, \ell \cdot 2^{2\gamma})$, bez vlivu na délku šumu výsledného kódu.

Důsledek 2.5. Nechť c_0 je soukromé kódové slovo účastníka zprávy $\vec{m}$, $c_1 = c_0 \cdot y$ a $\hat{c_1}$ vznikne z c_1 provedením redukce, $\rho_0 > 3$, $\lfloor \log_2 \gamma \rfloor < \lceil \log_2 \ell \rceil + \rho_0 + \alpha - 3$, pak

$$\hat{c_1} \in C^1_{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1}(\vec{m}).$$

Důkaz:

Víme, že $\rho(c_0) < \ell \cdot 2^{\rho_0}$ a $\rho(y) < 2^{\rho_0}$. Pokud použijeme předchozí tvrzení pro $\rho_1 = \rho_0 + \lceil \log_2 \ell \rceil$ a $\rho_2 = \rho_0$, dostáváme

$$\rho(\hat{c_1}) < 2^{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1}.$$

□

Poznámka. Kódové slovo c_1 je prvním redukovaným slovem. Vzhledem k tomu, že v průběhu výpočtů délka šumu kódu neklesá, dostáváme zde omezení pro parametr γ:

$$\log_2 \gamma < \lceil \log_2 \ell \rceil + \rho_0 + \alpha - 2. \tag{2.1}$$

A protože $\gamma = \ell_2(x_0) = \ell_2(\prod_{i=1}^{n} p_i)$, což znamená, že $n \cdot \eta - n \leq \gamma \leq n \cdot \eta$, dostáváme podmínku

$$\eta < \frac{2^{\lceil \log_2 \ell \rceil + \rho_0 + \alpha - 2} + n}{n}.$$

Podmínku můžeme také napsat jako

$$\ell > n(\eta - 1) \cdot 2^{-\rho_0 - \alpha + 2}.$$

3. Znáhodnění kódového slova

Kvůli zajištění bezpečnosti potřebujeme, aby hodnoty posílané mezi účastníky neposkytovaly žádné další informace. Proto vyžadujeme, aby se volba těchto hodnot v rámci $\mathbb{Z}_{x_0}$ blížila co nejvíce rovnoměrnému rozdělení. K tomuto účelu slouží proces znáhodnění. Použijeme při něm opět kódová slova nulové zprávy, tentokrát úrovně 1.

Nejprve je třeba doplnit chybějící pojmy, následně podrobně popíšeme proces znáhodnění s důrazem na velikost šumu výsledných kódových slov a s odkazem na podrobnější části článků, které popisují algoritmus generování parametrů, či důkaz podobnosti pravděpodobnostních rozdělení, což přesahuje rozsah práce.

Definice 3.1 (diagonálně dominantní matice)**.** Nechť $A = (a_{i,j})$ typu $m \times n$ je matice nad $\mathbb{R}$. Řekneme, že A je *(neostře) diagonálně dominantní*, jestliže pro každé $i \in \{1, 2, \ldots, m\}$ platí

$$|a_{i,i}| \geq \sum_{\substack{j \in \{1,2,\ldots,n\}, \\ i \neq j}} |a_{i,j}| \,,$$

a *ostře diagonálně dominantní*, jestliže pro každé $i \in \{1, 2, \ldots, m\}$ platí

$$|a_{i,i}| > \sum_{\substack{j \in \{1,2,\ldots,n\}, \\ i \neq j}} |a_{i,j}| \,.$$

3.1 Příprava kódových slov nulové zprávy

V této části nezávislá autorita nejprve vygeneruje parametr $\tau \in \mathbb{N}$, z bezpečnostních důvodů požadujeme $\tau \geq (n+2) \cdot \rho_0 + 2\lambda$ [CLT15, Lemma 2], a připraví $n+1$ vektorů náhodných čísel $\overrightarrow{\varpi_j} \in \mathbb{Z}^{n+1}$ a ty poskládá do sloupců čtvercové matice $\Pi = (\varpi_{i,j})$ řádu $n+1$.

$$\varpi_{i,j} \in \begin{cases} (-2^{\rho_0}, 2^{\rho_0}) \,, & i \neq j \\ \big((n+1) \cdot 2^{\rho_0}, (n+2) \cdot 2^{\rho_0} \big), & i = j \end{cases}$$

Vidíme, že matice Π je ostře diagonálně dominantní.

Dále autorita pomocí matice Π připraví τ vektorů celých čísel $\overrightarrow{r_j} \in \mathbb{Z}^{n+1}$. Vektory jsou generované uvnitř polouzavřeného rovnoběžnostěnu určeného sloupcovými vektory matice Π a jsou voleny tak, aby jejich volba odpovídala rozvnoměrnému rozdělení. Konkrétní algoritmus je uveden v [CLT13, Appendix E]. Tyto vektory autorita poskládá do sloupců matice $X = (r_{i,j})$ typu $(n+1) \times \tau$.

Tvrzení 3.2. Pro takto generované prvky platí

$$|r_{i,j}| < (n+1) \cdot 2^{\rho_0 + 1}$$

pro každé $i \in \{1, \ldots, n+1\}$, $j \in \{1, \ldots, \tau\}$.

Důkaz:

Prvky jsou generovány uvnitř polouzavřeného rovnoběžnostěnu

$$P = \left\{ \sum_{j=1}^{n+1} k_j \vec{\varpi}_j \;\middle|\; k_j \in [0,1)\,; 1 \leq j \leq n+1 \right\}.$$

Můžeme tedy omezit každý prvek $\vec{v} \in P$:

$$|v_i| < \sum_{j=1}^{n+1} \left|\varpi_{j_i}\right| < n \cdot 2^{\rho_0} + (n+2) \cdot 2^{\rho_0} = (n+1) \cdot 2^{\rho_0+1}$$

