Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Matemaatika ja statistika instituut

Brett Johannes Hankewitz

Diskreetse logaritmi probleemi entroopiline teisendus ja selle rakendused

Matemaatika

Bakalaureusetöö (9 EAP)

Juhendajad: PhD Jan Villemson, prof. Valdis Laan

Tartu 2023

DISKREETSE LOGARITMI PROBLEEMI ENTROOPILINE TEISENDUS JA SELLE RAKENDUSED

Bakalaureusetöö

Brett Johannes Hankewitz

Lühikokkuvõte

2023. aastal avaldas D. Gligoroski artikli, kus ta konstrueeris uue algebralise struktuuri nimega entropoid, mille abil oleks võimalik olemasolevaid krüptograafilisi skeeme teisendada postkvant-turvalisteks. Käesolevas bakalaureusetöös tutvustame entropoide ja seletame lahti vastava teisenduse. Anname ülevaate entropoidide baasteooriast, anname edasi vajalikke krüptograafilisi teadmisi ning kirjeldame entroopilist teisendust ja selle rakendusi.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria

Märksõnad: Krüptograafia, rühmad (matemaatika), automorfismid.

ENTROPIC LIFT OF THE DISCRETE LOGARITHM PROBLEM AND ITS APPLICATIONS

Bachelor thesis

Brett Johannes Hankewitz

Abstract

In the year 2023 D. Gligoroski published an article in which he constructed a new algebraic structure called an entropoid, with which it could be possible to transform existing cryptographic schemes to make them post-quantum secure. In this bachelor's thesis we will introduce these entropoids and explain the respective transformation. We will give an overview of the basic theory of entropoids, convey necessary cryptographic knowledge, and describe the

essence of Entropic Lift and its applications.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory

Key Words: Cryptography, groups (math.), automorphisms.

Sisukord

Sissejuhatus

2023. aastal avaldas D. Gligoroski artikli, milles kirjeldas viisi transformeerida arvutuslikult keeruline ülesanne kujule, mille põhjal saaks teha krüptograafilisi skeeme, mida kvantarvuti ei suudaks efektiivselt murda. Vastav teisendus põhineb entropoidi-nimelisel algebralisel struktuuril, mis kaldub eemale tavapärasest rühmateoreetilisest vaatest, mis on krüptograafias laialdaselt levinud. Antud töö on referatiivne ülevaade sellest teisendusest ning selle rakendamisest uute krüptograafiliste skeemide loomisel. Suurem osa tööst põhineb artiklil [1].

Töö esimeses peatükis esitame entropoidide baasteooria. Defineerime uue tehte, millega saab selle algebralise struktuuri konstrueerida. Esitame entropoidide omadused ja toome näite konkreetsest entropoidi struktuurist. Samuti kirjeldame astmeindeksite teooriat, mis mängib samuti suurt rolli entroopilises teisenduses.

Töö teises peatükis esitame vajalikke krüptograafilisi teadmisi, mis kolmandas peatükis ette tulevad. Selgitame, kuidas töötab asümmeetriline krüptograafia ja defineerime baasprobleemid, mille põhjal krüptograafilisi skeeme saab konstrueerida.

Töö kolmandas peatükis esitame diskreetse logaritmi probleemi entroopilise teisenduse definitsiooni. Tutvustame, kuidas see teisendus töötab ja kuidas sellega olemasolevaid krüptograafilisi skeeme teisendada. Toome näiteid kindlate skeemide teisendamistest (kusjuures näitame, et entroopiline teisendus ei taga tegelikult postkvant-turvalisust) ja esitame algoritmid, millega teisendatud diskreetse logaritmi probleemi lahendada.

1 Entropoidide teooria

Antud peatükis anname ülevaate entropoidist kui algebralisest struktuurist ja tutvustame töös ette tulevaid matemaatilisi mõisteid.

1.1 Vajalikud eelteadmised

Olgu $(G, \cdot)$ kommutatiivne rühm ühikelemendiga 1_G.

Definitsioon 1. [5, lk 84] Rühma G nimetatakse **tsüklililiseks**, kui leidub selline element $g \in G$, et $G = \langle g \rangle$, kus

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Elementi g nimetatakse tsüklilise rühma **tekitajaks**.

Definitsioon 2. [5, lk 86] Olgu $g \in G$. Kui $|\langle g \rangle| = n \in \mathbb{N}$, siis öeldakse, et elemendi g **järk** on n.

Definitsioon 3. [1, lk 2] Olgu $a, b \in G$. Öeldakse, et elemendid a ja b on **sõltumatud**, kui $\langle a \rangle \cap \langle b \rangle = \{1_G\}$.

