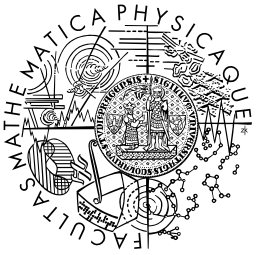

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Karolína Kučerová

Využití invertibilních prvků mřížky v ověření s nulovou znalostí

Katedra algebry

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

Studijní program: Obecná matematika

Studijní obor: MOMP

Praha 2021/2022

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

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

Chtěla bych velice poděkovat vedoucímu své bakalářské práce, doc. Mgr. et Mgr. Janu Žemličkovi, Ph.D., za jeho čas a ochotu provázet mne při tvorbě této bakalářské práce a omluvit se mu za všechny zmatky, které mne provází. Zároveň bych chtěla poděkovat své sestře Andy a kamarádce Lucii za neutuchající morální podporu a schopnost mne uklidnit v jakékoli situaci.

Název práce: Využití invertibilních prvků mřížky v ověření s nulovou znalostí

Autor: Karolína Kučerová

Katedra: Katedra algebry

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

Abstrakt: Práce se zaměřuje na popis kryptografického protokolu, který se řadí do skupiny ověřitelného šifrování, přesněji jde o metodu ověření s nulovou znalostí. Ověřitelné šifrování nám dovoluje dokázat vlastnosti určitého textu. Pokud je šifrovací schéma je bezpečné, nemělo by při důkazu dojít k prozrazení obsahu textu. Hlavním cílem metody je ověření znalosti soukromého klíče. Metodu lze využít k vytváření skupinových podpisů, předávání informací ve více krocích, nebo například k uschovávání klíčů. Je založena na složitosti okruhového-LWE šifrování v kombinaci s hledáním řešení soustav lineárních rovnic a využívá principu *rejection sampling*. Zkoumaná metoda spojuje principy dvou blíže popsaných kryptografických metod a to okruhového LWE a metody. Využívá konstrukci faktorokruhů $R = \mathbb{Z}[x]/(x^n + 1)$ a $R_q = \mathbb{Z}_q[x]/(x^n + 1)$.

Klíčová slova: mřížka ověření kryptografie okruh invertibilita

Title: Application of invertible elements in a zero-knowledge proof

Author: Karolína Kučerová

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., department of algebra

Abstract: This work is focused on the description of one verifiable encryption scheme, specifically a zero-knowledge proof of knowledge protocol. Verifiable encryption allows us to prove properties of data without revealing its content. The main goal of the presented method is verification of knowledge of a secret key. This method can be used for group signatures, multiple steps secret sharing, key escrow protocols, and many others cryptographic protocols. It is based on the hardness of the Ring-LWE problem and problems of finding solutions to linear relations over some ring. It uses the principle of rejection sampling. The method is build on two closely described cryptographic protocols, Ring-LWE and Fiat-Shamir with aborts. It uses the construction of polynomial rings $R = \mathbb{Z}[x]/(x^n+1)$ a $R_q = \mathbb{Z}_q[x]/(x^n + 1)$.

Keywords: lattice verification kryptografie ring invertibility

Obsah

Úvod

Cílem této práce je popsat kryptografickou metodu založenou na složitosti okruhového LWE problému a řešení soustav lineárních rovnic nad polynomiálním okruhem a dokázat její korektnost. Tato metoda se řadí do skupiny metod nazvaných ověření s nulovou znalostí. Účastní se jí dvě strany, které nazveme dokazující a ověřovatel. Dokazující účastník se na základě nějaké zašifrované zprávy snaží ověřující straně dokázat znalost určitého textu, kterému říkáme soukromý klíč.

Výslednou metodu lze využít k vytváření skupinových podpisů ve společnosti důvěryhodné strany. Tato strana vlastní rozdílné klíče ostatních účastníků, kteří s nimi mohou anonymně podepisovat dokumenty. Ty potom může důvěryhodná strana zpětně dohledat. Dále lze pomocí této metody předávat důvěrné informace ve dvou krocích. Nejprve proběhne vzájemný důkaz vlastnictví soukromého klíče a následně může dojít k předání zašifrované zprávy. V neposlední řadě lze metodu využít v protokolech pro uschování klíčů. V takovém protokolu jsou klíče potřebné k dešifrování potřebných dat uschovány tak, že je v určité situaci může autorizovaná třetí strana získat.

Pro prezentovanou konstrukci jsme využili faktorokruhů polynomů podle monického polynomu $x^n + 1$ nad celými čísly a tělesy $\mathbf{Z}_q$ pro q prvočíslo. Přesněji okruhy $R = \mathbb{Z}[x]/(x^n+1)$ a $R_q = \mathbb{Z}_q[x]/(x^n+1)$. Základním stavebním kamenem metody bude práce s lineární relací $\mathbf{Bm} = \mathbf{u} \mod p$, kde matice $\mathbf{B}$ nad okruhem R_q a vektor $\mathbf{u}$ nad R_q jsou během protokolu pro všechny účastníky známé, a $\mathbf{m}$ je tajný vektor s malými koeficienty, který ověřovatel zašifruje. Majitel soukromého klíče dokazuje jeho znalost nalezením prvků $\bar{\mathbf{m}}$ a $\bar{c}$ vyhovujících rozšířené soustavy rovnic $\mathbf{B}\bar{\mathbf{m}} = \bar{c}\mathbf{u} \mod p$. Dvojic, které dokazující pomocí definovaného algoritmu může zkonstruovat je více. Dokážeme, že parametry, použité při vytváření okruhu R_q a generování klíčů, lze omezit tak, že pro každé dva výstupy dešifrovacího algoritmu $(\bar{\mathbf{m}},\bar{c})$ a $(\bar{\mathbf{m}}',\bar{c}')$ existují inverzní prvky k $\bar{c}$ a $\bar{c}'$ a je splněna vlastnost $\bar{\mathbf{m}}(\bar{c})^{-1} \equiv \bar{\mathbf{m}}'(\bar{c}')^{-1} \pmod p$.

Před samotnou konstrukcí protokolu představíme dvě jednodušší kryptografické systémy, na jejichž principy výsledná metoda navazuje. Těmi jsou okruhové LWE šifrování (Learning with errors) a podpisové schéma, které nazýváme přerušovaný Fiat-Shamir.

V okruhovém LWE šifrování ze soukromého klíče vytvoříme odpovídající klíč veřejný. Hlavní součástí metody je algoritmus, který pomocí vzniklého veřejného klíče zašifruje nějaký prvek R_q, který lze získat jednoduše zpět použitím soukromého klíče. Přerušovaný Fiat-Shamir již stejně jako výsledná metoda pracuje se soustavou lineárních rovnic nad okruhem R_q. Hlavní algoritmus dané metody zašifruje prvek s a jeho výstupem je dvojice prvků $(\mathbf{z},c) \in R_q^k \times R_q$. Jeho varianta je pak v metodě použita na zašifrování dané zprávy m. Fiat-Shamir je protokol ověření s nulovou znalostí, které v hlavním algoritmu používá přístup s názvem *rejection sampling*. Při jeho běhu proběhne nedeterministický algoritmus závislý na $\mathbf{z}$. Na základě jeho výsledku algoritmus buď vrátí hodnoty $(\mathbf{z},c)$, nebo proběhne celý znovu a vypočítá hodnoty nové. Pravděpodobnost, že určité $\mathbf{z}$ je v dvojici výsledných hodnot, je díky tomuto přístupu nezávislá na vstupní hodnotě s.

Výsledná metoda používá ověření s nulovou znalostí z metody Fiat-Shamir a veřejný klíč k zašifrování dat. Princip okruhového LWE je součástí dešifrování,

neboli důkazu znalosti soukromého klíče.

U všech algoritmů dokážeme jejich korektnost, tedy zda s daným vstupem skutečně vrací očekávané hodnoty. Ověření bezpečnosti není předmětem této práce.

1. Zavedení základních objektů

Na začátku této kapitoly zopakujeme potřebné definice. V druhé části budou následně zavedeny okruhy, které budeme v práci diskutovat.

1.1 Základní definice

Nejprve zavedeme několik objektů z algebry týkajících se okruhů.

Definice 1 (Okruh)**.** *Okruhem R rozumíme pětici $(R, +, -, \cdot, 0)$, kde R je neprázdná množina, na které jsou definovány binární operace $+$, $\cdot$, unární operace $-$ a prvek $0 \in R$, splňující pro každé $a, b, c \in R$ následující podmínky:*

$$a + (b + c) = (a + b) + c, \quad a + b = b + a, \quad a + 0 = a,$$

$$a + (-a) = 0,$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Okruh nazveme komutativní, pokud je komutativní také operace násobení, tj. $a \cdot b = b \cdot a$ pro všechna $a, b \in R$. Okruhem s jednotkou pak rozumíme okruh, ve kterém existuje prvek $1 \in R$ splňující $a \cdot 1 = 1 \cdot a = a$ pro každé $a \in R$.

Okruh R nazveme oborem, pokud pro každé dva nenulové prvky a,$b \in R$ platí $a \cdot b \neq 0$.

Řekneme, že R je těleso, pokud je to okruh s jednotkou a platí, že pro každé $0 \neq a \in R$ existuje $b \in R$ takové, že platí $a \cdot b = b \cdot a = 1$. Prvku b říkáme inverzní prvek k a a značíme ho a^{-1}.

Charakteristikou tělesa R myslíme nejmenší přirozené číslo p takové, že v R platí $\sum_{i=1}^{p} 1 = 0$. Pokud takové číslo neexistuje, řekneme, že R má charakteristiku 0.

Pokud bude z kontextu jasné, o které operace se jedná, budeme okruhem zvát jeho nosnou množinu R.

Definice 2. *Neinvertibilní prvek a oboru R nazveme ireducibilní, pokud pro každé b, c takové, že $a = bc$ platí, že buď b je invertibilní, nebo c je invertibilní.*

Definice 3. *Nechť R a T jsou okruhy. Zobrazení $\varphi : R \to T$ nazýváme okruhový homomorfismus, pokud $\forall a$,$b \in R$ platí vztahy $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(-a) = -\varphi(a)$ a $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.*

Pokud je zobrazení φ bijekce, nazýváme ho izomorfismus.

Definice 4. *Ideálem okruhu R nazveme podmnožinu $I \subset R$, která je uzavřená na sčítání v I a na násobení prvky množiny R. Tedy pro každé i,$j \in I, s \in R$ platí: $i + j \in I$ a $i \cdot s \in I$.*

Ideál nazveme hlavním, pokud existuje prvek $a \in I$ takový, že pro všechna $i \in I$ $\exists s \in R : i = a \cdot s$. Prvek a nazveme generátor ideálu a ideál potom můžeme značit $I = (a)$.

Následující skupina definic se zabírá vlastnostmi celých čísel a operací modulu v celých číslech a polynomech nad okruhem.

Definice 5. *Nechť R je okruh, a,$b \in R$. Říkáme, že prvek a dělí prvek b, pokud existuje $c \in R$ takové, že*

$$b = ac.$$

Tuto skutečnost značíme $a|b$.

V opačném případě řekneme, že prvek a nedělí prvek b. Značíme $a \not| b$.

Definice 6. *Nechť $a \in \mathbb{Z}$, q je liché prvočíslo. Operaci modulu q v této práci definujeme následujícím předpisem:*

$$a \mod q = b \iff q|(b-a) \wedge b \in \{-(q-1)/2, \ldots, (q-1)/2\}$$

Díky této formulaci platí, že všechna čísla mají alespoň tak velkou normu jako jejich modul.

Definice 7. *Pro přirozené číslo n je hodnota Eulerovy funkce definována předpisem $\varphi(n) = |\{m \in \{1,2,\ldots,n\} : NSD(m,n) = 1\}|$.*

Definice 8. *Nechť $p \in \mathbb{Z}$ je prvočíslo a $n \in \mathbb{N}$. Pak p-valuaci prvku n definujeme jako největší přirozené číslo k takové, že platí $p^k|n$.*

Značíme $v_p(n) = k$ a definujeme $v_p(0) = \infty$

Definice 9. *Říkáme, že dva prvky a,$b \in R$, kde R je okruh, jsou kongruentní modulo $q \in R$, pokud $q|(b-a)$.*

Značíme $a \equiv b \pmod{q}$

Definice 10. *Množina $\mathbb{Z}_q = \{-(q-1)/2, \ldots, (q-1)/2\}$ pro q liché s binárními operacemi sčítání a násobení modulo q a unární operací odečítání modulo q tvoří okruh.*

Pokud je p prvočíslo, je tento objekt zároveň tělesem.