□

Následně nezávislá autorita připraví dvě řady kódových slov, $(\Pi_j)_{j=1}^{n+1}$ a $(x_j)_{j=1}^{\tau}$, úrovně 1 nulové zprávy, které budou sloužit ke znáhodnění kódu. K tomu použije připravené matice náhodných čísel $\Pi = (\varpi_{ij})_{(n+1)\times(n+1)}$ a $X = (r_{ij})_{(n+1)\times\tau}$. Definujme $u_i = t_i' N_i, 1 \leq i \leq n$, podle důsledku 1.9, tedy $N_i = \frac{x_0}{p_i}$ a pro $t_i' \in \mathbb{N}$ platí $t_i' \cdot z^1 N_i \equiv 1 \pmod{p_i}$, protože hledáme kódová slova úrovně 1. Připravované řady kódových slov vypadají následovně:

$$\Pi_j = \sum_{i=1}^{n} \varpi_{i,j} \cdot g_i \cdot u_i + \varpi_{n+1,j} \cdot x_0, \quad j \in \{1, 2, \ldots, n+1\},$$
$$x_j = \sum_{i=1}^{n} r_{i,j} \cdot g_i \cdot u_i + r_{n+1,j} \cdot x_0, \qquad j \in \{1, 2, \ldots, \tau\},$$

kde podle důsledku 1.9

$$\sum_{i=1}^{n} \varpi_{i,j} \cdot g_i \cdot u_i, \quad j \in \{1, 2, \ldots, n+1\},$$
$$\sum_{i=1}^{n} r_{i,j} \cdot g_i \cdot u_i, \quad j \in \{1, 2, \ldots, \tau\}$$

jsou kódová slova úrovně 1 nulové zprávy. Tedy i po přičtení násobků x_0 jsou Π_j, $1 \leq j \leq n+1$, a x_j, $1 \leq j \leq \tau$, opět kódová slova úrovně 1 nulové zprávy.

3.2 Průběh znáhodnění

Pro samotné znáhodnění mějme redukované kódové slovo c_1 úrovně 1. K němu přičteme kombinaci kódových slov $(\Pi_j)_{j=1}^{n+1}$ a $(x_j)_{j=1}^{\tau}$ nulové zprávy:

$$c_1' = c_1 + \sum_{j \in M'} x_j + \sum_{j=1}^{n+1} b_j \Pi_j, \tag{3.1}$$

kde $M' \subset \{1, \ldots, \tau\}$ a $b_j \in \mathbb{N}$, $b_j < 2^{\rho_0+\alpha+\lambda}$, $1 \leq j \leq n+1$.

Coron, Lepoint a Tibouchi popisují rozdělení c_1' z rovnice 3.1 jako rozdělení, které téměř nezávisí na vstupu $\vec{m}$ [CLT15, Lemma 2], což znamená, že rozdělení c_1' je statisticky blízko rovnoměrnému rozdělení.

3.3 Velikost šumu po znáhodnění

Následující odhady nejsou v [CLT15] podrobně popsány, jsou však nutné k omezení maximální délky šumu.

Tvrzení 3.3. Nechť $c \in C_\rho^k(\vec{m})$ je kódové slovo a c' vznikne z c provedením znáhodnění, pak

$$\rho(c') < 2^\rho + \tau \cdot (n+1) \cdot 2^{\rho_0+1} + (n+1) \cdot (n+2) \cdot 2^{2\rho_0+\alpha+\lambda}.$$

Důkaz:

Nechť $M' \subset \{1, \ldots, \tau\}$ a $b_j \in \mathbb{N}$, $b_j < 2^{\rho_0+\alpha+\lambda}$, $1 \leq j \leq n+1$ [CLT15] a nechť $c' = c + \sum_{j \in M'} x_j + \sum_{j=1}^{n+1} b_j \Pi_j$ je kódové slovo po provedení znáhodnění. Víme, že $\rho(\Pi_j) < (n+2) \cdot 2^{\rho_0}$, a z tvrzení 3.2 také, že $\rho(x_j) < (n+1) \cdot 2^{\rho_0+1}$.

Podle tvrzení 1.13 dostáváme

$$\rho\left(\sum_{j=1}^{\tau} x_j\right) < \tau \cdot (n+1) \cdot 2^{\rho_0+1}.$$

Dále pro každé $j \in \{1, \ldots, n+1\}$ máme $\rho(b_j \Pi_j) < (n+2) \cdot 2^{2\rho_0+\alpha+\lambda}$, tedy opět podle tvrzení 1.13 dostáváme

$$\rho\left(\sum_{j=1}^{n+1} b_j \Pi_j\right) < (n+1) \cdot (n+2) \cdot 2^{2\rho_0+\alpha+\lambda}.$$

□

Znáhodnění je vždy prováděno na kódovém slově $c_1 \in C^1_{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1}$, takže pro kódové slovo c_1' vzniklé znáhodněním platí

$$\rho(c_1') < 2^{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1} + \tau \cdot (n+1) \cdot 2^{\rho_0+1} + (n+1) \cdot (n+2) \cdot 2^{2\rho_0+\alpha+\lambda}. \quad (3.2)$$

Tvrzení 3.4. Nechť $\hat{c}_1'$ je redukované kódové slovo c_1' vzniklé znáhodněním, $n \geq 4$, pak

$$\rho(\hat{c}_1') < 4n^2 2^{2\rho_0+\alpha+\lambda}.$$

Důkaz:

V tomto důkazu najdeme podmínky pro jednotlivé parametry, abychom mohli omezit velikost šumu výsledného kódového slova. Nejprve omezíme jednotlivé členy součtu na pravé straně nerovnice 3.2.

$$2^{\lceil \log_2 \ell \rceil + 2\rho_0 + \alpha + 1} \leq (\ell+1) \cdot 2^{2\rho_0+\alpha+1} \leq \frac{1}{2} n^2 2^{2\rho_0+\alpha+\lambda} \quad (3.3)$$

Odtud dostáváme podmínku pro ℓ:

$$\ell \leq n^2 2^{\lambda-2} - 1.$$

Z druhého členu získáme podmínku pro τ:

$$\begin{aligned} & \tau \cdot (n+1) \cdot 2^{\rho_0+1} && \leq n^2 2^{2\rho_0+\alpha+\lambda} \\ \iff \quad & \tau \cdot (n+1) && \leq n^2 2^{\rho_0+\alpha+\lambda-1} \\ \implies \quad & \tau && \leq n 2^{\rho_0+\alpha+\lambda-2} \end{aligned}$$