Definitsioon 4. [1, lk 1, 2] Kujutus $\alpha : G \to G$ on **automorfism**, kui

- α on bijektiivne;
- $\forall x, y \in G$, $\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y)$.

Definitsioon 5. [1, lk 2] Automorfism $T : G \to G$ on **involutiivne**, kui

$$\forall x \in G,\ T(T(x)) = T^{(2)}(x) = x.$$

Kuna T on automorfism, siis saab järeldada järgmise omaduse:

Lause 1. [1, lk 2] *Olgu $T : G \to G$ automorfism. Siis iga $x \in G$ ja $j \in \mathbb{N}$ korral*

$$(T(x))^j = T(x^j).$$

1.2 Entropoid ja selle omadused

Tutvustame uut algebralist struktuuri nimega entropoid ja selle omadusi. See struktuur mängib edaspidises töös suurt rolli krüptograafiliste skeemide kvant-turvaliseks teisendamisel.

Edaspidiselt eeldame, et $(G, \cdot)$ on lõplik kommutatiivne rühm tehtega $\cdot$ ja ühikelemendiga 1_G. Samuti eeldame, et $|G| = q^2$, kus arvu q saab esitada ν erineva algarvu korrutisena ehk $q = q_1 \dots q_\nu$ (järjestatud mittekahanevas järjekorras) ja kõige väiksem tegur $q_1 > 2$ [1, lk 1].

Eeldame ka, et rühm G ei ole tsükliline, aga on tekitatud kahe sõltumatu elemendi $g_1, g_2 \in G$ poolt, s.t. iga $x \in G$ korral leiduvad $i, j \in \mathbb{Z}_q$ nii, et $x = g_1^i \cdot g_2^j$. Teisisõnu rühm G on kahe maksimaalse tsüklilise alamrühma $G_1 = \langle g_1 \rangle$ ja $G_2 = \langle g_2 \rangle$ otsekorrutis ehk

$$G \cong G_1 \times G_2,$$

kus $|G_1| = |G_2| = q$ [1, lk 1].

Selliselt defineeritud rühmal on järgmine omadus.

Lause 2. [1, lk 1] *Iga $x \in G$ korral leiduvad üheselt määratud $i, j \in \mathbb{Z}_q$ nii, et $x = g_1^i \cdot g_2^j$.*

Defineerime nüüd uue algebralise struktuuri: entropoidi.

Definitsioon 6. [1, lk 2] Olgu $T : G \to G$ involutiivne automorfism. Defineerime binaarse tehte $\boxplus$ hulgal G võrdusega

$$x \boxplus y = x \cdot T(y),$$

kus $x, y \in G$. Kutsume algebralist struktuuri $\mathbb{E}_{q^2} = (G, \boxplus, \cdot)$ lõplikuks **entropoidiks** järguga q^2.

Lause 3. [1, lk 2] *Olgu $T : G \to G$ involutiivne automorfism. Olgu $h \in G$ selline element, et h ja $T(h)$ on sõltumatud elemendid, mille järk on q. Siis iga $x \in G$ korral leidub selline üheselt määratud paar $(i, j) \in \mathbb{Z}_q \times \mathbb{Z}_q$ nii, et*

$$x = h^i \cdot T(h^j).$$

Tõestus. [1, lk 2] Olgu $H_1 = \langle h \rangle$ elemendi h poolt tekitatud alamrühm ja $H_2 = \langle T(h) \rangle$ elemendi $T(h)$ poolt tekitatud alamrühm. Kuna h ja $T(h)$ on sõltumatud elemendid, siis $H_1 \cap H_2 = \{1_G\}$. Samuti $|H_1| = |H_2| = q$, seega $G \cong H_1 \times H_2$. Sellest tulenevalt järeldub paari (i, j) olemasolu ja üheselt määratus lausest 2. □

Toome välja mõned tehte $\boxplus$ omadused.

Lause 4. [1, lk 2]

- *Tehe $\boxplus$ on üldiselt mittekommutatiivne.*
- *Element 1_G käitub kui parempoolne nullelement rühmoidis $(G, \boxplus)$, s.t. iga $x \in G$ korral $x \boxplus 1_G = x$.*
- *Vasakult poolt käitub element 1_G involutsioonina T, s.t. iga $x \in G$ korral $1_G \boxplus x = T(x)$.*
- *Tehte $\boxplus$ pöördtehe $\boxminus$ on defineeritud järgmiselt: iga $x, y \in G$ korral $x \boxminus y = x \cdot T(y^{-1}) = x \boxplus y^{-1}$. Seega, kui $x \boxminus y = z$, siis $x = z \boxplus y$.*

Nagu ka rühmal G, on ka võimalik defineerida entropoidi $\mathbb{E}_{q^2}$ tekitaja.