Definice 11. *Polynomem proměnné x, nad okruhem R rozumíme výraz*

$$a = a_0 + a_1 x + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

kde $a_0, \ldots, a_n \in R$ a $a_n \neq 0$. Přirozené číslo n nazýváme stupněm polynomu. Prvkům $a_0, \ldots, a_n$ říkáme koeficienty polynomu. Prvek a_n se nazývá vedoucí koeficient, prvek a_0 absolutní člen. Pokud je vedoucí koeficient roven jednotce, říkáme, že je polynom monický. Stupeň nulového polynomu definujeme jako -1. Na množině polynomů zadefinujeme operace $+$, $-$ a $\cdot$ takto:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{max\{n,m\}} (a_i + b_i) x^i$$

$$-\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (-a_i) x^i$$

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m+n} \left(\sum_{j=1}^{i} a_j \cdot b_{i-j} x^i \right),$$

kde dodefinujeme nepřímo zadané koeficienty nulami.

Definice 12. *Nechť g,$f \in R[x]$ jsou polynomy nad oborem R a g je monický. Operaci modulo polynom g definujeme předpisem*

$$f \mod g = r,$$

kde $r \in R[x]$ je polynom splňující

$$(f = gd + r) \wedge (deg(r) < deg(g)) \tag{1.1}$$

pro nějaké $d \in R[x]$.

Poznámka. Pokud je g monický, pak pro polynomy g a f v předchozí definici existuje právě jedna dvojice polynomů r a d splňující podmínky (1.1). Operace je tedy dobře definovaná.

Definice 13. *Nechť R je okruh a $m \in R[x]$ je monický polynom stupně $n > 0$. Faktorokruhem $R[x]/m$ budeme nazývat množinu všech polynomů stupně menšího než n se standardními operacemi $+$ a $-$ a s operací $\cdot$, kterou definujeme následovně:*

$$f \cdot g = f \cdot g \mod m.$$

Vzniklý faktorokruh s danými operacemi skutečně splňuje definici okruhu, jak můžeme nahlédnout v (Stanovský, 2021, str. 46-47)

Následuje soubor definic o tělesových rozšířeních.

Definice 14. *Řekneme, že $T < U$ je rozšíření těles, pokud T a U jsou tělesa a platí $T \subset U$.*

Říkáme, že T je podtěleso U, a U je nadtěleso T.

Řekneme, že prvek $a \in U$ je algebraický nad tělesem T, pokud existuje polynom $f \in T[x]$, pro který $f(a) = 0$.

Symbolem $T(a)$ označíme nejmenší nadtěleso T obsahující prvek a.

Definice 15. *Nechť T je těleso a $f \in T[x]$ je nenulový polynom. Řekneme, že U je kořenovým nadtělesem polynomu f nad tělesem T, pokud existuje $a \in U$ takové, že $f(a) = 0$ a $U = T(a)$.*

Řekneme, že U je rozkladovým nadtělesem polynomu f nad tělesem T, pokud se f v U rozkládá na kořenové činitele $f(x) = c(x - a_1) \cdots (x - a_n)$, kde c,$a_1, \ldots, a_n \in U$, a platí $U = T(a_1, \ldots, a_n)$

Tvrzení 1. *Nechť T je těleso a $f \in T[x]$ je polynom stupně většího než 0. Pak existuje kořenové nadtěleso polynomu f nad tělesem T a existuje rozkladové nadtěleso polynomu f nad tělesem T.*

Předchozí tvrzení bylo dokázáno v předmětu Úvod do komutativní algebry, a důkaz lze najít v (Kala, 2021, str. 20)

Definice 16. *Nechť T je těleso. Symbolem $T_{(n)}$ budeme značit rozkladové nadtěleso polynomu $x^n - 1$ a položíme $E_{(n)} = \{\alpha \in T_{(n)} : \alpha^n = 1\}$.*

Poznámka. Pokud charakteristika tělesa T je prvočíslo $p \in \mathbb{N}$, pak $E_{(n)}$ je cyklická podgrupa $T^*_{(n)}$ a pokud $p \nmid n$, potom platí $|E_{(n)}| = n$.

Definice 17. *Označíme $P_{(n)}$ množinu generátorů $E_{(n)}$. Polynom*

$$Q_n = \prod_{\alpha \in E_{(n)}} (x - \alpha) \in T_{(n)}[x]$$

nazveme n-tým cyklotomickým polynomem.

Tvrzení 2. *Nechť $q = p^n$ pro p prvočíslo, $P = \mathbb{F}_p$ je prvotěleso tělesa $\mathbb{F}_q$ a d značí řád prvku $(q \mod n)$ v $\mathbb{Z}_n^*$. Potom*

- $x^n - 1 = \prod_{k|n} Q_k$
- $Q_n \in P[x]$
- *Q_n se rozkládá na $\frac{\phi(n)}{d}$ polynomů stupně d.*

Tvrzení 2 je větou 4.7. z (Žemlička, str.11), kde je i dokázáno.

Definujeme mřížku podle bakalářské práce Kroutil (2019).

Definice 18. *Aditivní diskrétní podgrupa M v $\mathbb{R}^n$ se nazývá mřížka, pokud existuje m lineárně nezávislých vektorů $a_1, \ldots, a_m \in M$ takových, že*

$$M = \sum_{i=1}^{m} a_i \mathbb{Z} = \left\{ \sum_{i=1}^{m} x_i a_i : x_1, \ldots, x_m \in \mathbb{Z} \right\}.$$

Vektory $a_1, \ldots, a_m$ se nazývají bází mřížky M. Pokud platí $n = m$, mluvíme o mřížce plné hodnosti.
Pokud je M podgrupou $\mathbb{Z}^n \leq \mathbb{R}^n$, říkáme, že mřížka je celočíselná

Zde definujeme několik základních objektů z pravděpodobnosti.

Definice 19. *Nechť Ω je neprázdná spočetná množina. Nechť $P : \Omega \to [0,1]$ je zobrazení takové, že $\sum_{\omega \in \Omega} P(\omega) = 1$, pak říkáme, že (Ω, P) je diskrétní pravděpodobnostní prostor.*

Prvky množiny Ω nazýváme elementární jevy. Hodnotu $P(\omega)$ definujeme jako pravděpodobnost elementárního jevu $\omega \in \Omega$.

Libovolná podmnožina $E \subset \Omega$ se nazývá náhodný jev a definujeme pro něj $P(E) = \sum_{\omega \in E} P(\omega)$ pravděpodobnost jevu E.

V práci budeme používat pomocné algoritmy, díky kterým budeme schopni simulovat náhodné rozdělení podle diskrétní pravděpodobnosti.

Definice 20. *Nechť D je diskrétní pravděpodobnost na spočetné množině Ω. Potom definujeme nedeterministický algoritmus $Prav(D,\Omega)$, vracející prvky množiny Ω, takový, že je pro každé $x \in \Omega$ pravděpodobnost, že x je výsledkem algoritmu $Prav(D,\Omega)$ rovna hodnotě $D(x)$.*

Poznámka. Nedeterministický algoritmus je takový algoritmus, který může v alespoň jednom ze svých kroků zvolit z více možností dalších kroků. Na rozdíl od deterministického algoritmu může vracet různé výsledky pro stejná zadání.

Skutečnost, že elementární jev x je výsledkem algoritmu $Prav(D,\Omega))$ budeme značit $x \leftarrow Prav(D,\Omega)$. Stejně tak zavedeme značení pro přiřazení hodnoty y prvku x předpisem $x \leftarrow y$. Pokud U_Ω je pravděpodobnost na konečné množině Ω, pro kterou platí $\forall x \in \Omega : U_\Omega(x) = 1/|\Omega|$, budeme používat značení $x \leftarrow \Omega$, místo $x \leftarrow Prav(U_\Omega,\Omega)$.

Ve všech použitých případech, bude množina Ω nejvýše spočetná.

1.2 Okruh $\mathbb{Z}[x]/(x^n+1)$

Díky předchozím uvedeným definicím můžeme zavést základní objekty, se kterým budeme pracovat. Těmi jsou faktorokruhy $R = \mathbb{Z}[x]/(x^n+1)$ a $R_q = \mathbb{Z}_q[x]/(x^n+1)$, kde $n \in \mathbb{N}$ a q je liché prvočíslo.

Prvky těchto okruhů jsou tedy polynomy stupně menšího, než n s koeficienty v $\mathbb{Z}$, popřípadě $\mathbb{Z}_q$.

První z daných okruhů nemá omezení na velikost koeficientů daných polynomů. Koeficienty druhého okruhu budeme pro potřeby dalšího počítání brát v souladu s definicí 10 v intervalu $(-(q-1)/2,(q-1)/2)$. Množinu prvků okruhu R_q budeme moci chápat jako podmnožinu okruhu R.

Poznámka. Ve zbytku kapitoly budeme pracovat s prvky a, b a c okruhu R (resp. R_q), kde $a = \sum_{i=0}^{n-1} a_i x^i$, $b = \sum_{i=0}^{n-1} b_i x^i$ a $c = \sum_{i=0}^{n-1} c_i x^i$.

Definice 21. *Na okruhu R (resp. R_q) definujeme zobrazení $[\cdot] : R \to \mathbb{Z}^n$ (resp. $[\cdot] : R_q \to \mathbb{Z}_q^n$) předpisem:*

$$[a] = (a_0,a_2,\ldots,a_{n-1})^T.$$

Dále na množině $[R] \subset \mathbb{Z}^n$ (resp. $\mathbb{Z}_q^n$), kde $[R]$ je obraz množiny R zobrazením $[\cdot]$, zavedeme binární operaci násobení $\cdot$ předpisem:

$$[a] \cdot [b] = [a \cdot b],$$

kde $[a] = (a_0,a_2,\ldots,a_{n-1})^T$ a $[b] = (b_0,b_2,\ldots,b_{n-1})^T$.

Tvrzení 3. *Množina $\mathbb{Z}^n$ (resp. $\mathbb{Z}_q^n$) se standardními operacemi $+$ a $-$ (modulo q), které jsou definovány po složkách, a operací násobení $\cdot$ definovanou výše tvoří okruh a pro každé $a,b,c \in R$ takové, že $[a] \cdot [b] = [c]$, platí*

$$c_l = \left(\sum_{i+j=l} a_i b_j - \sum_{i+j=n+l} a_i b_j \right),$$

respektive

$$c_l = \left(\sum_{i+j=l} a_i b_j - \sum_{i+j=n+l} a_i b_j \right) \mod q,$$

$\forall l \in \{0,\ldots,n-1\}$.

Zobrazení $[\cdot] : R \to \mathbb{Z}^n$ (resp. $[\cdot] : R_q \to \mathbb{Z}_q^n$) je izomorfismus okruhů.

Důkaz. Tvrzení dokážeme pro zobrazení $[\cdot] : R \to \mathbb{Z}^n$. Pro okruh modulo prvočíslo q se tvrzení dokáže stejně.

Nejprve ukážeme, že zobrazení $[\cdot]$ je bijekce.

To lze nahlédnout ze vztahu $[a] = [b] \Leftrightarrow \forall i \in \{0,\ldots,n-1\}$ platí $a_i = b_i \Leftrightarrow a = b$.

Zobrazení $[\cdot]$ zachovává z definice operaci násobení. Dále platí

$$[a] + [b] = (a_0,\ldots,a_{n-1})^T + (b_0,\ldots,b_{n-1})^T = (a_0+b_0,\ldots,a_{n-1}+b_{n-1})^T = [a+b],$$

$$-[a] = -(a_0,\ldots,a_{n-1})^T = (-a_0,\ldots,-a_{n-1})^T = [-a].$$

Operace v $\mathbb{Z}^n$ tedy přesně odpovídají operacím v R a všechny axiomy okruhu jsou v $\mathbb{Z}^n$ splněny, protože jsou splněny v R.