Jelikož uvažujeme $n \geq 4$, dostáváme

$$(n+1) \cdot (n+2) = n^2 + 3n + 2 < 2n^2.$$

Z tvrzení 2.3 dostáváme poslední člen, který popisuje nárůst velikosti šumu vlivem redukce. Ten můžeme omezit díky nerovnici 2.1:

$$2^{\rho_0 + \lfloor \log_2 \gamma \rfloor + 2} < 2^{2\rho_0 + \lceil \log_2 \ell \rceil + \alpha}$$

Nyní můžeme použít první odhad z nerovnice 3.3. Dohromady už dostáváme, že

$$\rho\left(\hat{c}_1'\right) < 4n^2 2^{2\rho_0 + \alpha + \lambda}.$$

□

Poznámka. Z podmínek pro generování parametrů a z předchozího tvrzení dostáváme dohromady podmínky pro parametry ℓ a τ:

$$n \cdot \alpha + 2\lambda \leq \ell \leq n^2 2^{\lambda - 2} - 1$$
$$(n+2) \cdot \rho_0 + 2\lambda \leq \tau \leq n 2^{\rho_0 + \alpha + \lambda - 2}.$$

Další podmínkou je

$$n \geq 4.$$

4. Finální kód

Finální kódové slovo slouží k získání společného klíče, nesmí se ovšem jednat o kódové slovo nulové zprávy. V této kapitole si ukážeme, jakým způsobem účastník získá finální kódové slovo, jak ověří, zda se nejedná o kódové slovo nulové zprávy, a jakým způsobem z něj extrahuje sdílené tajemství.

V této kapitole získáme rozhodující omezení pro maximální délku šumu kódu. Popíšeme jaké parametry musí ještě nezávislá autorita vygenerovat pro testování finálního kódu. Dále následuje podrobný klíčový důkaz, který ukazuje, za jakých podmínek celé schéma funguje. V závěru kapitoly je návod, jak mají účastníci s finálním kódem naložit.

Definice 4.1 (finální kód)**.** Nechť $\overrightarrow{m_i}$, $0 \leq i \leq \kappa$, jsou počáteční zprávy jednotlivých účastníků, $\rho_f \in \mathbb{N}$. Pak *finálním kódem* nazveme kód

$$C^{\kappa}_{\rho_f}\left(\prod_{i=0}^{\kappa} \overrightarrow{m_i}\right).$$

4.1 Výpočet finálního kódového slova

Uvažujme účastníka a jeho vlastní soukromé kódové slovo c_0 a veřejná kódová slova $c_1^1, c_1^2, \ldots, c_1^\kappa$ úrovně 1 ostatních účastníků. Těmto kódovým slovům odpovídají počáteční zprávy $\overrightarrow{m_0}, \overrightarrow{m_1}, \ldots, \overrightarrow{m_\kappa} \in R$. Nyní lze spočítat finální kódové slovo

$$c_\kappa = c_0 \cdot \prod_{i=1}^{\kappa} c_1^i.$$

V průběhu výpočtu je třeba, aby účastník znovu provedl redukci po vynásobení každým kódovým slovem, dostáváme tedy finální kódové slovo v základním tvaru.

Tvrzení 4.2 (maximální délka šumu)**.** Nechť c_κ je finální kódové slovo zprávy $\vec{m}$, $\alpha \geq \kappa$, pak

$$c_\kappa \in C^{\kappa}_{(2\rho_0+2\alpha+\lambda+2\log_2 n+3)\cdot\kappa+\rho_0+\log_2 \ell+1}\left(\vec{m}\right),$$

tedy $\rho_f = (2\rho_0 + 2\alpha + \lambda + 2\log_2 n + 3) \cdot \kappa + \rho_0 + \log_2 \ell + 1$

Důkaz:

Z tvrzení 3.4 víme, že $\rho\left(c_1^i\right) < 4n^2 2^{2\rho_0+\alpha+\lambda}$ pro každé $i \in \{1, \ldots, \kappa\}$. Dále z tvrzení 1.15 víme, že $\rho\left(c_0\right) < 2^{\lceil \log_2 \ell \rceil + \rho_0}$ a z tvrzení 2.4, že při redukci mezi násobením se délka šumu nemění. Podle tvrzení o násobení kódových slov 1.12 dostáváme:

$$\begin{aligned}\log_2 \rho\left(c_0 \cdot \prod_{i=1}^{\kappa} c_1^i\right) &< (2 + 2\log_2 n + 2\rho_0 + \alpha + \lambda) \cdot \kappa + \lceil \log_2 \ell \rceil + \rho_0 + \kappa \cdot (\alpha + 1) \\ &< (2\rho_0 + 2\alpha + \lambda + 2\log_2 n + 3) \cdot \kappa + \rho_0 + \log_2 \ell + 1\end{aligned}$$

□

4.2 Parametry pro testování

Parametry generované nezávislou autoritou popsané v této sekci s odkazem na algoritmy v [CLT15] jsou zapotřebí v následující sekci pro důkaz správnosti testování. Nejdůležitějším parametrem pro testování, který používají přímo i účastníci, je $\vec{\theta} \in \mathbb{Z}_N^n$, dále čísla N, β a ν. Parametry popsané v této sekci, které není třeba zveřejňovat účastníkům, ale jsou zapotřebí pro důkaz správnosti jsou matice H a čísla α_i, β_i, $i \in \{1, 2, \ldots, n\}$. Dále ještě zavedeme značení pro u'_i, v_i, $i \in \{1, 2, \ldots, n\}$.