Definitsioon 7. [1, lk 2] Element $g \in G$ on **entropoidi $\mathbb{E}_{q^2}$ tekitaja**, kui g ja $T(g)$ on sõltumatud elemendid järguga q.

Leidub efektiivne algoritm, mille väljundiks on entropoidi $\mathbb{E}_{q^2}$ tekitaja. Olgu meil entropoid $\mathbb{E}_{q^2} = (G, \boxplus, \cdot)$ ja olgu meil teada element q algarvude korrutisena $q = q_1 \dots q_\nu$. Valime suvalise elemendi $g \in G$. Leiame hulgad

$$\mathcal{B} = \{b \mid b = g^{(q^2/q_i)}, i \in \{1, \dots, \nu\}\}$$

ja

$$\mathcal{B}_T = \{b \mid b = T(g)^{(q^2/q_i)}, i \in \{1, \dots, \nu\}\}.$$

Kontrollime, kas ühikelement 1_G kuulub hulka $\mathcal{B}$ või $\mathcal{B}_T$. Kui 1_G kuulub vähemalt ühte nendest hulkadest, siis valime uue elemendi $g \in G$, mida pole veel vaadatud, ja alustame algoritmiga uuesti. Kui 1_G ei kuulu kumbagi hulka, siis kontrollime, kas $\mathcal{B} \cap \mathcal{B}_T = \emptyset$. Kui nende ühisosa ei ole tühi hulk, siis liigume jälle algoritmi algusesse tagasi. Vastasel juhul olemegi leidnud entropoidi $\mathbb{E}_{q^2}$ tekitaja g [1, lk 3].

Tõestame, et see algoritm on korrektne.

Lemma 1. [1, lk 2] *Kui g on väljund antud algoritmil, siis g on entropoidi $\mathbb{E}_{q^2}$ tekitaja.*

Tõestus. [1, lk 2] Tuletame meelde, et $G \cong G_1 \times G_2$, kus rühmade G_1 ja G_2 järgud on q. Hulk $\mathcal{B}$ ja ühikelemendi olemasolu kontroll selles hulgas tagavad, et g on maksimaalse tsüklilise alamrühma, mille järk on q, tekitaja, s.t. $|\langle g \rangle| = q$. Analoogiliselt, hulk $\mathcal{B}_T$ ja ühikelemendi kontroll tagavad, et $|\langle T(g) \rangle| = q$. Viimane samm kontrollib, kas g ja $T(g)$ on üksteisest sõltumatud elemendid, mis Definitsiooni 7 kohaselt on tarvilik tingimus, et g saaks olla entropoidi $\mathbb{E}_{q^2}$ tekitaja. □

1.3 Näide konkreetsest entropoidi struktuurist

Kindel näide paragraafi 1.2 alguses defineeritud rühmast $(G, \cdot)$ on multiplikatiivne rühm $C(n, 2)$ ehk pööratavate $n \times n$ ringmaatriksite rühm üle lõpliku korpuse $\mathbb{F}_2$ [1, lk 7].

Definitsioon 8. [6, Definitsioon 13.2.29, lk 504] $n \times n$ maatriks $C = (c_{ij})$ on **ringmaatriks**, kui see on kujul

$$C = \begin{pmatrix} c_0 & c_1 & \dots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-3} & c_{n-2} \\ c_{n-2} & c_{n-1} & \dots & c_{n-4} & c_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_1 & c_2 & \dots & c_{n-1} & c_0 \end{pmatrix}.$$

Sellist maatriksi tähistatakse $\mathrm{circ}(c_0, \dots, c_{n-1})$.

Järgmine tulemus on teada rühma $C(n, 2)$ elementide arvu kohta.

Lause 5. [6, Järeldus 13.2.34, lk 505] *Olgu n paaritu arv. Siis*

$$|C(n,2)| = \prod_{j=1}^{r} (2^{m_j} - 1),$$

kus $m_1, \dots, m_r$ on polünoomi $x^n - 1$ üle korpuse $\mathbb{F}_2$ taandumatute tegurite astmed.

Meid huvitavad juhud, kus n on algarv, $|C(n,2)| = q^2$, $q = 2^{\frac{n-1}{2}} - 1$. Samuti, kui arv q esitada ν algarvu korrutisena $q = q_1 q_2 \dots q_\nu$ (järjestatud mittekahanevas järjekorras), siis algarvude arv ν peaks olema võimalikult väike, aga suurim algtegur $q_\nu > q^{1/2}$. Kõik need tingimused on täidetud, kui valida näiteks $n = 167$ [1, lk 7].