$\mathbb{Z}^n$ s danými operacemi tvoří okruh, který je izomorfní okruhu R. Nyní již stačí dokázat explicitní vzorec pro násobení v $\mathbb{Z}^n$.

$$[a] \cdot [b] = [c] \Leftrightarrow a \cdot b = c$$

Víme, že v $\mathbb{Z}[x]$ pro všechna $i \in \{0, \ldots, n-1\}$ platí $x^{n+i} \mod (x^n+1) = -x^i$.

Z tohoto vztahu získáváme

$$\begin{aligned}
a \cdot b &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{i+j} \mod (x^n+1) \\
&= \sum_{l=0}^{2n-2} \sum_{i+j=l} a_i b_j x^l \mod (x^n+1) \\
&= \sum_{l=0}^{n-1} \left(\sum_{i+j=l} a_i b_j x^l + \sum_{i+j=n+l} a_i b_j x^{n+l} \right) \mod (x^n+1) \\
&= \sum_{l=0}^{n-1} \left(\sum_{i+j=l} a_i b_j - \sum_{i+j=n+l} a_i b_j \right) x^l,
\end{aligned}$$

což jsme chtěli dokázat. □

Aditivní grupa okruhu R je izomorfní aditivní grupě $\mathbb{Z}^n$, je tedy izomorfní podgrupě $\mathbb{R}^n$. Všechny její prvky se dají zapsat jako součet celočíselných násobků n-prvkové kanonické báze. Splňuje tedy definici mřížky. R_q s operací sčítání již mřížkou není. Stále v sobě ale zachovává jisté vlastnosti okruhu R a s ním spojené mřížky.

Prvky okruhů R a R_q budeme ztotožňovat s prvky $\mathbb{Z}^n$ a $\mathbb{Z}_q^n$ pomocí zobrazení $[\cdot]$.

Definice 22. *Nechť S je abelovská grupa. Normu na S definujeme jako reálné zobrazení $l : S \to \mathbb{R}_0^+$, splňující pro všechna $a,b \in S$ a všechna $\alpha \in \mathbb{Z}$ následující vlastnosti:*

- $l(a) = 0 \Leftrightarrow a = 0$
- $l(a+b) \leq l(a) + l(b)$
- $l(\alpha a) = |\alpha| l(a)$

Pokud budeme hovořit o normách prvku $s \in R_q$, budeme tím vždy myslet normu prvku s jakožto prvku okruhu R. Na R_q normy neexistují.

Definice 23. *Na R definujeme zobrazení l_1, l_2 a l_∞ do reálných čísel předpisy:*

$$l_1(a) = \|a\|_1 = \sum_{i=0}^{n-1} |a_i|,$$

$$l_2(a) = \|a\| = \sqrt{\sum_{i=0}^{n-1} a_i^2} \qquad a$$

$$l_\infty(a) = \|a\|_\infty = \max_{i \in \{0,1,\ldots,n-1\}} |a_i|,$$

kde $a = \sum_{i=0}^{n-1} a_i x^i \in R$.

Tvrzení 4. *Zobrazení l_1, l_2 a l_∞ splňují definici normy na R. Těmto normám se postupně říká jednotková, euklidovská a maximová.*

Důkaz. Tvrzení vyplývá z vlastností norem reálných čísel. První a třetí vlastnost je splněna triviálně. Druhá vlastnost u norem l_1 a l_∞ platí díky trojúhelníkovému pravidlu $|a_i + b_i| \leq |a_i| + |b_i|$ pro a_i, $b_i \in \mathbb{R}$, které platí pro reálná čísla. U normy l_2 lze druhá vlastnost nahlédnout z následujících vlastností reálných čísel:

$$\forall 0 \leq a,b \in \mathbb{R} \text{ platí } a \leq b \Leftrightarrow a^2 \leq b^2$$

a obecného vztahu mezi koeficienty

$$(a_i + b_i)^2 \leq (a_i)^2 + (b_i)^2.$$

□

Tyto normy jsou obdobou klasicky definovaných norem na prostoru $[R] \subset Z^n$.

Poznámka. Nechť $k \in \mathbb{N}$ a $\mathbf{r} = (r_1, \ldots, r_k)^T \in R^k$. Normy l_1, l_2 a l_∞ vektoru $\mathbf{r}$ budeme chápat jako normy v abelovské grupě $\mathbb{Z}^n \times \cdots \times \mathbb{Z}^n \simeq R^k$, definované následovně:

$$l_1(r) = \|\mathbf{r}\|_1 = \sum_{j=1}^{k} \|r_i\|_1,$$

$$l_2(r) = \|\mathbf{r}\| = \sqrt{\sum_{j=1}^{k} \|r_i\|^2} \quad \text{a}$$

$$l_\infty(r) = \|\mathbf{r}\|_\infty = \max_{j \in \{1,\ldots,k\}} \|a_i\|_\infty.$$

Pro vytvoření lepší představy si ukážeme jednoduchý příklad. Při využití v šifrování chceme používat větší objekty. Mnohdy budeme také chtít, aby použitá přirozená čísla n a q vůči sobě splňovala specifická kritéria.

Příklad. Nechť $n = 8$, $q = 5$. Potom uvažujeme okruh $R_5 = \mathbb{Z}_5[x]/(x^8 + 1)$.

Ukážeme, jak v tomto konkrétním okruhu fungují operace a spočítáme si normy prvků tohoto okruhu.

První důležitou připomínkou může být, že okruh R_5 je konečný. Každý prvek má 8 koeficientů, z nichž každý z nich je prvkem množiny $\{-2, -1,0,1,2\}$. Dohromady máme tedy okruh řádu 40.

Označíme si dva prvky tohoto okruhu.

$$[a] = [1 - 1x^1 - 2x^2 + x^4 - 2x^5 + 2x^6 + 2x^7] = (1, -1, -2,0,1, -2,2,2)^T,$$

$$[b] = [1 + 1x^1 + 2x^2 + 1x^3 - 2x^4 - 2x^5] = (1,1,2,1, -2, -2,0,0)^T.$$

Tento zápis umožňuje snadnou orientaci v jednotlivých prvcích a jejich koeficientech, a velice zjednodušuje sčítání prvků, které probíhá stejně jako ve vektorovém prostoru $\mathbb{Z}_5^8$.

$$[a+b] = \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 2 \\ 1 \\ -2 \\ -2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+1 \\ -1+1 \\ -2+2 \\ 0+1 \\ 1+(-2) \\ -2+(-2) \\ 2+0 \\ 2+0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \\ -1 \\ 1 \\ 2 \\ 2 \end{pmatrix}$$

Násobení x bude v tomto zápise reprezentováno bitovým posunem o jednu pozici dolů, kde na první pozici nového vektoru zapíšeme opačnou hodnotu prvku na poslední pozici v násobeném vektoru. Takový zápis odpovídá opravdovému vynásobení x a následnému modulu polynomem $x^8 + 1$. Pro ukázku nejprve vynásobíme prvek a mocninou x.

$$[x \cdot a] = [x \cdot (1 - 1x^1 - 2x^2 + x^4 - 2x^5 + 2x^6 + 2x^7)] = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \end{pmatrix}$$

Nyní by už mělo být jednoduché spočítat násobek dvou prvků. Použijeme distributivitu a asociativitu sčítání prvků v okruhu.

$$[ab] = \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} + [x] \cdot \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} + [2x^2] \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} + [x^3] \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} - [2x^4] \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} - [2x^5] \begin{pmatrix} 1 \\ -1 \\ -2 \\ 0 \\ 1 \\ -2 \\ 2 \\ 2 \end{pmatrix} =$$

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

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

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

Nyní spočítáme normy prvku $a \in R_q$ jakožto prvku v okruhu R.

$$\|a\|_1 = \sum_{i=0}^{7} |a_i| = 1+1+2+0+1+2+2+2 = 11,$$

$$\|a\| = \sqrt{\sum_{i=0}^{7} a_i^2} = \sqrt{1+1+4+0+1+4+4+4} = \sqrt{19},$$

$$\|a\|_\infty = \max_i |a_i| = 2.$$

Pro velké prvočíslo q operace v R_q s prvky malých norem odpovídají operacím v R. Pokud bereme R_q jako podmnožinu R, jsou vlastnosti norem pro prvky R_q s dostatečně malými velikostmi koeficientů zachovány.

1.2.1 Vlastnosti okruhu R_q pro specifické zadání n a q

Pro správnost algoritmu 7 budeme potřebovat aby prvky malých nenulových norem v R_q byly invertibilní.

Použijeme obdobu Lemmat 2.1 a 2.2 z Lyubashevsky a Neven (2017)

Lemma 5. *Nechť $q \equiv 5 \pmod 8$ je prvočíslo a $\kappa \in \mathbb{Z}$. Potom q je prvek řádu 2^κ v grupě $\mathbb{Z}_{2^{\kappa+2}}$.*

Důkaz. Protože $q \equiv 5 \pmod 8$, víme, že $|\mathbb{Z}_q^*| = q - 1 = 4h$, kde $h \in \mathbb{N}$ je liché. Stáčí ověřit, že platí

$$(1+4h)^{2^\kappa} \equiv 1 \pmod{2^{\kappa+2}} \text{ a zároveň } (1+4h)^{2^{\kappa-1}} \not\equiv 1 \pmod{2^{\kappa+2}}.$$

Podle binomického vzorce získáme rovnost

$$(1+4h)^{2^\kappa} = \sum_{l=0}^{2^\kappa} \binom{2^\kappa}{l} 4^l h^l$$

V tuto chvíli se nám bude hodit důsledek z Kapitoly 2.9 v práci Drápal, který říká, že pro prvočíslo p, $s \in \mathbb{N}_0$ platí

$$v_p\left(\binom{p^s}{l}\right) = s - v_p(l), \text{ pokud } 1 \le l \le p^s.$$

Dále platí $v_2(l) \le l - 1$. Pro $l \in \{1, \ldots, 2^\kappa\}$ získáme nerovnost

$$v_2\left(\binom{2^\kappa}{l} 4^l h^l\right) = v_2\left(\binom{2^\kappa}{l}\right) + 2l = \kappa - v_2(l) + 2l \ge \kappa - (l-1) + 2l \ge \kappa + 2,$$

tedy $2^{\kappa+2} \left| \binom{2^\kappa}{l} 4^l h^l \right.$ a

$$q^{2^\kappa} = (1+4h)^{2^\kappa} = 1 + \sum_{l=1}^{2^\kappa} \binom{2^\kappa}{l} 4^l h^l \equiv 1 \pmod{2^{\kappa+2}}.$$

Na druhou stranu máme

$$(1+4h)^{2^{\kappa-1}} = \sum_{l=0}^{2^{\kappa-1}} \binom{2^{\kappa-1}}{l} 4^l h^l$$

a pro $l \in \{2, \ldots, 2^{\kappa-1}\}$ platí

$$v_2\left(\binom{2^{\kappa-1}}{l} 4^l h^l\right) = (\kappa-1) - v_p(l) + 2l \geq (\kappa-1) - (l-1) + 2l = \kappa + l \geq \kappa + 2,$$

proto

$$(1+4h)^{2^{\kappa-1}} = 1 + 2^{\kappa-1}4h + \sum_{l=2}^{2^{\kappa-1}} \binom{2^{\kappa-1}}{l} 4^l h^l \equiv 1 + 2^{\kappa+1}h \not\equiv 1 \pmod{2^{\kappa+2}}.$$

□

Lemma 6. *Nechť $q \equiv 5 \pmod 8$ je prvočíslo. Pak existuje $r \in \mathbb{N}$ takové, že $r^2 \equiv -1 \pmod q$ a pro každé $\kappa \in \mathbb{N}$ jsou polynomy $x^{2^\kappa} - r$ a $x^{2^\kappa} + r$ ireducibilní nad $\mathbb{Z}_q[x]$.*

Důkaz. Z vět 16.4. a 16.7. v publikaci Stanovský (2021) víme, že multiplikativní grupa tělesa je cyklická grupa a že cyklická grupa obsahuje právě $\varphi(d)$ prvků řádu d, kde d dělí velikost grupy. V $\mathbb{Z}_q^*$ tedy existují přesně $\varphi(4) = 2$ prvky řádu 4 a jeden prvek řádu 2, který se rovná -1. Nechť a je pevně zvolený generátor grupy $\mathbb{Z}_q^*$, pak označme $r = a^h$ prvek řádu 4. Platí $r^2 = a^{2h} = -1$. Tím jsme dokázali existenci prvku r.