Definice 4.3 (operátorová norma matice)**.** Mějme matici A typu $m \times n$ určující zobrazení z normovaného lineárního prostoru $(\mathbb{R}^n, ||\cdot||)$ do normovaného lineárního prostoru $(\mathbb{R}^m, ||\cdot||)$. Definujme *operátorovou normu matice*

$$||A|| = \sup\{||A\vec{x}|| : \vec{x} \in \mathbb{R}^n, ||\vec{x}|| \leq 1\}.$$

Poznámka (maximová norma)**.** V obou vektorových prostorech $\mathbb{R}^n$ i $\mathbb{R}^m$ budeme uvažovat maximovou normu $||\cdot||_\infty$. Pro $x \in \mathbb{R}^n$ máme

$$||x||_\infty = \max_{i \in \{1,2,\ldots,n\}} \{x_i\},$$

a vzhledem k tomu, že dle definice 4.3 uvažujeme jen vektory $x \in \mathbb{R}^n$, $||x||_\infty \leq 1$, tak $|x_i| \leq 1$ pro každé $i \in \{1, 2, \ldots, n\}$. Dále $Ax \in \mathbb{R}^m$ a tedy máme

$$||Ax||_\infty = \max_{j \in \{1,2,\ldots,m\}} \left\{ \sum_{i=1}^{n} a_{i,j} \cdot x_i \right\}.$$

Můžeme tedy použít horní mez pro $|x_i|$ a omezit tak i normu $||Ax||_\infty$, čímž získáváme $||Ax||_\infty \leq \max_{j \in \{1,2,\ldots,m\}} \{\sum_{i=1}^{n} |a_{i,j}|\}$. Nyní pro každé $j \in \{1, 2, \ldots, m\}$ můžeme snadno zvolit $\vec{x_j} \in \{1, -1\}^n$ tak, že $a_{i,j} \cdot x_{j_i} = |a_{i,j}|$ pro každé $i \in \{1, 2, \ldots, n\}$. Odtud už přímo plyne, že

$$||A||_\infty = \max_{j \in \{1,2,\ldots,m\}} \left\{ \sum_{i=1}^{n} |a_{i,j}| \right\}.$$

Pro testování nulovosti a následnou extrakci klíče nezávislá autorita generuje tyto parametry: prvočíslo N takové, aby platilo $\ell_2(N) = \gamma + 2\eta + 1$ [CLT15, Section 2.1], dále čísla $\beta = 3\lambda$ [CLT15, Section 4.3] a $\nu = \eta - \rho_f - \lambda - \beta - 3$ [CLT15, Lemma 3]. Všechny tyto parametry jsou veřejné.

Zbývajícím veřejným parametrem je vektor $\vec{\theta} \in \mathbb{Z}^n$. Způsobem, jakým ho nezávislá autorita vytváří se budeme zabývat nyní. Další parametry použité při jeho přípravě zůstávají tajné.

Prvním takovým parametrem ja matice $H = (h_{i,j}) \in \mathbb{Z}^{n \times n}$. Po této matici požadujeme, aby byla invertibilní nad $\mathbb{Z}$ a splňovala $\left|\left|H^T\right|\right|_\infty \leq 2^\beta$ a zároveň $\left|\left|\left(H^{-1}\right)^T\right|\right|_\infty \leq 2^\beta$. Konkrétní algoritmus, jak vygenerovat vhodnou matici, je uveden v [CLT15, Appendix C].

Pro další potřebné parametry obdobně jako v důsledku 1.9 uvažujme $N_i = \frac{x_0}{p_i}$ a $t'_i \cdot z^\kappa N_i \equiv 1 \pmod{p_i}$. Dále položme $\bar{t_i} \equiv g_i \cdot t'_i \pmod{p_i}$ a $u'_i = \bar{t_i} \cdot N_i$. Z důsledku 1.9 vyplývá, že pro kódové slovo c_κ, kde pro každé $i \in \{1, 2, \ldots, n\}$ platí

$c_\kappa \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i}$, platí pro každé $i \in \{1, 2, \ldots, n\}$ také

$$c_\kappa \equiv \sum_{i=1}^{n} u'_i \cdot \left(r_i + m_i \cdot {g_i}^{-1}\right) \pmod{p_i}.$$

Pokud tedy označíme $v_i \equiv r_i + m_i \cdot {g_i}^{-1} \mod p_i$, můžeme napsat

$$c_\kappa = \sum_{i=1}^{n} u'_i \cdot v_i - a \cdot x_0,$$

pro nějaké $a \in \mathbb{Z}$. Hledanými parametry pak jsou (α_i, β_i); $i \in \{1, 2, \ldots, n\}$, splňující

$$\begin{aligned} |\alpha_i| &< 2^{\eta-1}, \\ |\beta_i| &< 2^{2-\eta} \cdot N, \\ \beta_i &\equiv \alpha_i \cdot \frac{u'_i}{p_i} \pmod{N}, \end{aligned}$$

postup vytvoření takových čísel je popsán v [CLT15].

Označme $\bar{p_i} \equiv p_i^{-1} \pmod{N}$. S výše popsanými parametry může autorita vygenerovat vektor $\vec{\theta}$ tak, aby pro každé $j \in \{1, \ldots, n\}$ platilo

$$\theta_j = \sum_{i=1}^{n} h_{i,j} \cdot \alpha_i \cdot \bar{p_i} \bmod N.$$

4.3 Správnost testování

Důkaz provedený v této části je využit v následujících sekcích pro testování nulovosti a následné umožnění extrakce klíče. V následujícím důkazu budeme používat notaci a parametry z předchozí sekce.

Tvrzení 4.4. Nechť c_κ je finální kódové slovo v základním tvaru zprávy $\vec{m}$ a nechť $\vec{\omega} = c_\kappa \cdot \vec{\theta} \bmod N$. Pokud $\vec{m}$ je nulová zpráva, pak

$$||\vec{\omega}||_\infty < \frac{N}{2^{\nu+\lambda}},$$

pokud $\vec{m}$ není nulová zpráva, pak

$$||\vec{\omega}||_\infty > \frac{N}{2^{\nu-2}}.$$

Důkaz:

Slovo c_κ je v základním tvaru, tedy $0 \leq c_\kappa < x_0$. Současně platí $0 \leq u'_i < x_0$. Jelikož $v_i \in \mathbb{Z}_{p_i}$, můžeme odhadnout

$$c_\kappa = \sum_{i=1}^{n} u'_i \cdot v_i - a \cdot x_0 < \sum_{i=1}^{n} x_0 \cdot p_i - a \cdot x_0 < n \cdot x_0 \cdot 2^\eta - a \cdot x_0,$$

a odtud dostáváme

$$a < n \cdot 2^\eta - \frac{c_\kappa}{x_0} \leq n \cdot 2^\eta.$$

Dále položme vektory $\vec{s}$ a $\vec{t}$ tak, aby pro každé $i \in \{1, 2, \ldots, n\}$ platilo

$$\begin{aligned} s_i &= v_i \cdot \beta_i \bmod N, \\ t_i &= \alpha_i \cdot \sum_{\substack{k=1,\\ k\neq i}}^{n} \left(v_k \cdot \frac{u'_k}{p_i} \right) - a \cdot \alpha_i \cdot N_i. \end{aligned}$$