Involutiivseks automorfismiks $T : C(n,2) \to C(n,2)$ sobib maatriksi transponeerimistehe. Kui maatriksile $A = \mathrm{circ}(a_0, \dots, a_{n-1}) \in C(n,2)$ seada vastavusse polünoom

$$a_0 + a_1 x + a_2 x^2 + \dots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1},$$

siis maatriksile a^T vastab polünoom

$$a_0 + a_{n-1} x + a_{n-2} x^2 + \dots + a_2 x^{n-2} + a_1 x^{n-1}$$

[1, lk 8].

Elemente ringis $C(n, 2)$ saab esitada selliste polünoomidena järgmise lemma alusel.

Lemma 2. [6, Lemma 13.2.31, lk 505] *Olgu F korpus. Kõikide $n \times n$ ringmaatriksite ring üle korpuse F on isomorfne ringiga $R = F[x]/(x^n - 1)$. Selle isomorfismi realiseerib kujutus*

$$\varphi(circ(c_0, \ldots, c_{n-1})) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}.$$

1.4 Astmeindeks

Defineerime astmeindeksi ning esitame sellega seonduvad tehted ja omadused. Astmeindeks on oluline osa entroopilisest teisendusest.

Definitsioon 9. [1, lk 3] Kutsume kahedimensioonilisi astendajaid $X = (x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$ **astmeindeksiteks**. Defineerime iga $g \in G$ korral astendamise astmeindeksiga $X = (x_1, x_2)$ võrdusega

$$g^X = g^{(x_1, x_2)} = g^{x_1} \cdot T(g)^{x_2}.$$

Paneme tähele, et kuna T on automorfism, siis $g^X = g^{x_1} \boxplus g^{x_2}$.

Definitsioon 10. [1, lk 3] Olgu $X = (x_1, x_2)$ ja $Y = (y_1, y_2)$ astmeindeksid. Defineerime järgmised tehted astmeindeksitega:

- **liitmine**: $X + Y = (x_1, x_2) + (y_1, y_2) = ((x_1 + y_1), (x_2 + y_2))$;
- **lahutamine**: $X - Y = (x_1, x_2) - (y_1, y_2) = ((x_1 - y_1), (x_2 - y_2))$;
- **korrutamine**: $XY = (x_1, x_2) \times (y_1, y_2) = ((x_1 y_1 + x_2 y_2), (x_1 y_2 + x_2 y_1))$;
- **jagamine**: $\frac{X}{Y} = \frac{(x_1, x_2)}{(y_1, y_2)} = \left(\frac{x_1 y_1 - x_2 y_2}{y_1^2 - y_2^2}, \frac{x_2 y_1 - x_1 y_2}{y_1^2 - y_2^2}\right)$, eeldusel, et $\text{SÜT}(y_1^2 - y_2^2, q) = 1$.

Paneme tähele, et astmeindeksite liitmine ja korrutamine on kommutatiivsed, sest $\mathbb{Z}_q$ on korpus.

Lause 6. [1, lk 3] *Olgu $X = (x_1, x_2)$ ja $Y = (y_1, y_2)$ astmeindeksid. Iga $h \in G$ korral kehtivad järgmised seosed:*

- $h^X \cdot h^Y = h^{(X+Y)}$;
- $h^X \cdot (h^Y)^{-1} = h^{(X-Y)}$;
- $(h^X)^Y = h^{XY}$.

$h^{\frac{X}{Y}}$ väärtuse leidmiseks lahendatakse järgmine probleem: antud h, X ja Y korral leida lahend $h^{\frac{X}{Y}}$ võrrandile

$$\left(h^{\frac{X}{Y}}\right)^Y = h^X.$$

Tõestus. Tõestame väite $h^{\frac{X}{Y}}$ leidmise kohta. Olgu $h \in G$ ja olgu $X = (x_1, x_2)$, $Y = (y_1, y_2)$ astmeindeksid. Eeldame ka, et $\text{SÜT}(y_1^2 - y_2^2, q) = 1$, vastasel juhul ei ole $\frac{X}{Y}$ määratud. Näitame, et võrrand $\left(h^{\frac{X}{Y}}\right)^Y = h^X$ on lahenduv.