Dále využijeme Lemma 5 a třetí bod Tvrzení 2. Polynom $Q_{2^{\kappa+2}}$ se rozkládá na $\phi(2^{\kappa+2})/ord(q) = 2^{\kappa+1}/2^\kappa = 2$ ireducibilní polynomy řádu $ord(q) = 2^\kappa$ v $\mathbb{Z}_q[x]$.

Zároveň víme, že

$$x^{2^{\kappa+2}} - 1 = \prod_{l \mid 2^{\kappa+2}} Q_l = Q_{2^{\kappa+2}} \prod_{l \mid 2^{\kappa+1}} Q_l = Q_{2^{\kappa+2}}(x^{2^{\kappa+1}} - 1)$$

a proto

$$Q_{2^{\kappa+2}} = x^{2^{\kappa+1}} + 1 = (x^{2^\kappa} - r)(x^{2^\kappa} + r)$$

a polynomy $x^{2^\kappa} - r$ a $x^{2^\kappa} + r$ jsou ireducibilní v $\mathbb{Z}_q[x]$.

□

Lemma 7. *Nechť $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, kde $n > 1$ je mocninou dvojky a $q \equiv 5 \pmod 8$ je prvočíslo. Potom všechny nenulové polynomy $a \in R_q$ takové, že $\|a\|_\infty < \sqrt{q/2}$, jsou invertibilní.*

Důkaz. Vycházíme z důkazu Lemmatu 2.2 v Lyubashevsky a Neven (2017). Podle Lemmatu 6 má faktorizující polynom ireducibilní rozklad

$$x^n + 1 = (x^{n/2} + r)(x^{n/2} - r),$$

kde pro $r \in \mathbb{Z}_q$ platí $r^2 = -1$.

Každý neinvertibilní polynom $f(x) \in R_q$ je stupně menšího, než n, a musí být dělitelný jedním z polynomů $x^{n/2} + r$, nebo $x^{n/2} - r$. Polynom můžeme zapsat jako $f(x) = f_0(x) + x^{n/2} f_1(x)$, pro $f_0(x), f_1(x)$ stupně menšího než $n/2$. Tedy platí jedna z rovností

$$f(x) \mod (x^{n/2} + r) = f_0(x) - r f_1(x) = 0,$$

$$f(x) \mod (x^{n/2} - r) = f_0(x) + r f_1(x) = 0$$

Nechť a_i a b_i jsou koeficienty u x^i postupně v polynomech $f_0(x)$ a $f_1(x)$. Pokud platí první z rovnic, dostáváme $f_0(x) = r f_1(x)$ a také $a_i = r b_i$. Pokud platí druhá rovnice, získáme analogicky $f_0(x) = -r f_1(x)$ a $a_i = -r b_i$. Dohromady tedy

$$a_i = \pm r b_i$$

a umocněním dostáváme

$$(a_i)^2 = (r b_i)^2 = -(b_i)^2 \text{ a } (a_i)^2 + (b_i)^2 = 0$$

Pro $0 \neq \|f(x)\|_\infty < \sqrt{q/2}$ ale máme $(a_i)^2 + (b_i)^2 < q$ a v $\mathbb{Z}_q$ je tento výraz roven 0, jen pokud $a_i = b_i = 0$. Polynom f je tedy invertibilní v $\mathbb{Z}_q$. □

Od této chvíle budeme pro potřeby naší práce uvažovat $n = 2^l$, pro $l \in \mathbb{N}$ a $q \equiv 5 \pmod 8$ prvočíslo.

2. Přípravné algoritmy

Zkoumaný protokol je jedním z algoritmů, které nazýváme *ověření s nulovou znalostí*. Patří do části asymetrické kryptografie, která používá existenci soukromého a veřejného klíče. Klíč určený k šifrování nazýváme veřejný a budeme značit pk. Na druhou stranu příslušný soukromý klíč, který značíme sk, zná pouze jeho majitel a v kryptografických protokolech slouží k dešifrování zpráv zašifrovaných klíčem veřejným. K výpočtu veřejného klíče používáme příslušný klíč soukromý. Klíče jsou na sobě závislé, je však důležité, aby z veřejného klíče nebylo možné vypočítat klíč soukromý.

Strany, které se ověření s nulovou znalostí účastní nazveme dokazující a ověřovatel. Dokazující účastník se snaží ověřující straně dokázat že zná soukromý klíč, zároveň však dokazující nesmí v průběhu prozradit obsah tohoto klíče, ani žádné jeho důležité vlastnosti. Jde tedy o ověření, zda je dokazující majitelem soukromého klíče.

Cílem této kapitoly je představit dvě metody, předvedené v textu (Lyubashevsky a Neven, 2017, str. 300-303), jejichž principy bude využívat metoda jednorázového šifrování prezentovaná v následující kapitole.

Výsledná metoda je tedy vylepšením těchto samo o sobě funkčních kryptografických metod.

2.1 Okruhové LWE

LWE v názvu metody je zkratkou anglického „Learning with errors“. Podrobnější informace o metodě lze nalézt v článku Lyubashevsky a kol. (2013).

Definice 24. *Nechť $\lambda \in \mathbb{N}$ a g je prvočíslo takové, že $2\lambda < q$. Množinu $S_\lambda \subset R_q$ definujeme jako množinu všech bodů $a \in R$, pro které platí $\|a\|_\infty \leq \lambda$.*

Lemma 8. *Nechť l,k,$\lambda \in \mathbb{N}$, q je prvočíslo, $n = 2^l$ a nechť platí $2\lambda < q$ a $k < n$. Definujeme množinu $S_\lambda^{(k)} = \{a \in R_q : \|a\|_\infty \leq \lambda \wedge |\{i : a_i \neq 0\}| \leq k\}$. Potom pro každé dva prvky a a $b \in S_\lambda^{(k)}$ platí:*

$$\|ab\|_\infty \leq k\lambda^2.$$

Pro $\lambda = 1$, je druhé omezení na množinu $S_\lambda^{(k)}$ ekvivalentní podmínce $\|a\|_1 \leq k$, neboť $\forall a \in S_1 : \|a\|_1 = \sum_{i=0}^{n-1} |a_i| = \sum_{a_i \neq 0} |a_i| = \sum_{a_i \neq 0} 1 = |\{i : a_i \neq 0\}|$.

Důkaz. Označíme $[ab] = [c] = (c_0, \ldots, c_{n-1})^T$. Víme, že

$$\|c\|_\infty = \max_{i \in \{0,1,\ldots,n-1\}} |c_i|.$$

Stačí nám tedy pro obecné $l \in \{0,1,\ldots,n-1\}$ omezit hodnotu $|c_l|$. Zároveň pro libovolné $a \in \mathbb{Z} : |a \mod q| \leq |a|$ z definice modulu. Podle vztahu z Tvrzení 3 budeme počítat:

$$|c_l| \leq \left| \sum_{i+j=l} a_i b_j - \sum_{i+j=n+l} a_i b_j \right| \leq \left| \sum_{i+j=l} a_i b_j \right| + \left| \sum_{i+j=n+l} a_i b_j \right| \leq \sum_{i+j \equiv l \pmod n} |a_i b_j|.$$

Dále platí, že nenulových koeficientů v a a b je nejvýše k. Dvojic koeficientů (i,j) takových, že $i+j \equiv l \pmod n$, pro které je násobek $a_i b_j$ nenulový, je také nejvýše k, neboť pro každé $l \in \mathbb{Z}$ a pro každé $i \in \{0,1,\ldots,n-1\}$ existuje právě jedno $j \in \{0,1,\ldots,n-1\}$, takové, že $i+j \equiv l \pmod n$. Proto tedy:

$$\sum_{i+j \equiv l \pmod n} |a_i b_j| \leq k \max_{0 \leq i,j < n} |a_i b_j| \leq k\lambda^2$$

Platí tedy, že $\|ab\|_\infty \leq k\lambda^2$. □

Dále můžeme nahlédnout, že

$$\|a \cdot b\|_\infty = \max_l \left\{ \sum_{i+j \equiv l \pmod n} |a_i b_j| \right\} \leq \sum_{i=0}^{n-1} |a_i| \max_j |b_j| \leq \|a\|_1 \|b\|_\infty. \tag{2.1}$$

Definice 25. *Nechť $l,k_1,k_2,\lambda \in \mathbb{N}$, q je prvočíslo, $n = 2^l$ a nechť platí $\lambda < q$ a $k_1 \leq k_2 < n$. Definujeme množinu*

$$S_\lambda^{(k_1,k_2)} = \{a \in R_q : \|a\|_\infty \leq \lambda \wedge k_1 \leq |\{i : a_i \neq 0\}| \leq k_2\}.$$

Množina $S_\lambda^{(k_1,k_2)}$ je konečná.
Dále budeme pro pevná k_1 a k_2 množinu $S_1^{(k_1,k_2)}$ zapisovat jako S.

2.1.1 Algoritmus

Nechť $l,k_1,k_2,p \in \mathbb{N}$, $q \equiv 5 \pmod 8$ je prvočíslo, $n = 2^l$ a nechť platí

$$k_1 \leq k_2 < n \text{ a } p(2k_2+2) \leq q/2.$$

Z množiny S zvolíme tajné parametry s_1 a s_2. A z množiny R_q zvolíme veřejný parametr a. Z těchto veličin vypočítáme $t = s_1 a + s_2$. Parametry jsou zvoleny uniformě náhodně jako výsledky algoritmů $Prav(U_S,S)$ a $Prav(U_{R_q},R_q)$. Jako soukromý klíč bereme hodnotu s_1 a klíčem veřejným myslíme dvojici (a,t). Parametr s_2 v algoritmu reprezentuje chybu (od toho slovo „error“ v názvu algoritmu).

Algorithm 1: LWE algoritmus

Input: Prvočísla p, q, prvky $sk,a,t \in R_q$.
Output: Prvek množiny $\{0,1\}$
$r,e,e' \leftarrow S$;
$m \leftarrow R_p$;
$v \leftarrow p(ar+e)$;
$w \leftarrow p(tr+e') + m$;
$d \leftarrow w - sk \cdot v \mod q \mod p$;
if $m = d$ **then**
  return *1*;
end
return *0*

Vztah prvků v a w k předchozím hodnotám můžeme maticově zapsat takto:

$$\begin{pmatrix} v \\ w \end{pmatrix} = \begin{pmatrix} pa & p & 0 & 0 \\ pt & 0 & p & 1 \end{pmatrix} \begin{pmatrix} r \\ e \\ e' \\ m \end{pmatrix} \mod q,$$

kde je operace modulo q brána po prvcích výsledného vektoru. Hodnoty r,e,e' a m si tázající volí. Pokud by je však zvolil předvídatelně, mohl by se dokazující pokusit dané m uhodnout. Proto je lepší volit tyto parametry uniformě náhodně.

Tvrzení 9. *Nechť s_1, s_2,r,e,$e' \in S$, $a \in R_q$, $t = s_1 a + s_2$ a $m \in R_p$. Dále nechť $v = p(ar + e)$ a $w = p(tr + e') + m$ jsou prvky R, potom platí:*

$$((w - vs_1) \mod q) \mod p = m.$$

Důkaz. Podle zadání víme:

$$w = p(tr + e') + m = p((as_1 + s_2)r + e') + m = p(as_1 r + s_2 r + e') + m$$

$$vs_1 = p(ar + e)s_1,$$
$$w - vs_1 = p(s_2 r + e' - es_1) + m.$$

Hledáme tedy hodnotu výrazu $p(s_2 r + e' - es_1) + m \mod q \mod p$.