Protože pro každé $j \in \{1, 2, \ldots, n\}$ máme

$$\begin{aligned} \omega_j &= c_\kappa \cdot \theta_j \bmod N \\ &= \left(\sum_{k=1}^{n} (u'_k \cdot v_k) - a \cdot x_0 \right) \cdot \left(\sum_{i=1}^{n} h_{i,j} \cdot \alpha_i \cdot \bar{p_i} \right) \bmod N \\ &= \sum_{i=1}^{n} h_{i,j} \cdot \left(\sum_{k=1}^{n} \left(\alpha_i \cdot v_k \cdot \frac{u'_k}{p_i} \right) - a \cdot \alpha_i \cdot \frac{x_0}{p_i} \right) \bmod N \\ &= \sum_{i=1}^{n} h_{i,j} \cdot \left(\alpha_i \cdot v_i \cdot \frac{u'_i}{p_i} + \sum_{\substack{k=1,\\ k\neq i}}^{n} \left(\alpha_i \cdot v_k \cdot \frac{u'_k}{p_i} \right) - a \cdot \alpha_i \cdot \frac{x_0}{p_i} \right) \bmod N \\ &= \sum_{i=1}^{n} h_{i,j} \cdot \left(v_i \cdot \beta_i + \alpha_i \cdot \sum_{\substack{k=1,\\ k\neq i}}^{n} \left(v_k \cdot \frac{u'_k}{p_i} \right) - a \cdot \alpha_i \cdot N_i \right) \bmod N \\ &= \sum_{i=1}^{n} h_{i,j} \cdot (s_i + t_i) \bmod N, \end{aligned}$$

platí zde, že

$$\vec{\omega}^T = H^T \left(\vec{s} + \vec{t} \right)^T \bmod N.$$

Dále využíváme, že $N > 2^{\gamma+2\eta}$:

$$\begin{aligned} |t_i| &\leq |\alpha_i| \cdot \sum_{\substack{k=1,\\ k\neq i}}^{n} \left(p_k \cdot \frac{|u'_k|}{p_i} \right) + |\alpha_i| \cdot |a| \cdot \frac{x_0}{p_i} \\ &\leq 2^{\eta-1} \cdot (n-1)\, 2^{\eta} \frac{2^{\gamma}}{2^{\eta-1}} + 2^{\eta-1} \cdot n 2^{\eta} \cdot \frac{2^{\gamma}}{2^{\eta-1}} \\ &\leq (n-1)\, 2^{\eta+\gamma} + n 2^{\eta+\gamma} < 2n 2^{\eta+\gamma} = \frac{n \cdot 2^{\gamma+2\eta}}{2^{\eta-1}} \\ &< \frac{n}{2^{\eta-1}} \cdot N, \end{aligned}$$

a tedy $\left|\left| \vec{t} \right|\right|_\infty < n 2^{-\eta+1} N$.

Nyní předpokládejme, že $\vec{m}$ je nulová zpráva. Pak pro každé $i \in \{1, 2, \ldots, n\}$ máme $|v_i| \leq |r_i|$ a tedy

$$|s_i| \leq |r_i| \cdot |\beta_i| < 2^{\rho_f - \eta + 2} N.$$

Dohromady dostáváme $\left|\left|\vec{t}+\vec{s}\right|\right|_\infty < 2^{\rho_f-\eta+3}N$. A protože $\nu = \eta-\rho_f-\lambda-\beta-3$, máme

$$\begin{aligned}||\vec{\omega}||_\infty &= \left|\left|H^T\left(\vec{s}+\vec{t}\right)^T \bmod N\right|\right|_\infty \\ &\leq \left|\left|H^T\left(\vec{s}+\vec{t}\right)^T\right|\right|_\infty \leq \left|\left|H^T\right|\right|_\infty \left|\left|\vec{s}+\vec{t}\right|\right|_\infty \\ &< 2^{\beta+\rho_f-\eta+3}N < 2^{-\nu-\lambda}N.\end{aligned}$$

Nyní nechť $\vec{m}$ není nulová zpráva a tedy $\exists i_0 \in \{1,2,\ldots,n\}$, že $m_{i_0} \neq 0$. Pro každé $i \in \{1,2,\ldots,n\}$ máme $\beta_i \equiv \alpha_i \cdot \frac{u_i'}{p_i} \pmod N$. Nejprve najdeme spodní odhad pro $|\beta_i|$. To provedeme sporem a stejný postup v průběhu důkazu ještě zopakujeme. Protože p_i, N jsou různá prvočísla a tedy čísla nesoudělná, můžeme napsat $\beta_i \cdot p_i \equiv \alpha_i \cdot u_i' \pmod N$. Víme, že:

$$|\alpha_i \cdot u_i'| \leq |\alpha_i| \cdot |u_i'| \leq 2^{\eta-1} \cdot |x_0| \leq 2^{\eta+\gamma-1} < \frac{N}{2}$$