Teame, et

$$\frac{X}{Y} = \frac{(x_1, x_2)}{(y_1, y_2)} \equiv \left(\frac{x_1y_1 - x_2y_2}{y_1^2 - y_2^2}, \frac{x_2y_1 - x_1y_2}{y_1^2 - y_2^2}\right),$$

seega astmeindeksi definitsiooni kasutades saame, et

$$h^{\frac{X}{Y}} = h^{\left(\frac{x_1y_1 - x_2y_2}{y_1^2 - y_2^2}, \frac{x_2y_1 - x_1y_2}{y_1^2 - y_2^2}\right)} = h^{\frac{x_1y_1 - x_2y_2}{y_1^2 - y_2^2}} \cdot T(h)^{\frac{x_2y_1 - x_1y_2}{y_1^2 - y_2^2}}.$$

Kasutades lauset 1, saame, et

$$h^{\frac{x_1y_1 - x_2y_2}{y_1^2 - y_2^2}} \cdot T(h)^{\frac{x_2y_1 - x_1y_2}{y_1^2 - y_2^2}} = h^{\frac{x_1y_1 - x_2y_2}{y_1^2 - y_2^2}} \cdot T\left(h^{\frac{x_2y_1 - x_1y_2}{y_1^2 - y_2^2}}\right).$$

Jällegi, astmeindeksi definitsioonist saame, et

$$\begin{aligned}\left(h^{\frac{X}{Y}}\right)^Y &= \left(h^{\frac{x_1y_1-x_2y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1-x_1y_2}{y_1^2-y_2^2}}\right)\right)^{(y_1,y_2)} \\ &= \left(h^{\frac{x_1y_1-x_2y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1-x_1y_2}{y_1^2-y_2^2}}\right)\right)^{y_1} \cdot T\left(h^{\frac{x_1y_1-x_2y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1-x_1y_2}{y_1^2-y_2^2}}\right)\right)^{y_2}.\end{aligned}$$

Rühma elemendi astendamise omadusi ja lauset 1 kasutades saame, et

$$\begin{aligned}\left(h^{\frac{x_1y_1-x_2y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1-x_1y_2}{y_1^2-y_2^2}}\right)\right)^{y_1} &= h^{\frac{x_1y_1^2-x_2y_1y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1-x_1y_2}{y_1^2-y_2^2}}\right)^{y_1} \\ &= h^{\frac{x_1y_1^2-x_2y_1y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1^2-x_1y_1y_2}{y_1^2-y_2^2}}\right)\end{aligned}$$

ning analoogiliselt

$$T\left(h^{\frac{x_1y_1-x_2y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1-x_1y_2}{y_1^2-y_2^2}}\right)\right)^{y_2} = T\left(h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}}\right)\right).$$

Kuna T on involuutne automorfism, siis

$$\begin{aligned}T\left(h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}}\right)\right) &= T\left(h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}}\right) \cdot T\left(T\left(h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}}\right)\right) \\ &= T\left(h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}}\right) \cdot h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}}\end{aligned}$$

Seega

$$\left(h^{\frac{X}{Y}}\right)^Y = h^{\frac{x_1y_1^2-x_2y_1y_2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1^2-x_1y_1y_2}{y_1^2-y_2^2}}\right) \cdot T\left(h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}}\right) \cdot h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}}.$$

Kuna rühm G on kommutatiivne ja T on automorfism, siis

$$\begin{aligned}\left(h^{\frac{X}{Y}}\right)^Y &= h^{\frac{x_1y_1^2-x_2y_1y_2}{y_1^2-y_2^2}} \cdot h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1^2-x_1y_1y_2}{y_1^2-y_2^2}}\right) \cdot T\left(h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}}\right) \\ &= h^{\frac{x_1y_1^2-x_2y_1y_2}{y_1^2-y_2^2}} \cdot h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1^2-x_1y_1y_2}{y_1^2-y_2^2}} \cdot h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}}\right).\end{aligned}$$

Rühma elemendi astendamise omaduste põhjal

$$\begin{aligned}\left(h^{\frac{X}{Y}}\right)^Y &= h^{\frac{x_1y_1^2-x_2y_1y_2}{y_1^2-y_2^2}} \cdot h^{\frac{x_2y_1y_2-x_1y_2^2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1^2-x_1y_1y_2}{y_1^2-y_2^2}} \cdot h^{\frac{x_1y_1y_2-x_2y_2^2}{y_1^2-y_2^2}}\right) \\ &= h^{\frac{x_1y_1^2-x_1y_2^2}{y_1^2-y_2^2}} \cdot T\left(h^{\frac{x_2y_1^2-x_2y_2^2}{y_1^2-y_2^2}}\right) \\ &= h^{x_1} \cdot T\left(h^{x_2}\right) \\ &= h^{x_1} \cdot T(h)^{x_2} && \text{(lause 1)} \\ &= h^{(x_1,x_2)} && \text{(astmeindeksi def.)} \\ &= h^X.\end{aligned}$$

Teisi omadusi saab analoogiliselt tõestada. □

Lause 7. *Olgu astmeindeks $S = (s_1, s_2)$ selline, et $\mathrm{SÜT}(s_1^2 - s_2^2, q) = 1$. Siis kujutus $\sigma : G \to G$, $\sigma(x) = x^S$ on endomorfism, s.t. iga $x, y \in G$ korral $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$.*