Víme, že s_2, r, e', s_1 i e jsou prvky S. Zároveň $m \in R_p$. Díky Lemmatu 8 víme, že platí:

$$\|s_2 r\|_\infty, \|s_1 e\|_\infty \leq k_2, \ \ \|e'\|_\infty \leq 1$$
$$\|m\|_\infty \leq p/2.$$

Dále pomocí trojúhelníkové nerovnosti získáme

$$\|s_2 r + e' - s_1 e\|_\infty \leq \|s_2 r\|_\infty + \|e'\|_\infty + \|s_1 e\|_\infty \leq 2k_2 + 1$$

$$\|p(s_2 r + e' - s_1 e) + m\|_\infty \leq p(2k_2 + 1) + p/2 < p(2k_2 + 2) \leq q/2$$

Proto víme, že hodnoty koeficientů prvku $p(s_2 r + e' - s_1 e) + m$ se nacházejí v množině $\{-(q-1)/2, (q+2)/2\}$ a použitím modula q se nezmění:

$$p(s_2 r + e' - s_1 e) + m \mod q \mod p = p(s_2 r + e' - s_1 e) + m \mod p = m,$$

neboť $m \in R_p$. □

Podle Tvrzení 9 tedy víme, že se správným soukromým klíčem je možné z parametrů v w w vypočítat prvek m.

Pokud je dokazující majitelem soukromého klíče s_1, může do vstupu algoritmu dosadit soukromý klíč s_1. V tom případě je podle Tvrzení 9 výsledkem algoritmu hodnota 1. Takový výsledek je brán jako důkaz znalosti klíče s_1. Představený protokol může být sám o sobě použit jako ověření s nulovou znalostí. Konstrukce v původním článku Lyubashevsky a Neven (2017) dovolovala ověřovateli vybrat si hodnoty r,e,e' a m a dokazovateli poslat dvojici (v,w). Dokazovatel vypočítal hodnotu $p(s_2 r + e' - s_1 e) + m \mod q \mod p$, kterou vrátil ověřovateli. Námi představený algoritmus však spojuje kroky ověřovatele i dokazujícího dohromady, což se bude hodit pro konstrukci výsledné metody.

2.1.2 Vektorová verze

Pro pozdější použití budeme potřebovat algoritmus 1 upravit tak, aby v jednu chvíli pracoval s posloupností zadaných prvků.

Budeme pracovat s abelovskou grupou

$$R^k = \{(r_1,\ldots,r_k)^T | r_i \in R, i \in \{1,\ldots,k\}\}$$

pro $k \in \mathbb{N}$.

Poznámka. Nechť $k \in \mathbb{N}$ a (P,Ω) je diskrétní pravděpodobnostní prostor, pak $\mathbf{x} \leftarrow Prav^k(P,\Omega)$ (resp. $\mathbf{x} \leftarrow \Omega^k$) bude značit situaci, kdy $x_i \leftarrow Prav(P,\Omega)$ (resp. $x_i \leftarrow \Omega$)) pro $i \in \{1,\ldots,k\}$ a $\mathbf{x} = (x_1,\ldots,x_k)$.

Prvky $q,p \in \mathbb{N}$ a $s_1,s_2,a,t \in R$ jsou stejné jako v předchozí sekci, $k \in \mathbb{N}$.

Poznámka. Nechť $\mathbf{v} \in R$ je vektor. Zápis $\mathbf{v} \mod q$ pro q liché bude nadále značit situaci, kdy jsme použili operaci modulo q samostatně na každou složku vektoru $\mathbf{v}$. Výsledný vektor je prvkem R_q.

Algorithm 2: LWE vektorová verze

Input: Prvočísla p, q, prvky $sk,a,t \in R_q$.
Output: Prvek množiny $\{0,1\}$
$\mathbf{r},\mathbf{e},\mathbf{e'} \leftarrow S^k$;
$\mathbf{m} \leftarrow R_p^k$;

$$\begin{pmatrix}\mathbf{v}\\ \mathbf{w}\end{pmatrix} \leftarrow \begin{pmatrix} pa\mathbf{I}_k & p\mathbf{I}_k & 0^{k\times k} & 0^{k\times k} \\ pt\mathbf{I}_k & 0^{k\times k} & p\mathbf{I}_k & \mathbf{I}_k \end{pmatrix} \begin{pmatrix}\mathbf{r}\\ \mathbf{e}\\ \mathbf{e}'\\ \mathbf{m}\end{pmatrix} \mod q$$

$\mathbf{d} \leftarrow \mathbf{w} - sk \cdot \mathbf{v} \mod q \mod p$;
if $\boldsymbol{m} = \boldsymbol{d}$ **then**
  return *1*;
end
return *0*

Algoritmus 2 pro jednotlivé koeficienty vektorů odpovídá předchozímu Algoritmus 1. O vektorové verzi můžeme vyslovit tvrzení odpovídající Tvrzení 9.

Tvrzení 10. *Nechť* $s_1,s_2 \in S$, $\boldsymbol{r},\boldsymbol{e},\boldsymbol{e}' \in S^k$, $a \in R_q$, $t = s_1a + s_2$, $\boldsymbol{m} \in R_q^k$, $\boldsymbol{v} = p(a\boldsymbol{r} + \boldsymbol{e})$ *a* $\boldsymbol{w} = p(t\boldsymbol{r} + \boldsymbol{e}')$, *potom platí*

$$((\boldsymbol{w} = \boldsymbol{v}s_1) \mod q) \mod p = \boldsymbol{m}.$$

Důkaz je obdobou důkazu Tvrzení 9.

I zde tedy můžeme se správným soukromým klíčem získat hodnotu $\mathbf{m}$ z vektorů $\mathbf{v}$ a $\mathbf{w}$.

2.2 Přerušovaný Fiat-Shamir

Druhá přípravná metoda se skládá z dvojice algoritmů. První z nich zašifruje hodnotu $\mathbf{s} \in S^k$. V ověření s nulovou znalostí jej používá dokazující, aby dokázal znalost řešení soustavy lineárních rovnic nad R_q. Druhý algoritmus používá ověřovatel, aby zjistil, zda je možné z předchozího algoritmu získat šifrovaný text, který získal od dokazujícího.

Ve výsledném algoritmu používá první zašifrovací algoritmus naopak ověřovatel. První z algoritmů, spolu s veřejným klíčem, je použit k zašifrování nějaké zprávy. Tato zašifrovaná zpráva je posléze použita jako výzva, kterou má za úkol dokazující dešifrovat.

Definice 26. *Pro celočíselnou mřížku plné hodnosti M, $\boldsymbol{c} \in M$ a $\sigma \in \mathbb{R}^+$, definujeme funkci $D_{M,c,\sigma} : M \to [0,1]$ předpisem:*

$$D_{M,\boldsymbol{c},\sigma}(\boldsymbol{v}) = e^{\frac{-\|v-c\|^2}{2\sigma^2}} \Big/ \sum_{\boldsymbol{w}\in M} e^{\frac{-\|w-c\|^2}{2\sigma^2}}, \quad \forall \boldsymbol{v} \in M$$

kde daná norma je klasická eukleidovská norma na $\mathbb{Z}^n$.

Lemma 11. *Hodnota součtu $\sum_{\boldsymbol{w}\in M} e^{\frac{-\|w-c\|^2}{2\sigma^2}}$ je kladné reálné číslo a daná dvojice $(M,D_{M,\boldsymbol{c},\sigma})$ tvoří diskrétní pravděpodobnostní prostor.*

Důkaz. Nejprve odhadneme hodnotu dané sumy.

Pro každý vektor $a \in \mathbb{Z}^n$ je hodnota $e^{\frac{-\|\mathbf{a}\|^2}{2\sigma^2}}$ nezáporné reálné číslo z intervalu (0,1). Součet přes prvky libovolné celočíselné mřížky $M \subseteq \mathbb{Z}^n$ bude nejvýše tak velký, jako celkový součet přes prvky $\mathbb{Z}^n$. Položíme $\mathbf{c} = \vec{o}$, neboť platí

$$\{\mathbf{w} - \mathbf{c} : \mathbf{w} \in \mathbb{Z}^n\} = \mathbb{Z}^n.$$

Budeme postupovat indukcí podle n.

Pro $n = 1$ platí:

$$\sum_{\mathbf{w}\in\mathbb{Z}} e^{\frac{-\|\mathbf{w}\|^2}{2\sigma^2}} = \sum_{j\in\mathbb{Z}} e^{\frac{-j^2}{2\sigma^2}} = \sum_{j\in\mathbb{Z}} (e^{-\frac{1}{2\sigma^2}})^{j^2} = 1 + 2\sum_{j\in\mathbb{N}} (e^{-\frac{1}{2\sigma^2}})^{j^2} \leq 1 + 2\sum_{j\in\mathbb{N}} (e^{-\frac{1}{2\sigma^2}})^{j} \in \mathbb{R},$$

kde poslední nerovnost platí, neboť $e^{-\frac{1}{2\sigma^2}}$ je prvkem v intervalu (0,1) a proto $(e^{-\frac{1}{2\sigma^2}})^{j^2} \leq (e^{-\frac{1}{2\sigma^2}})^{|j|}$.

Dále nechť je součet nekonečné sumy reálný pro mřížku $\mathbb{Z}^n$. Ukážeme, že to samé platí i pro mřížku $\mathbb{Z}^{n+1} = \mathbb{Z}^n \times \mathbb{Z}$.

Nechť $\mathbf{w} = (w_0, \ldots, w_{n-1}, w_n) \in \mathbb{Z}^n$. Potom

$$\|\mathbf{w}\|^2 = \sqrt{w_0^2 + \cdots + w_{n-1}^2 + w_n^2}^2 = w_0^2 + \cdots + w_{n-1}^2 + w_n^2 = \|(w_0, \ldots, w_{n-1})\|^2 + w_n^2.$$

Můžeme tedy psát:

$$\begin{aligned}
\sum_{\mathbf{w'}\in\mathbb{Z}^{n+1}} e^{\frac{-\|\mathbf{w'}\|^2}{2\sigma^2}} &= \sum_{(\mathbf{w},i)\in\mathbb{Z}^n\times\mathbb{Z}} e^{\frac{-\|(\mathbf{w},\mathbf{i})\|^2}{2\sigma^2}} \\
&= \sum_{\mathbf{w}\in\mathbb{Z}^n} \sum_{i\in\mathbb{Z}} e^{\frac{-\|\mathbf{w}\|^2 - i^2}{2\sigma^2}} \\
&= \sum_{\mathbf{w}\in\mathbb{Z}^n} \sum_{i\in\mathbb{Z}} \left(e^{\frac{-\|\mathbf{w}\|^2}{2\sigma^2}} \cdot e^{\frac{-i^2}{2\sigma^2}} \right) \\
&= \sum_{\mathbf{w}\in\mathbb{Z}^n} e^{\frac{-\|\mathbf{w}\|^2}{2\sigma^2}} \cdot \sum_{i\in\mathbb{Z}} e^{\frac{-i^2}{2\sigma^2}},
\end{aligned}$$

kde součet první sumy je kladné reálné číslo z indukčního předpokladu a součet druhé sumy leží v $\mathbb{R}^+$ podle prvního kroku.

Nyní ověříme vlastnosti pravděpodobnosti:

- $D_{M,c,\sigma}(A) \geq 0$, $\forall A \subset M$, neboť $\forall \mathbf{v} \in M$:

$$D_{M,\mathbf{c},\sigma}(\mathbf{v}) = e^{\frac{-\|\mathbf{v}-\mathbf{c}\|^2}{2\sigma^2}} \Big/ \sum_{\mathbf{w}\in M} e^{\frac{-\|\mathbf{w}-\mathbf{c}\|^2}{2\sigma^2}} \geq 0,$$

- $P(M) = \sum_{\mathbf{v}\in M} D_{M,c,\sigma}(\mathbf{v}) = \sum_{\mathbf{v}\in M} e^{\frac{-\|\mathbf{v}-\mathbf{c}\|^2}{2\sigma^2}} \Big/ \sum_{\mathbf{w}\in M} e^{\frac{-\|\mathbf{w}-\mathbf{c}\|^2}{2\sigma^2}} = 1$.

□

Definice 27. *Hashovací funkce je zobrazení* $H : \{0,1\}^* \to \{0,1\}^i$, *kde* $i \in \mathbb{N}$. *Obraz* $H(x)$ *nazýváme otisk prvku* x. *Jestliže* $x' \neq x$ *a zároveň* $h(x') = h(x)$, *nazýváme pár* (x', x) *kolizí funkce* H.