Předpokládejme nyní, že také $|p_i| \cdot |\beta_i| < \frac{N}{2}$. Díky předchozím nerovnostem dostáváme z kongruence rovnost nad celými čísly:

$$\beta_i \cdot p_i = \alpha_i \cdot u_i'.$$

Potom platí $p_i | (\alpha_i \cdot u_i')$, zároveň ale $\alpha_i < p_i$ a $u_i' = \bar{t_i} \cdot N_i$, kde $\bar{t_i} < p_i$ a $N_i = \frac{x_0}{p_i}$ je s p_i nesoudělné. Jelikož p_i je prvočíslo, nemůže být dělitelem $(\alpha_i \cdot u_i')$ a dostáváme se ke sporu, čímž dostáváme, že $|p_i| \cdot |\beta_i| \geq \frac{N}{2}$ a tedy $|\beta_i| \geq \frac{N}{2|p_i|} > \frac{N}{2^{\eta+1}}$. To znamená, že

$$2^{-\eta-1} \cdot N < |\beta_i| < 2^{2-\eta} \cdot N.$$

Uvážíme $\bar{g_i} \in \left(-\frac{p_i}{2}, \frac{p_i}{2}\right]$, $\bar{g_i} \equiv g_i^{-1} \pmod{p_i}$. Nechť $f_i = \bar{g_i} \cdot \beta_i \bmod N$. To znamená, že

$$f_i = \frac{\bar{g_i} \cdot \alpha_i \cdot u_i'}{p_i} \bmod N,$$

a obdobně jako v předchozím případě najdeme spodní odhad pro $|f_i|$. Víme, že

$$|\bar{g_i} \cdot \alpha_i \cdot u_i'| < 2^\eta \cdot 2^{\eta-1} \cdot |x_0| \leq 2^{2\eta+\gamma-1} \leq \frac{N}{2},$$

A stejně jako p_i je nesoudělné s $\alpha_i \cdot u_i'$, tak protože $\bar{g_i} < p_i$, je p_i nesoudělné i s $\bar{g_i} \cdot \alpha_i \cdot u_i'$. Zbytek argumentace je totožný jako jsme použili výše. Odtud dostáváme, že

$$|f_i| \geq \frac{N}{2\,|p_i|} > \frac{N}{2^{\eta+1}}.$$

Platí $g_i \cdot \bar{g_i} \equiv 1 \pmod{p_i}$, a tedy existuje celé číslo μ, že $g_i\bar{g_i} = 1 + \mu p_i$. Protože p_i a g_i jsou nesoudělná, podle tvrzení 1.7 platí $|\mu| \leq \frac{g_i}{2}$, a protože $2 \nmid g_i$, platí

$$|\mu| < \frac{g_i}{2}.$$

Dále můžeme rozepsat:

$$f_i = \frac{g_i\bar{g_i} \cdot \beta_i}{g_i} \bmod N = \frac{(1+\mu p_i) \cdot \beta_i}{g_i} \bmod N = \frac{\beta_i + \mu\alpha_i u_i'}{g_i} \bmod N.$$

Nyní ukážeme, že čitatel a jmenovatel posledního výrazu jsou nesoudělné. Předpokládejme, že $g_i \mid (\beta_i + \mu\alpha_i u_i')$. Potom

$$|f_i| \leq \left|\frac{\beta_i + \mu\alpha_i u_i'}{g_i}\right| < \frac{2^{2-\eta}\cdot N}{g_i} + \frac{\frac{g_i}{2}2^{\gamma+\eta-1}}{g_i} \leq 2^{3-\eta-\alpha}\cdot N + 2^{\gamma+\eta-2}$$

a s využitím $N > 2^{\gamma+2\eta}$ dostáváme pro $\alpha \geq 5$:

$$|f_i| < 2^{3-\eta-\alpha}\cdot N + 2^{-\eta-2}\cdot N \leq \left(2^{3-\eta-\alpha} + 2^{-\eta-2}\right)\cdot N \leq 2^{-\eta-1}\cdot N.$$

Jelikož ale víme, že $|f_i| > 2^{-\eta-1}\cdot N$, jsou prvočíslo g_i a $(\beta_i + \mu\alpha_i u_i')$ nesoudělné. Dále jsou g_i a N různá prvočísla, a tedy opět čísla nesouděná, a jelikož $\eta > \alpha$:

$$|\beta_i + \mu\alpha_i u_i'| < 2^{2-\eta}\cdot N + 2^{\alpha-1+\eta-1+\gamma} < \left(2^{2-\eta} + 2^{\alpha-\eta-2}\right)\cdot N < \frac{N}{2}.$$

Obdobně jako v předchozích případech dostáváme $|f_i| \geq \frac{N}{2|g_i|} > \frac{N}{2^{\alpha+1}}$.

Máme $m_{i_0} \neq 0$, a protože g_{i_0} je prvočíslo, najdeme $\overline{m}_{i_0} \in \left(-\frac{g_{i_0}}{2}, \frac{g_{i_0}}{2}\right]$ tak, že $\overline{m}_{i_0} \equiv m_{i_0}^{-1} \pmod{g_{i_0}}$. Platí $m_{i_0}\cdot\overline{m}_{i_0} \equiv 1 \pmod{g_{i_0}}$, a tedy existuje celé číslo μ', že $m_{i_0}\cdot\overline{m}_{i_0} = 1 + \mu' g_{i_0}$. Z tvrzení 1.7 dostaneme, že

$$|\mu'| \leq \frac{m_{i_0}}{2} < \frac{g_{i_0}}{2}.$$

Protože $s_{i_0} = v_{i_0}\cdot\beta_{i_0} \bmod N$, $v_{i_0} \equiv m_{i_0}\cdot {g_{i_0}}^{-1} + r_{i_0} \bmod p_{i_0}$ a $f_{i_0} = \overline{g}_{i_0}\cdot\beta_{i_0} \bmod N$, kde $\overline{g}_{i_0} \equiv g_{i_0}^{-1} \pmod{p_{i_0}}$, dostáváme dohromady:

$$s_{i_0} = m_{i_0} f_{i_0} + r_{i_0}\beta_{i_0} \bmod N.$$

Jelikož $f_{i_0} = \frac{\beta_{i_0} + \mu\alpha_{i_0}u_{i_0}'}{g_{i_0}} \bmod N$, dostáváme

$$\begin{aligned}
\overline{m}_{i_0} s_{i_0} &\equiv \overline{m}_{i_0} m_{i_0} f_{i_0} + \overline{m}_{i_0} r_{i_0}\beta_{i_0} \\
&\equiv \left(1 + \mu' g_{i_0}\right) f_{i_0} + \overline{m}_{i_0} r_{i_0}\beta_{i_0} \\
&\equiv f_{i_0} + \mu' g_{i_0} f_{i_0} + \overline{m}_{i_0} r_{i_0}\beta_{i_0} \\
&\equiv f_{i_0} + \mu'\left(\beta_{i_0} + \mu\alpha_{i_0}u_{i_0}'\right) + \overline{m}_{i_0} r_{i_0}\beta_{i_0} \pmod N.
\end{aligned}$$