Tõestus. Iga $x, y \in G$ korral

$$\begin{aligned}
\sigma(x \cdot y) &= (x \cdot y)^S && (\sigma \text{ def.}) \\
&= (x \cdot y)^{s_1} \cdot T((x \cdot y))^{s_2} && (\text{astmeindeksi def.}) \\
&= x^{s_1} \cdot y^{s_1} \cdot T(x^{s_2} \cdot y^{s_2}) && (\text{korrutise astendamine, lause 1}) \\
&= x^{s_1} \cdot y^{s_1} \cdot T(x^{s_2}) \cdot T(y^{s_2}) && (\text{automorfismi def.}) \\
&= x^{s_1} \cdot T(x^{s_2}) \cdot y^{s_1} \cdot T(y^{s_2}) && (\text{kommutatiivsus}) \\
&= x^{(s_1,s_2)} \cdot y^{(s_1,s_2)} && (\text{astmeindeksi def.}) \\
&= x^S \cdot y^S \\
&= \sigma(x) \cdot \sigma(y).
\end{aligned}$$

□

Märgime, et artiklis [1] on väidetud, et σ on automorfism, aga bijektiivsuse tõestamisel on seal lünki. Nimelt ei ole selge tõestuses oleva kahe esimese eraldi real oleva võrrandi samaväärsus.

2 Vajalikud krüptograafilised teadmised

Selles peatükis toome välja mõned vajalikud krüptograafilised teadmised, mis järgmises peatükis ette tulevad.

2.1 Asümmeetriline krüptograafia

Sümmeetriline ehk privaatse võtmega krüptograafia seeldab, et kaks osapoolt, kes soovivad üksteisele krüpteeritud sõnumeid saata, peavad varasemalt kokku leppima ühise privaatse võtme, mille abil sõnumeid krüpteerida ja dekrüpteerida. Selleks peavad nad varasemalt kokku saama, et vastav võti üksteisele turvaliselt edastada. Asümmeetriline ehk avaliku võtmega krüptograafia lihtsustab osapoolte tööd, eemaldades kokkusaamise vajaduse. Sõnumi saaja genereerib kaks võtit (pk, sk), mida kutsutakse vastavalt avalikuks ja privaatseks võtmeks. Sõnumi saatja kasutab saaja avalikku võtit, et sõnum krüpteerida, ning saaja kasutab oma privaatset võtit, et see sõnum dekrüpteerida [4, lk 375].

Kuna eesmärgiks on vältida kahe osapoole kokkusaamist, on vaja see saaja avalik võti kuidagi saatjale edastada. Abstraksel tasemel võib see toimida kahte moodi. Esimesel juhul, saaja (olgu ta nimi Alice) saab teada, et talle soovitakse sõnum saata (olgu saatja nimi Bob). Alice genereerib oma võtmed (pk, sk) ja saadab võtme pk Bobile läbi avaliku kanali (eeldatakse, et vastav kanal on autentitud, s.t. ükski kõrvaline osapool ei saa võtit edastamise ajal muuta) [4, lk 375].

Teistpidi, Alice võib genereerida oma võtmed (pk, sk) juba varasemalt, olenemata sellest, kas keegi soovib talle parasjagu sõnumit saata või mitte. Seejärel saab Alice oma avalikku võtit edastada kogu maailmale, näiteks pannes selle võtme oma veebilehele. Sedasi saab igaüks talle saata selle avaliku võtmega krüpteerituid sõnumeid ning Alice saab need sõnumid oma privaatse võtmega sk need dekrüpteerida [4, lk 375, 376].

2.2 Baasprobleemid ja nende lahendamine

Kaasaegne krüptograafia on üles ehitatud eeldusel, et mingid matemaatilised probleemid on n.-ö. keerulised — neid on raske klassikalise arvutiga lahendada. Nende probleemide põhjal tehakse krüptograafilisi skeeme, sest nii saab kindel olla, et neid on raske rünnata [4, lk 285].

Järgnevad kaks sellist probleemi, mis kolmandas peatükis rolli mängivad.

Diskreetse logaritmi probleem: [4, lk 319, 320] Olgu G tsükliline rühm tekitajaga g, kus $|G| = q$. Antud $h \in G$ korral leida selline $x \in \mathbb{Z}_q$ nii, et

$$g^x = h.$$

Eksponentsiaalsete kongruentside probleem: [1, lk 4] Olgu $(G, +, \cdot)$ algebraline struktuur q elemendiga ja kahekohaliste tehetega $+$ ja $\cdot$. Olgu $g_1, g_2 \in G$, kus $|\langle g_1 \rangle| = s$ ja $|\langle g_2 \rangle| = t$ ning $s, t < q$, aga $st \geq q$. Leida lahend $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$ võrrandile

$$ag_1^{x_1} + bg_2^{x_2} = c,$$

kus $a, b, c \in G$.