Poznámka. Pro použití v této práci zobecníme definici klasické hashovací funkce. Budeme uvažovat funkci H vedoucí z nekonečné spočetné množiny I, do nějaké konečné množiny J. Prvky množiny I ztotožníme s jednoznačně určenými prvky množiny $\{0,1\}^*$. Pro dostatečně velké $j \in \mathbb{N}$ zvolíme prosté zobrazení z J do $\{0,1\}^j$, pomocí něhož ztotožníme prvky J s jejich obrazy v $\{0,1\}^j$. Potom budeme funkci H chápat jako příslušnou hashovací funkci z $\{0,1\}^*$ do $\{0,1\}^i$ ve smyslu uvedené definice 27.

V algoritmech budeme využívat nově definované diskrétní pravděpodobnostní prostory na množině $\{0,1\}$. Skutečnost, že $D(0) = x \in (0,1)$ a $D(1) = 1 - x$ budeme značit $D[0 : x, 1 : 1 - x]$, nebo jen $D[0 : x]$.

2.2.1 Algoritmus ověření s nulovou znalostí, zašifrování

Poznámka. Dále budeme používat operaci modulo $\mathbf{q} = (q_1, \ldots, q_l)^T \in \mathbb{Z}^l$ pro $l \in \mathbb{N}$ a q_i liché pro všechna $i \in \{1, \ldots, l\}$. Pro vektor $\mathbf{v} \in R^l$ bude platit

$$\mathbf{v} \mod \mathbf{q} = (v_1, \ldots, v_l)^T \mod \mathbf{q} = (v_1 \mod q_1, \ldots, v_l \mod q_l)^T.$$

Algoritmus 3 slouží k nalezení prvku $\mathbf{z} \in R$ a $c \in C$ malých norem, které vyhovují rovnici

$$\mathbf{Az} = c\mathbf{d} \mod \mathbf{q}, \tag{2.2}$$

za předpokladu, že známe $\mathbf{s}$, pro které

$$\mathbf{As} = \mathbf{d} \mod \mathbf{q}. \tag{2.3}$$

Lemma 12. *Nechť* $\boldsymbol{A} \in R^{k\times l}$, $\boldsymbol{s} \in S$, $\boldsymbol{d} \in R^l$, $\boldsymbol{q} \in \mathbb{Z}^l$, $\sigma \in \mathbb{R}^+$, *dále ať* $c \in R$ *a* $\boldsymbol{z} = \boldsymbol{s}c + \boldsymbol{y}$. *Pokud*

$$\boldsymbol{As} = \boldsymbol{d} \mod \boldsymbol{q}$$

pak platí

$$\boldsymbol{Ay} \mod \boldsymbol{q} = \boldsymbol{Az} - \boldsymbol{d}c \mod \boldsymbol{q}.$$

Důkaz. $\mathbf{Az} - \mathbf{d}c \mod \mathbf{q} = \mathbf{A}(\mathbf{s}c + \mathbf{y}) - \mathbf{d}c \mod \mathbf{q} = (\mathbf{As} - \mathbf{d})c + \mathbf{Ay} \mod \mathbf{q} =$
$= \mathbf{Ay} \mod \mathbf{q}$ □

Algorithm 3: Fiat-Shamir: Zašifrování

Input: l,$k \in \mathbb{N}$, matice $\mathbf{A} \in R^{k \times l}$, vektory $\mathbf{s} \in S^k$, $\mathbf{d} \in R^l$ a $\mathbf{q} \in \mathbb{Z}^l$, množina $C \subset R$, hashovací funkce $H : R^{k \times l} \times R^k \times R^k \to C$ a konstanta $\sigma \in \mathbb{R}^+$, pro kterou platí: $\sigma > 11 \cdot \max_{s \in S, c \in C} \|cs\|$.

Output: vektor $\mathbf{z} \in R^k$, s malými normami koeficientů, a prvek $c \in C$.

a,$b \leftarrow 1$;
while *b=1* **do**
  while *a=1* **do**
    $\mathbf{y} \leftarrow Prav^l(D_{R,0,\sigma},R)$;
    $c \leftarrow H(\mathbf{A},\mathbf{d},\mathbf{Ay} \mod \mathbf{q})$;
    $\mathbf{z} \leftarrow \mathbf{s}c + \mathbf{y}$;
    $a \leftarrow Prav\left(D\left[0 : \min\left\{\frac{D_{R^n,0,\sigma}(\mathbf{z})}{3 \cdot D_{R^n,\mathbf{s}c,\sigma}(\mathbf{z})},1\right\}\right],\{0,1\}\right)$;
  end
  if $\|\boldsymbol{z}\|_\infty \leq 6\sigma$ **then**
    $b = 0$
  end
  $a = 1$;
end
return $(\boldsymbol{z}, c)$

V tom případě algoritmem zvolené ($\mathbf{z}$,c) vyhovují rovnosti

$$c = H(\mathbf{A},\mathbf{d},\mathbf{Az} - \mathbf{d}c \mod \mathbf{q}) = H(\mathbf{A},\mathbf{d},\mathbf{Ay} \mod \mathbf{q}).$$

Poznámka. Vnitřní cyklus, který v Algoritmu 3 definuje nový diskrétní pravděpodobnostní prostor a posléze udává hodnotu proměnné a spolu s existencí dané hashovací funkce způsobuje, že pravděpodobnost, že jsme získali určité $\mathbf{z} \in R^k$ na konci cyklu není závislé na $\mathbf{s}$. Tento princip se nazývá *rejection sampling*. Důkaz tohoto tvrzení není obsahem této práce a jeho variantu lze najít v Lyubashevsky (2012).

2.2.2 Ověřovací algoritmus

Předchozí algoritmus generoval šifrovaný text ($\mathbf{z}$,c) pro hodnoty $\mathbf{A}$, $\mathbf{s}$ a $\mathbf{d}$.

Algorithm 4: Fiat-Shamir: Ověření

Input: l,$k \in \mathbb{N}$, matice $\mathbf{A} \in R^{k \times l}$, vektory $\mathbf{d} \in R^l$ a $\mathbf{q} \in \mathbb{Z}^l$, množina $C \subset R$, hashovací funkce $H : R^{k \times l} \times R^k \times R^k \to C$ a konstanta $\sigma \in \mathbb{R}^+$ a dvojice $(\mathbf{z}, c) \in R^k \times C$.

Output: $x \in \{0,1\}$

if $\|\boldsymbol{z}\|_\infty > 6\sigma$ **then**
  return *0*
end
if $c \neq H(\boldsymbol{A},\boldsymbol{d},\boldsymbol{Az} - \boldsymbol{d}c \mod \boldsymbol{q})$ **then**
  return *0*
end
return *1*

Hodnota výstupu Algoritmu 4 udává informaci, zda hodnoty ($\mathbf{z}$,c) mohou být výsledkem Algoritmu 3 s počátečními hodnotami $\mathbf{A}$ a $\mathbf{d}$, neboli zda dané hodnoty mohou skutečně vyhovovat rovnici (2.2).

Poznámka. Nechť hodnoty ($\mathbf{z}$,c) jsou výsledkem Algoritmu 3 se zadanými hodnotami $\mathbf{A}$, $\mathbf{s}$, $\mathbf{d}$ a $\mathbf{q}$, které vyhovují rovnici (2.3). Potom vyhovují rovnici (2.2) a Algoritmus 4 pro tyto hodnoty vrátí 1.

Předpokládáme, že pravděpodobnost, že Algoritmus 4 vrátí hodnotu 1, pro vstupní parametry $\mathbf{A}$, $\mathbf{s}$, $\mathbf{q}$, $\mathbf{z}$ a c, ale hodnoty nevyhovují rovnici (2.2) je zanedbatelná. Tato skutečnost patří do důkazu bezpečnosti dané metody.

3. Jednotlivé části metody

Nyní představíme metodu jednorázového ověřitelného šifrování pro lineární relace z okruhového LWE, která je představena v třetí kapitole článku Lyubashevsky a Neven (2017).

Definice 28. *Definujeme množiny C a $\bar{C}$ předpisem*

$$C = \{c \in R : \|c\|_\infty = 1, \|c\|_1 < 36\}$$

a

$$\bar{C} = \{c - c' : c, c' \in C\}.$$

Označme $J = \max_{\bar{c} \in \bar{C}} \|\bar{c}\|_1$

Tyto množiny jsou pevně dané a dále je nebudeme měnit.

Metoda se skládá ze čtyř částí. Těmi jsou generování klíče Kg, jednorázové zašifrování a ověření Enc a V a dešifrování Dec. Účastníky nazveme dokazující a ověřovatel. Jak již bylo řečeno, dokazující se snaží ověřovateli dokázat, že zná soukromý klíč sk. Straně, která zná soukromý klíč říkáme majitel klíče.

Generování klíčů probíhá před veškerou další komunikací. Majitel vygeneruje soukromý klíč a s jeho pomocí vytvoří klíč veřejný, který zveřejní, nebo předá budoucímu ověřovateli. Ten jej bude používat k ověření, zda komunikuje s majitelem klíče, a k šifrování zpráv pro majitele.

Ověření, že dokazující je majitelem klíče probíhá ve dvou krocích. Nejprve ověřující strana vygeneruje tajnou zprávu $\mathbf{m} \in R_p^k$ a matici $\mathbf{B} \in R_p^{l \times k}$ pro prvočíslo p a vypočítá hodnotu $\mathbf{u} \in R_p^l$ pomocí rovnosti $\mathbf{u} = \mathbf{Bm} \mod p$. Všechny tyto hodnoty zašifruje pomocí algoritmu Enc. Jako výsledek algoritmu Enc získá šifrovaný text g. Zašifrovaná data a dvojici $x = (\mathbf{B}, \mathbf{u})$ odešle dokazujícímu.

Dokazující pomocí algoritmu V ověří, zda šifrovaný text g může být výstupem algoritmu Enc se vstupními parametry x a pk. Posléze použije algoritmus Dec, do kterého vloží šifrovaný text g, prvek x a soukromý klíč sk, k nalezení dvojice prvků $(\bar{\mathbf{m}}, \bar{c}) \in R_q^k \times \bar{C}$ s malými normami. Ukážeme, že pokud dokazující skutečně použil soukromý klíč sk a $(\bar{\mathbf{m}}, \bar{c})$ je výsledek algoritmu Dec, potom je $\bar{c}$ invertibilní a platí $\mathbf{m} = \bar{\mathbf{m}}/\bar{c} \mod p$.

Nalezení dvojice $(\bar{\mathbf{m}}, \bar{c})$ prvků považuje ověřovatel za důkaz, že dokazující je majitelem příslušného soukromého klíče sk.

3.1 Generování klíče Kg

Hodnoty $s_1, s_2 \in S$ a $a \in R$ jsou generovány uniformě náhodně pomocí nedeterministických algoritmů $Prav(U_S, S)$ a $Prav(U_{R_q}, R_q)$. Dále nechť $t = as_1 + s_2$. Soukromým klíčem bude prvek

$$sk = s_1$$

a veřejným klíčem bude posloupnost

$$pk = (a, t, p, q),$$

kde $p < q$ jsou prvočísla, pro která platí

$$q \equiv 5 \pmod 8, \quad (12(2k_1+1)p+12)\sigma \leq \frac{q}{2J} \text{ a } p > 12\sigma$$

pro

$$\sigma = 11 \cdot \max_{c \in C} \|c\|_1 \cdot \sqrt{kn(3+\lambda)}$$

a hodnotu $\lambda \in \mathbb{N}, \lambda < p$. Nechť k,$l \in \mathbb{N}$ jsou pevně určená přirozená čísla a pro koeficient k_2 v definici množiny $S = S_1^{(k_1,k_2)}$ platí $p(2k_2+2) < \frac{q}{2J}$.

Všechny tyto hodnoty jsou zvoleny pevně před použitím zbylých algoritmů a po zbytek práce se nebudou měnit.

Podobně jako v metodě Fiat-Shamir budeme pracovat se soustavou lineárních rovnic nad okruhem R_q. Pro danou rovnici

$$\mathbf{Bm} = \mathbf{u} \mod p, \tag{3.1}$$

budeme hledat $\bar{\mathbf{m}} \in R_p^k$ s malou normou a $\bar{c} \in \bar{C}$, takové, že bude vyhovovat rovnici

$$\mathbf{B}\bar{\mathbf{m}} = \bar{c}\mathbf{u} \mod p. \tag{3.2}$$

Hodnoty $\mathbf{B} \in R_p^{l \times k}$, $\mathbf{m} \in R^k$ a $\mathbf{u} \in R^l$ jsou určeny ověřovatelem na začátku protokolu. Hodnota $\mathbf{m}$ je známá pouze ověřovateli.