Odtud vyjádříme f_{i_0}:

$$\begin{aligned}
f_{i_0} &= \overline{m}_{i_0} s_{i_0} - \mu'\left(\beta_{i_0} + \mu\alpha_{i_0}u_{i_0}'\right) - \overline{m}_{i_0} r_{i_0}\beta_{i_0} \bmod N \\
&= \overline{m}_{i_0} s_{i_0} - \beta_{i_0}\left(\mu' + \overline{m}_{i_0} r_{i_0}\right) - \mu'\mu\alpha_{i_0}u_{i_0}' \bmod N
\end{aligned}$$

a shora odhadneme $|f_{i_0}|$ za pomoci $N > 2^{2\eta+\gamma}$, a protože $\rho_f > \alpha - 5$:

$$\begin{aligned}
|f_{i_0}| &< \frac{g_{i_0}}{2}\cdot|s_{i_0}| + 2^{2-\eta}N\left(\frac{g_{i_0}}{2} + \frac{g_{i_0}}{2}\cdot 2^{\rho_f}\right) + \frac{g_{i_0}}{2}\cdot\frac{g_{i_0}}{2}\cdot 2^{\eta-1}\cdot x_0 \\
&< 2^{\alpha-1}|s_{i_0}| + 2^{2-\eta}N\left(2^{\alpha-1} + 2^{\alpha-1+\rho_f}\right) + 2^{2(\alpha-1)+\eta-1+\gamma} \\
&< 2^{\alpha-1}|s_{i_0}| + 2^{2-\eta}N\left(2^{\alpha+\rho_f}\right) + 2^{2\alpha+\eta+\gamma-3} \\
&< 2^{\alpha}\left(|s_{i_0}| + N2^{\rho_f-\eta+2} + 2^{\alpha+\eta+\gamma-3}\right) \\
&< 2^{\alpha}\left(|s_{i_0}| + N2^{\rho_f-\eta+2} + N2^{\alpha-\eta-3}\right) \\
&< 2^{\alpha}\left(|s_{i_0}| + N2^{\rho_f-\eta+3}\right).
\end{aligned}$$

Dále odtud odhadneme zespodu $|s_{i_0}|$, přičemž využijeme, že $\rho_f \leq \eta - 2\alpha - 5$, čímž dostaneme, že $2^{\rho_f - \eta + 3} \leq 2^{-2\alpha-2}$, a jelikož $|f_{i_0}| > N2^{-\alpha-1}$, máme:

$$\begin{aligned} |s_{i_0}| &> |f_{i_0}|\, 2^{-\alpha} - N2^{\rho_f - \eta + 3} \\ &> N2^{-2\alpha-1} - N2^{-2\alpha-2} = N2^{-2\alpha-2}. \end{aligned}$$

Totéž platí pro každé $i \in \{1, 2, \ldots, n\}$, pro které $m_i \neq 0$, takže $||s||_\infty > 2^{-2\alpha-2}N$. A protože $||t||_\infty < n2^{-\eta+1}N$ a $\eta > 2\alpha + \log_2 n + 4$, máme také:

$$||t||_\infty < n2^{-(2\alpha+\log_2 n+4)+1}N \leq 2^{-2\alpha-3}N$$

Dohromady dostáváme

$$||s+t||_\infty \geq ||s||_\infty - ||t||_\infty > 2^{-2\alpha-2}N - 2^{-2\alpha-3}N \geq 2^{-2\alpha-3}N.$$

A protože $\vec{\omega}^T = H^T \left(\vec{s} + \vec{t}\right)^T \bmod N$, můžeme napsat

$$||s+t||_\infty = \left|\left|\left(H^T\right)^{-1} \vec{\omega}^T \bmod N\right|\right|_\infty \leq \left|\left|\left(H^T\right)^{-1} \vec{\omega}^T\right|\right|_\infty \leq \left|\left|\left(H^T\right)^{-1}\right|\right|_\infty \cdot ||\vec{\omega}||_\infty$$

a nakonec odhadnout

$$||\vec{\omega}||_\infty \geq \frac{||s+t||_\infty}{\left|\left|(H^T)^{-1}\right|\right|_\infty} > \frac{2^{-2\alpha-3}N}{2^\beta} \geq 2^{-2\alpha-\beta-3}N.$$

Máme $\nu = \eta - \rho_f - \lambda - \beta - 3$ a uvážíme $\eta \geq \rho_f + 2\alpha + 2\beta + \lambda + 8$. Pak dostáváme

$$\nu = \eta - \rho_f - \lambda - \beta - 3 \geq 2\alpha + \beta + 5,$$

odtud také

$$-\nu + 2 \leq -2\alpha - \beta - 3,$$

a tedy

$$||\vec{\omega}||_\infty > 2^{-\nu+2}N.$$

□

Poznámka. Z podmínek v důkazu dostáváme podmínku pro bitovou délku prvočísel p_i; $i \in \{1, 2, \ldots, n\}$:

$$\eta \geq \rho_f + 2\alpha + 2\beta + \lambda + 8$$

Další podmínka plyne pro bitovou délku prvočísel g_i; $i \in \{1, 2, \ldots, n\}$:

$$\alpha \geq 5.$$

Poznámka. Protože $\frac{N}{2^{\nu-2}} > \frac{N}{2^{\nu+\lambda}}$, z tvrzení 4.4 plynou přímo ekvivalence, tedy $\vec{m}$ je nulová zpráva právě, když $||\vec{\omega}||_\infty < \frac{N}{2^{\nu+\lambda}}$, a $\vec{m}$ není nulová zpráva právě, když $||\vec{\omega}||_\infty > \frac{N}{2^{\nu-2}}$.

Pokud by totiž platilo $||\vec{\omega}||_\infty < \frac{N}{2^{\nu+\lambda}}$ a zároveň, že $\vec{m}$ není nulová zpráva, tak ovšem musí také platit, že $||\vec{\omega}||_\infty > \frac{N}{2^{\nu-2}}$. Obdobně platí i pro druhou ekvivalenci.