Märgime, et nende probleemide keerukus oleneb vastava algebralise struktuuri valikul.

3 Entroopiline teisendus ja selle rakendused

Käesolev peatükk annab ülevaate entroopilisest teisendusest ning selle rakendustest erinevate krüptograafiliste skeemide teisendamisel. Samuti esitatakse entroopiliste teisenduste nõrkused ning analüüsitakse ründeid selle vastu.

3.1 Entroopiline teisendus

Defineerime diskreetse logaritmi probleemi entroopilise teisenduse.

Definitsioon 11. [1, lk 4] Olgu g entropoidi $\mathbb{E}_{q^2}$ tekitaja. Olgu diskreetse logaritmi probleem arvutuslikult keeruline ülesanne üle tsüklilise alamrühma $(G_1, \cdot)$, kus $G_1 = \langle g \rangle$. Teisisõnu, mingi $y \in G_1$ korral, kus $y = g^x$, eeldame, et ei leidu sellist (klassikalist) polünomiaalse keerukusega algoritmi, mis leiaks $x \in \mathbb{Z}_q$. Diskreetse logaritmi probleemi **entroopiline teisendus** on teisendus, mis asendab astendajad $x \in \mathbb{Z}_q$ kahedimensiooniliste astmeindeksitega $X = (x_1, x_2)$, kus $x_1, x_2 \in \mathbb{Z}_q$. Täpsemalt, mingi $y \in G$ korral, kus $y = g^X$, on tarvis leida astmeindeks $X = (x_1, x_2)$.

Tuleb välja, et diskreetse logaritmi probleemi entroopiline teisendus on lihtsustatud versioon eksponentsiaalsete kongruentside probleemile. Seda väidab järgmine lemma.

Lemma 3. [1, lk 4] *Entroopiliselt teisendatud diskreetse logaritmi probleem on lihtsustatud eksponentsiaalsete kongruentside probleem entropoidis* $\mathbb{E}_{q^2} = (G, \boxplus, \cdot)$, *kus* $a = b = 1$ *ja* $g_1 = g_2 = g$, *s.t. otsitakse lahendit* $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$ *võrrandile*

$$y = g^{x_1} \boxplus g^{x_2}.$$

Tõestus. Entroopiliselt teisendatud diskreetse logaritmi probleem on järgnev ülesanne: mingi $y \in G$ korral leia $x_1, x_2 \in \mathbb{Z}_q$ nii, et $y = g^{(x_1, x_2)}$. Definitsioonist 9 saame, et $y = g^{x_1} \boxplus g^{x_2}$. Oluline on tähele panna, et g ja $T(g)$ on sõltumatud

elemendid, seega elementi g ei saa esitada $T(g)$ astmena ja vastupidi. Sellest tulenevalt ei saa astmeindeksite kahedimensionaalsust taandada ühele dimensioonile ehk jõuda tagasi diskreetse logaritmi probleemini. Seega saadud teisendus on tõesti lihtsustatud versioon eksponentsiaalsete kongruentside probleemist, kus $a = b = 1$ ja $g_1 = g_2 = g$. □

Seetõttu kõiki krüptograafisi skeeme, mis põhinevad diskreetse logaritmi probleemi lahenduvusel, on võimalik entroopiliselt teisendada. Olgu g entropoidi $\mathbb{E}_{q^2}$ tekitaja ja olgu $\mathcal{S}(g, \mathcal{A})$ krüptograafiline skeem algoritmide hulgaga $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_\nu\}$, mille turvalisus baseerub diskreetse logaritmi probleemil. Olgu diskreetse logaritmi probleem arvutuslikult keeruline üle tsüklilise alamrühma $(G_1, \cdot)$, mille tekitajaks on g. Olgu hulgas $\mathcal{A}$ kokku μ astmemuutujat, mida tähistame $x^{(i)} \in \mathbb{Z}_q$, kus $i \in \{1, \ldots, \mu\}$. **Skeemi $\mathcal{S}$ entroopiline teisendus** on teisendus, mis asendab kõik algoritmide hulga $\mathcal{A}$ astmemuutujad $x^{(i)} \in \mathbb{Z}_q$ kahedimensiooniliste astmeindeksitega $X^{(i)} = (x_1^{(i)}, x_2^{(i)})$, $i \in \{1, \ldots, \mu\}$. Asendusi tehakse kõikides avaldistes. [1, lk 4, 5]

Tuleb tähele panna, et teisendatud skeemis võib tekkida vajadus sooritada tehet astmeindeksi ja rühma elemendi muutujate vahel, kuigi sellist tehet ei ole astmeindeksi aritmeetikas defineeritud. Sel juhul tuleb proovida seada vastavusse rühma elemendi muutuja astmeindeksi muutujaga läbi mõne räsifunktsiooni, et sellist tehet võimaldada. [1, lk 5]

3.2 Näiteid skeemide entroopilistest teisendustest

Toome näiteid erinevate krüptograafiliste skeemide entroopilistest teisendustest.