V Algoritmu 3 jsme pracovali s rovnicí zadanou na vstupu algoritmu. Tentokrát nejprve původní rovnici (3.1) rozšíříme na vztah

$$\begin{pmatrix} pa\mathbf{I}_k & p\mathbf{I}_k & 0^{k\times k} & 0^{k\times k} \\ pt\mathbf{I}_k & 0^{k\times k} & p\mathbf{I}_k & \mathbf{I}_k \\ 0^{l\times k} & 0^{l\times k} & 0^{l\times k} & \mathbf{B} \end{pmatrix} \begin{pmatrix} \mathbf{r} \\ \mathbf{e} \\ \mathbf{e}' \\ \mathbf{m} \end{pmatrix} = \begin{pmatrix} \mathbf{v} \\ \mathbf{w} \\ \mathbf{u} \end{pmatrix} \mod \begin{pmatrix} \mathbf{q} \\ \mathbf{q} \\ \mathbf{p} \end{pmatrix}, \tag{3.3}$$

kde hodnoty $\mathbf{r}$,$\mathbf{e}$,$\mathbf{e}' \in S^k$ jsou generovány uniformě náhodně v průběhu algoritmu.

Dále budeme značit $x = (\mathbf{B},\mathbf{u})$ a

$$\mathbf{B'} = \begin{pmatrix} pa\mathbf{I}_k & p\mathbf{I}_k & 0^{k\times k} & 0^{k\times k} \\ pt\mathbf{I}_k & 0^{k\times k} & p\mathbf{I}_k & \mathbf{I}_k \\ 0^{l\times k} & 0^{l\times k} & 0^{l\times k} & \mathbf{B} \end{pmatrix}.$$

Naším cílem bude dokázat korektnost dané metody. Řekneme, že metoda (Kg,Enc,V,Dec) je korektní, pokud pro každou dvojici $(sk,pk) \leftarrow Kg$ a pro všechny dvojice $x = (\mathbf{B},\mathbf{u})$ a $\mathbf{m}$ splňující rovnici (3.1) platí

$$Dec(sk,x,Enc(pk,x,\mathbf{m})) = (\bar{\mathbf{m}},\bar{c})$$

takové, že

$$\mathbf{m} \equiv \bar{\mathbf{m}}/\bar{c} \pmod p$$

Poznámka. Pro ověření korektnosti budeme potřebovat, aby pro všechny prvky z podmnožin C,$\bar{C} \in R_q$ existovaly inverzní prvky. To přímo vyplývá z Lemma 7. Předpoklady lemmatu jsou splněny a pro všechny prvky c množiny C a $\bar{c}$ množiny $\bar{C}$ platí

$$\|c\|_\infty \leq 1 < \sqrt{q/2}, \quad \|\bar{c}\|_\infty \leq 2 < \sqrt{q/2},$$

tedy nenulové prvky množin C a $\bar{C}$ jsou invertibilní v R_q.

3.2 Jednorázové ověřitelné šifrování $Enc(pk,x,\mathbf{m})$

Tento algoritmus používá ověřovatel. Pracuje s pevně určenou množinou C, hashovací funkcí $H : R_q^{(2k+l)\times 4k} \times R^{2k+l} \times R^{2k+l} \to C$ a hodnotou

$$\sigma = 11 \cdot \max_{c \in C} \|c\|_1 \cdot \sqrt{kn(3+\lambda)} \in \mathbb{R}.$$

Za vstup bere daný veřejný klíč pk a prvky $x = (\mathbf{B},\mathbf{u})$ a $\mathbf{m}$, kde $\mathbf{B}$ a $\mathbf{m}$ jsou generovány uniformě náhodně pomocí algoritmů $Prav^{l\times k}(U_S,S)$ a $Prav^k(U_{R_q},R_q)$ a $\mathbf{u} = \mathbf{Bm} \mod p$. Prvek $\mathbf{m}$ je známý pouze ověřovateli. Cílem Algoritmu 5 je zašifrovat prvek $\mathbf{m} \in R_\lambda^k$, vyhovující rovnici (3.1).

Budeme značit $\mathbf{q} = (q,\ldots,q)^T \in \mathbb{N}^k$ a $\mathbf{p} = (p,\ldots,p)^T \in \mathbb{N}^l$.

Algoritmus je variací Algoritmu 3 z Kapitoly 2.2.1 o protokolu Fiat-Shamir. Jeho výsledku budeme říkat šifrovaný text.

Budeme používat značení z poznámky 2.2.1 pro operaci modulo vektorem $\mathbf{q}$.

Algorithm 5: Jednorázové ověřitelné šifrování $Enc(pk,x,\mathbf{m})$

Input: $pk = (a,t,p,q)$, $\mathbf{B} \in R_p^{l\times k}$, $\mathbf{u} \in R_p^l$, $\mathbf{m} \in S_\lambda^k$.
Output: Čtveřice $(\mathbf{v},\mathbf{w},c,\mathbf{z}) \in R^k \times R^k \times R \times R^{4k}$.

$a,b \leftarrow 1$;
$\mathbf{r}$, $\mathbf{e}$, $\mathbf{e}' \leftarrow S^k$;

$$\begin{pmatrix}\mathbf{v}\\ \mathbf{w}\end{pmatrix} \leftarrow \begin{pmatrix} pa\mathbf{I}_k & p\mathbf{I}_k & 0^{k\times k} & 0^{k\times k} \\ pt\mathbf{I}_k & 0^{k\times k} & p\mathbf{I}_k & \mathbf{I}_k \end{pmatrix} \begin{pmatrix}\mathbf{r}\\ \mathbf{e}\\ \mathbf{e}'\\ \mathbf{m}\end{pmatrix} \mod \begin{pmatrix}\mathbf{q}\\ \mathbf{q}\end{pmatrix};$$

while *b=1* **do**
  while *a=1* **do**
    $\mathbf{y} \leftarrow Prav^{4k}(D_{R,0,\sigma},R)$;
    $$c \leftarrow H\left(\mathbf{B'}, \begin{pmatrix}\mathbf{v}\\ \mathbf{w}\\ \mathbf{u}\end{pmatrix}, \begin{pmatrix} pa\mathbf{I}_k & p\mathbf{I}_k & 0^{k\times k} & 0^{k\times k} \\ pt\mathbf{I}_k & 0^{k\times k} & p\mathbf{I}_k & \mathbf{I}_k \\ 0^{l\times k} & 0^{l\times k} & 0^{l\times k} & \mathbf{B}\end{pmatrix}\mathbf{y} \mod \begin{pmatrix}\mathbf{q}\\ \mathbf{q}\\ \mathbf{p}\end{pmatrix}\right);$$
    $$\mathbf{s} \leftarrow c \begin{pmatrix}\mathbf{r}\\ \mathbf{e}\\ \mathbf{e}'\\ \mathbf{m}\end{pmatrix};$$
    $\mathbf{z} \leftarrow \mathbf{s} + \mathbf{y}$;
    $a \leftarrow Prav\left(D\left[0 : \frac{D_{R^4k,0,\sigma}\mathbf{z}}{D_{R^4k,\mathbf{s},\sigma}\mathbf{z}}\right],\{0,1\}\right)$;
  end
  if $\|\boldsymbol{z}\|_\infty \leq 6\cdot\sigma$ **then**
    $b \leftarrow 0$
  end
  $a = 1$;
end
return $g = (\boldsymbol{v},\boldsymbol{w},c,\boldsymbol{z})$

Poznámka. Smysl nastavení požadavků na průběh algoritmu a vstupních hodnot je součástí pravděpodobnostní analýzy v důkazu bezpečnosti zkoumané metody, který vynecháváme.

3.3 Jednorázové ověření $V(pk,x,g)$

Algoritmus **V** slouží k ověření, že šifrovaný text g lze získat pomocí **Enc**, pokud do něj dosadíme parametry $x \in R^{k\times l} \times R^k$ a pk.

Algoritmus 5 vrací čtveřici $g = (\mathbf{v},\mathbf{w},c,\mathbf{z})$ takovou, že $\|\mathbf{z}\|_\infty \leq 6{\cdot}\sigma$ a c je výsledkem hashovací funkce H po dosazení hodnoty $(\mathbf{B'},(\mathbf{v},\mathbf{w},\mathbf{u})^T,\mathbf{B'y} \mod (\mathbf{q},\mathbf{q},\mathbf{p})^T)$. Obě tyto podmínky musí Algoritmus 6 ověřit. Protože dokazující nemá přístup k hodnotě $\mathbf{y} \in R^{4k}$ použité v dané funkci v průběhu Algoritmu 5, použijeme Lemma 12, podle kterého víme, že platí

$$\mathbf{B'y} \mod \begin{pmatrix}\mathbf{q}\\ \mathbf{q}\\ \mathbf{p}\end{pmatrix} = \left(\mathbf{B'z} - c\begin{pmatrix}\mathbf{v}\\ \mathbf{w}\\ \mathbf{u}\end{pmatrix}\right) \mod \begin{pmatrix}\mathbf{q}\\ \mathbf{q}\\ \mathbf{p}\end{pmatrix}.$$

Algorithm 6: Jednorázové ověření $V(pk,x,g)$

Input: Veřejný klíč $pk = (a,t,p,q)$, matice $\mathbf{B} \in R_p^{l\times k}$, vektor $\mathbf{u} \in R_p^l$, čtveřice $g = (\mathbf{v},\mathbf{w},c,\mathbf{z})$.
Output: Prvek množiny $\{0,1\}$
if $\|\boldsymbol{z}\|_\infty > 6 \cdot \sigma$ **then**
  return *0*
end
if $c \neq H\left(\boldsymbol{B'}, \begin{pmatrix}\boldsymbol{v}\\ \boldsymbol{w}\\ \boldsymbol{u}\end{pmatrix}, \begin{pmatrix}pa\boldsymbol{I}_k & p\boldsymbol{I}_k & 0^{k\times k} & 0^{k\times k}\\ pt\boldsymbol{I}_k & 0^{k\times k} & p\boldsymbol{I}_k & \boldsymbol{I}_k\\ 0^{l\times k} & 0^{l\times k} & 0^{l\times k} & \boldsymbol{B}\end{pmatrix}\boldsymbol{z} - c\begin{pmatrix}\boldsymbol{v}\\ \boldsymbol{w}\\ \boldsymbol{u}\end{pmatrix} \mod \begin{pmatrix}\boldsymbol{q}\\ \boldsymbol{q}\\ \boldsymbol{p}\end{pmatrix}\right)$ **then**
  return *0*
end
return *1*

Vlastnost, že pro dané g je výsledek Algoritmu 6 roven jedné označíme (V).

Tvrzení 13. *Popisovaná kryptografická metoda (Kg,Enc,V,Dec) je kompletní. To znamená, že pro všechny dvojice klíčů $(sk,pk) \leftarrow Kg$ a pro každé zadání $x = (\boldsymbol{B},\boldsymbol{u})$ a $\boldsymbol{m}$ splňující rovnici* (3.1) *platí, že*

$$V(pk,x,Enc(pk,x,\boldsymbol{m})) = 1.$$

Důkaz tohoto tvrzení plyne přímo z popisu Algoritmů 5 a 6 a lemmatu 12.

3.4 Jednorázové dešifrování $Dec(sk,x,g)$

Toto je poslední používaný algoritmus. Bude jej používat dokazující. Pracujeme se známou konstantou $J = \max_{c,c'\in C} \|c - c'\|_1$.

Algorithm 7: Jednorázové dešifrování $Dec(sk,x,g)$

Input: Prvek sk, matice $\mathbf{B}$, vektor $\mathbf{u}$, šifrovaný text $g = (\mathbf{v},\mathbf{w},c,\mathbf{z})$.
Output: $(\bar{\mathbf{m}},\bar{c}) \in R^k \times \bar{C}$, pro které platí $\|\bar{\mathbf{m}}\|_\infty < \frac{q}{2J}$, nebo $False$, pokud vstup neodpovídá podmínce (V).

```
if V(pk,x,g) = 1 then
    while True do
        c' ← C \ {c};
        c̄ ← c − c';
        m̄ ← (w − sk · v)c̄ mod q;
        if ‖m̄‖∞ < q/(2J) then
            m̄ ← m̄ mod p;
            return (m̄,c̄);
        end
    end
end
return False
```

Dokazující se správným soukromým klíčem sk dosadí tento klíč do vstupu algoritmu společně se zadanými x a g, které získal od ověřovatele. Výstup Algoritmu 7, $(\bar{\mathbf{m}},\bar{c})$, poté předá ověřovateli. Pokud výstup splňuje rovnici (3.2), považuje to ověřovatel za důkaz, že dokazující vlastní soukromý klíč sk.