4.4 Testování nulovosti

S využitím znalosti z předchozí sekce nyní můžeme provést relativně jednoduchý test nulovosti finálního kódového slova.

Mějme finální kódové slovo c v základním tvaru. Dále použijeme veřejné parametry $\vec{\theta}$, N a ν. Spočítáme $\vec{\omega} \in \mathbb{Z}_N^n$ tak, aby

$$\omega_i = c \cdot \theta_i \bmod N$$

pro každé $i \in \{1, 2, \ldots, n\}$. Pokud platí

$$||\vec{\omega}||_\infty < \frac{N}{2^\nu},$$

pak z tvrzení 4.4 vyplývá, že c je kódovým slovem nulové zprávy, tedy $c \in C_{\rho_f}^{\kappa}(0)$.

Pokud se ukáže, že finální kódové slovo je kódovým slovem nulové zprávy, je třeba, aby účastníci provedli celý proces znovu a každý si při tvorbě svého soukromého kódového slova úrovně 0 zvolil jinak svoji množinu $M' \subset M$.

4.5 Extrakce klíče

Pokud finální kódové slovo není kódovým slovem nulové zprávy, může účastník extrahovat společný klíč.

Mějme finální kódové slovo c nenulové zprávy $\vec{m} \in R$ v základním tvaru. K němu určíme $\vec{\omega} \in \mathbb{Z}_N^n$ podle předchozího oddílu a zkonstruujeme $\vec{\omega}' \in \mathbb{Z}_{2^\nu}^n$ tak, aby pro každé $i \in \{1, 2, \ldots, n\}$ platilo

$$\omega_i' = \left\lfloor \frac{\omega_i}{2^{\nu'}} \right\rfloor,$$

kde $\nu' = \ell_2(N) - \nu$. To znamená, že nás zajímá ν nejvyšších bitů každé složky $\vec{\omega}$.

Z tvrzení 4.4 vyplývá, že vektor $\vec{\omega}'$ závisí pouze na zprávě $\vec{m}$ a je nenulový právě tehdy, když je nenulová i zpráva $\vec{m}$.

Definice 4.5 (extrakt)**.** Výše popsaný vektor $\vec{\omega}'$ nazveme *extraktem* finálního kódového slova c.

Tvrzení 4.6. Nechť c_1 je finální kódové slovo zprávy $\vec{m_1}$ a c_2 je finální kódové slovo zprávy $\vec{m_2}$, vektor $\vec{\omega}_1'$ je extrakt kódového slova c_1 a vektor $\vec{\omega}_2'$ je extrakt kódového slova c_2. Potom platí:

$$\vec{m_1} \neq \vec{m_2} \iff \vec{\omega}_1' \neq \vec{\omega}_2'$$

Důkaz:

$\vec{m_1} \neq \vec{m_2}$, to znamená, že $\vec{m_1} - \vec{m_2} \neq (0, \ldots, 0)$. Podle tvrzení 4.4 je ekvivalentní, že

$$(c_1 - c_2) \cdot \vec{\theta} \bmod N > \frac{N}{2^{\nu-2}},$$

To znamená, že extrakt kódového slova $(c_1 - c_2)$ je nenulový. A protože

$$(c_1 - c_2) \cdot \vec{\theta} \equiv c_1 \cdot \vec{\theta} - c_2 \cdot \vec{\theta} \pmod N,$$

také vektor $\vec{\omega}_1' - \vec{\omega}_2'$ je nenulový, a tedy $\vec{\omega}_1' \neq \vec{\omega}_2'$. □

Výše popsaným způsobem tedy každý účastník získá extrakt $\vec{\omega}'$ jednoznačně určený zprávou $\vec{m}$. Tento extrakt je hledaným sdíleným tajemstvím a může být použit k vytvoření společného klíče.

Závěr

Cílem práce bylo popsat schéma, na které článek [CLT15] upravuje původní schéma z [CLT13], a to pokud možno lineárně a srozumitelně, jelikož původní články jsou s ohledem na komplexnost schématu psány poměrně chaoticky. Mimo to jsou v mnoha ohledech velmi stručné, ať už se jedná o popis použití schématu nebo o důkazy, převážně odhadů, takže úkolem této práce bylo rozepsat podrobně základní principy a taktéž podrobně ukázat funkčnost schématu.

Výrazně jsem oproti původním článkům rozšířil značení a terminologii, čímž jsem se snažil docílit zvýšení přehlednosti celého popisu a umožnit korektní důkazy tvrzení, která v původních článcích nejsou dokazována. Dále jsem se zaměřil na odhady změn velikosti náhodného šumu při jednotlivých operacích, jelikož se jedná o důležitý prvek základu funkčnosti schématu a ve zdrojových článcích se obvykle pracuje až s konečnými výsledky.

Bylo by zajímavé provést kryptoanalýzu, případně se zaměřit také na konkrétní útoky. Zajímavým útokem je bezesporu [CHL+15], který prolomil původní schéma a je také popsán společně s analýzou v [CLT15]. Další útoky, proti kterým jsou schémata bezpečná, jsou, společně s kryptoanalýzou, uvedeny v obou článcích, [CLT13] i [CLT15]. Na kryptoanalýzu ani popis útoků bohužel nezbyl prostor, podobně jako na některé algoritmy generování parametrů, na které práce pouze odkazuje.

Seznam použité literatury

[BS11] L. Barto and D. Stanovský. *Počítačová algebra*. MatfyzPress, Praha, 2011.

[CHL+15] J.H. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehlé. Cryptanalysis of the multilinear map over the integers. *In: Advances in Cryptology – EUROCRYPT 2015, LNCS*, vol. 9056:3–12, 2015.

[CLT13] J.-S. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. *In: Advances in Cryptology - CRYPTO 2013, Part I. LNCS*, vol. 8042:476–493, 2013.

[CLT15] J.-S. Coron, T. Lepoint, and M. Tibouchi. New multilinear maps over the integers. *In: Advances in Cryptology - CRYPTO 2015, LNCS*, vol. 9215:267–286, 2015.