Na začátku Algoritmu 7 dokazující ověří, zda šifrovaný text splňuje podmínku (V). O textech, které podmínku nesplňují nejsme obecně schopni nic říci. Jde vlastně o ověření, zda ověřovatel má přístup k veřejnému klíči pk.

Nyní zformulujeme a ukážeme Tvrzení 3.1. z článku Lyubashevsky a Neven (2017).

Tvrzení 14. *Nechť (s_1,s_2) a (a,t,p,q) jsou hodnoty zavedené v části 3.1. Nechť pro $v,w \in R_q$ existují $\bar{r},\bar{e},\bar{e}',\bar{m} \in R_q$ a $\bar{c} \in \bar{C}$ a $J = \max_{c,c' \in C} \|c - c'\|_1$, takové, že platí*

$$\begin{pmatrix} pa & p & 0 & 0 \\ pt & 0 & p & 1 \end{pmatrix} \begin{pmatrix} \bar{r} \\ \bar{e} \\ \bar{e}' \\ \bar{m} \end{pmatrix} = \bar{c} \begin{pmatrix} v \\ w \end{pmatrix} \mod q$$

a zároveň

$$\|p(\bar{r}s_2 + \bar{e}' + \bar{e}s_1) + \bar{m}\|_\infty < \frac{q}{2J},$$

Potom platí

1. $\|(w - vs_1)\bar{c} \mod q\|_\infty < \frac{q}{2J}$
2. *Pro každé $\bar{c}' \in \bar{C}$ takové, že*

$$\|(w - vs_1)\bar{c}' \mod q\|_\infty < \frac{q}{2J},$$

platí

$$((w - vs_1)\bar{c}' \mod q)/\bar{c}' \mod p = \bar{m}/\bar{c} \mod p$$

Důkaz. První část dokážeme snadno dosazením a použitím předpokladu tvrzení

$$\|(w - vs_1)\bar{c} \mod q\|_\infty = \|p(\bar{r}s_2 + \bar{e'} + \bar{e}s_1) + \bar{m}\|_\infty < \frac{q}{2J}.$$

K důkazu druhé části připomeňme, že všechny prvky množiny C mají inverzní prvek v R_q podle Lemmatu 7. Prvky množiny C tedy můžeme dělit. Nejprve ukážeme

$$\begin{aligned}(w - vs_1)\bar{c}\bar{c}' \mod q \mod p &= (p(\bar{r}s_2 + \bar{e}' + \bar{e}s_1) + \bar{m})\bar{c}' \mod q \mod p \\ &= p(\bar{r}s_2 + \bar{e}' + \bar{e}s_1)\bar{c}' + \bar{m}\bar{c}' \mod p \\ &= \bar{m}\bar{c}' \mod p\end{aligned} \tag{3.4}$$

kde druhá rovnost platí z předpokladu $\|p(\bar{r}s_2 + \bar{e'} + \bar{e}s_1) + \bar{m}\|_\infty < \frac{q}{2J}$, nerovnosti $\|\bar{c}'\|_1 < J$ a nerovnosti (2.1), tedy

$$\|(p(\bar{r}s_2 + \bar{e'} + \bar{e}s_1) + \bar{m})\bar{c}'\|_\infty < \frac{q}{2}.$$

Dále budeme počítat

$$\begin{aligned}(((w - vs_1)\bar{c}' \mod q)/\bar{c}') \mod p &= ((w - vs_1)\bar{c}' \mod q) \cdot \bar{c}/(\bar{c}\bar{c}') \mod p \\ &= ((w - vs_1)\bar{c}\bar{c}' \mod q)/(\bar{c}\bar{c}') \mod p \\ &= ((w - vs_1)\bar{c}\bar{c}' \mod q \mod p)/(\bar{c}\bar{c}') \mod p \\ &= \bar{m}\bar{c}'/(\bar{c}\bar{c}') \mod p \\ &= \bar{m}/\bar{c} \mod p,\end{aligned}$$

kde druhá rovnost plyne z předpokladu $\|(w - vs_1)\bar{c}' \mod q\|_\infty < \frac{q}{2J}$, protože násobení prvkem $\bar{c} \in \bar{C}$ v tomto případě nezpůsobuje redukci modulo q, a třetí rovnost vychází ze vztahu (3.4). □

Nyní dokážeme, že metoda je korektní.

Tvrzení 15. *Pro všechny* $x = (\boldsymbol{B},\boldsymbol{u}) \in R_p^{l\times k} \times R_p^l$ *a* $\boldsymbol{m} \in R_p^k$ *splňující rovnost* (3.1) *a pro všechny dvojice* $(sk,pk) \leftarrow Kg$ *platí*

$$Dec(sk,x,Enc(pk,x,\boldsymbol{m})) = (\bar{\boldsymbol{m}},\bar{c}),\ \boldsymbol{m} \equiv \bar{\boldsymbol{m}}/\bar{c} \pmod p.$$

Důkaz. K důkazu korektnosti budeme potřebovat aby byly splněny předpoklady Tvrzení 14. Zvolíme $(\bar{\mathbf{r}},\bar{\mathbf{e}},\bar{\mathbf{e}}',\bar{\mathbf{m}}) = (\mathbf{r},\mathbf{e},\mathbf{e}',\mathbf{m})$ a $\bar{c} = 1$.

Víme, že $\mathbf{m} \in R_p^k$, tedy $\|\mathbf{m}\|_\infty \leq p$, $s_1,s_2 \in S$ a proto platí $\|s_1\|_1,\|s_2\|_1 \leq k_2$ a $\mathbf{r},\mathbf{e},\mathbf{e}' \in S^k$, potom $\|\mathbf{r}\|_\infty,\|\mathbf{e}\|_\infty,\|\mathbf{e}'\|_\infty \leq 1$. Pomocí nerovnosti (2.1) spočítáme

$$\|\mathbf{r}s_2\|_\infty \leq \|\mathbf{r}\|_\infty \cdot \|s_2\|_1 \leq k_2, \quad \|\mathbf{e}s_1\|_\infty \leq \|\mathbf{e}\|_\infty \cdot \|s_1\|_1 \leq k_2$$

Potom platí nerovnost

$$\begin{aligned}\|p(\mathbf{r}s_2 + \mathbf{e}' + \mathbf{e}s_1) + \mathbf{m}\|_\infty &\leq p\|(\mathbf{r}s_2 + \mathbf{e}' + \mathbf{e}s_1)\|_\infty + \|\mathbf{m}\|_\infty \\ &\leq p(\|\mathbf{r}s_2\|_\infty + \|\mathbf{e}'\|_\infty + \|\mathbf{e}s_1\|_\infty) + \|\mathbf{m}\|_\infty \\ &\leq p(2k_2 + 1) + p \\ &< \frac{q}{2J},\end{aligned} \tag{3.5}$$

Podmínky Tvrzení 14 jsou tedy splněny. V průběhu Algoritmu 7 probíhá výpočet hodnoty $\bar{\mathbf{m}}$ a následná kontrola, zda platí

$$\|\bar{\mathbf{m}}\|_\infty = \|(\mathbf{w} - sk \cdot \mathbf{v})\bar{c} \mod q\|_\infty < \frac{q}{2J}.$$

Algoritmus vrátí dvojici $(\bar{\mathbf{m}},\bar{c})$, jen v tom případě, že tato nerovnost platí. Podmínka v druhém bodu Tvrzení 14 je tedy pro výstup Algoritmu 7 splněna a platí

$$((\mathbf{w} - \mathbf{v}s_1)\bar{c}' \mod q)/\bar{c}' \mod p = \bar{\mathbf{m}}/\bar{c} \mod p = \mathbf{m}/1,$$

neboť všechny operace jsou počítány po složkách. Dále vypočítáme

$$\mathbf{B}\bar{\mathbf{m}} \equiv \mathbf{B}\bar{\mathbf{m}}(\bar{c}^{-1}\bar{c}) \equiv \mathbf{B}\mathbf{m}\bar{c} \equiv \mathbf{u}\bar{c} \pmod p.$$

Výsledné hodnoty odpovídají rovnici (3.2).

Tímto jsme dokázali korektnost metody (Kg,Enc,V,Dec). □

Poznamenejme, že nenulové prvky množin C a $\bar{C}$ jsou sice invertibilní, výpočet jejich inverzu je však mnohdy složitý. Konečný výpočet hodnoty $\mathbf{m}$ z prvků $\bar{\mathbf{m}}$ a $\bar{c}$ se proto neprovádí.

Délka průběhu dešifrovacího algoritmu je z konstrukce neomezená. V článku (Lyubashevsky a Neven, 2017, str. 311) je ukázáno jak se vypočítá předpokládaný počet prošlých cyklů, před nalezením odpovídajícího výsledku.

Závěr

Popsali jsme metodu jednorázového šifrování, která souží k důkazu znalosti soukromého klíče v ověření s nulovou znalostí publikovanou v článku Lyubashevsky a Neven (2017), kde byla dokázána také její bezpečnost.

Práce obsahuje popis vlastností polynomiálních faktorokruhů R a R_q. Tyto okruhy jsou ilustrovány v příkladu 1.2. Dokázali jsme Lemma 6 o ireducibilitě polynomů $x^{2^\kappa} \pm r$ v R_q pro specificky zadané parametry q a n, které je ve zpracovávaném článku pouze citováno a je klíčové pro navazující Lemma 7, o invertibilitě prvků malých norem v R_q, které využívá výsledný dešifrovací algoritmus. Dále jsme vyslovili a dokázali Lemma 8 o maximové normě násobku dvou prvků z $S_\lambda^{(k)}$ a Tvrzení 9 o správnosti výsledku algoritmu LWE. V neposlední řadě jsme sepsali a dokázali Lemma 11 definující diskrétní pravděpodobnostní prostor $(M,D_{M,\mathbf{c},\sigma})$ a popsali souvislost Tvrzení 14 s korektností algoritmu *Dec* pomocí Tvrzení 15.

Hlavním přínosem této práce je zjednodušený popis průběhu daných částí metody jednorázového ověření z dokumentu Lyubashevsky a Neven (2017).

Poznamenejme, že bezpečnost popisované metody lze dokázat, a metodu můžeme využít k ověření vlastnictví soukromého klíče. Důkaz bezpečnosti není předmětem této práce.

Seznam použité literatury

Drápal, A. Teorie čísel. https://www2.karlin.mff.cuni.cz/~drapal/teorie_cisel.pdf. Navštíveno: červenec 2022.

Kala, V. (2021). Komutativní okruhy. http://karlin.mff.cuni.cz/~kala/files/KO-2021.pdf. Navštíveno: červenec 2022.

Kroutil, J. (2019). Krátké invertibilní prvky v cyklotomických okruzích.

Lyubashevsky, V. (2012). Lattice signatures without trapdoors. In *Advances in Cryptology – EUROCRYPT 2012*, Lecture Notes in Computer Science, pages 738–755, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 3642290108.

Lyubashevsky, V. a Neven, G. (2017). One-shot verifiable encryption from lattices. In *Advances in Cryptology – EUROCRYPT 2017*, Lecture Notes in Computer Science, pages 293–323. Springer International Publishing, Cham. ISBN 9783319566191.

Lyubashevsky, V., Peikert, C. a Regev, O. (2013). On ideal lattices and learning with errors over rings. *JOURNAL OF THE ACM*, **60**(6), 1–35. ISSN 0004-5411.

Stanovský, D. (2021). Učební text algebra 2020/21. http://karlin.mff.cuni.cz/~kala/2021alg/algebra21.pdf. Navštíveno: červen 2022.

Žemlička, J. Samoopravné kódy. https://www2.karlin.mff.cuni.cz/~zemlicka/21-22/SoKn.pdf. Navštíveno: červenec 2022.