Näide 1. Klassikalise Diffie-Hellmani võtmevahetusskeemi entroopiline teisendus on lihtne muutujate vahetus. Kui klassikalises skeemis valivad Alice ja Bob mingi kindla lõpliku tsüklilise rühma $(G, \cdot)$, mille järk on n ja tekitaja on g, siis entroopilise Diffie-Hellmani juhul valivad Alice ja Bob mingi kindla lõpliku entropoidi

$\mathbb{E}_{q^2} = (G, \boxplus, \cdot)$, milles on q^2 elementi ja tekitaja on g. [1, lk 8]

(a) Klassikaline Diffie-Hellman võtmevahetus	**(b)** Entroopiline Diffie-Hellman võtmevahetus
1. Alice valib suvalise naturaalarvu a, kus $1 < a < n$, ja saadab elemendi $g^a \in G$ Bobile.	1. Alice valib suvalise astmeindeksi $A = (a_1, a_2)$, kus $1 < a_1, a_2 < q$, ja saadab elemendi $g^A \in G$ Bobile.
2. Bob valib suvalise naturaalarvu b, kus $1 < b < n$, ja saadab elemendi $g^b \in G$ Alice'ile.	2. Bob valib suvalise astmeindeksi $B = (b_1, b_2)$, kus $1 < b_1, b_2 < n$, ja saadab elemendi $g^B \in G$ Alice'ile.
3. Alice arvutab elemendi $JagatudVõti = (g^b)^a = g^{ba} \in G$.	3. Alice arvutab elemendi $JagatudVõti = (g^B)^A = g^{BA} \in G$.
4. Bob arvutab elemendi $JagatudVõti = (g^a)^b = g^{ab} \in G$.	4. Bob arvutab elemendi $JagatudVõti = (g^A)^B = g^{AB} \in G$.

Tabel 1: Klassikaline ja entroopiline Diffie-Hellman võtmevahetusskeem [1, lk 8]

Näide 2. DSA skeemi entroopiline teisendus ei ole see-eest nii lihtne. Skeemi definitsioonis on muutujaid, mis sisalduvad ühes rühmas, aga mida hiljem tõlgendatakse teise rühma elementidena. Sellest tulenevalt tekib sobimatuid aritmeetilisi tehteid astmeindeksite ja rühma elementide vahel. Selliseid situatsioone saab aga parandada vastavalt paragraafi 3.1 viimases lõigus kirjeldatud meetodiga. [1, lk 9]

Klassikalises DSA skeemis valitakse N-bitine algarv q ja L-bitine algarv p nii, et arv $p - 1$ jagub arvuga q. Valitakse tekitaja kujul $g = h^{(p-1)/q} \pmod{p}$, kus h on

suvaline arv hulgast $\{2, \ldots, p-1\}$. Samuti valitakse krüptograafiline räsifunktsioon $H : \{0,1\}^* \mapsto \mathbb{Z}_q$. Entroopilises skeemis valitakse lõplik entropoid $\mathbb{E}_{q^2} = (G, \boxplus, \cdot)$, milles on q^2 elementi, tekitaja on $g \in G$ ja mille korral eeldatakse, et eksponentsiaalsete kongruentside probleem on keeruline. Valitakse ka krüptograafiline räsifunktsioon $H : \{0,1\}^* \mapsto \mathbb{Z}_q \times \mathbb{Z}_q$. [1, lk 9, 10]

Paneme tähele, et entroopilises variandis ei ole muutujal s liidetavaks $x \cdot r$, vaid hoopis $x \cdot H(r)$. See tuleb sellest, et entroopilises skeemis on $x \in \mathbb{Z}_q \times \mathbb{Z}_q$ ja $r \in G$, seega korrutis $x \cdot r$ ei ole hästi defineeritud. Samas $H(r) \in \mathbb{Z}_q \times \mathbb{Z}_q$, seega $x \cdot H(r)$ on valiidne aritmeetiline operatsioon. [1, lk 9, 10]

Võtme genereerimine

$PrivaatneVõti \equiv x \xleftarrow{\$} \mathbb{Z}_q^*$

$AvalikVõti \equiv y = g^x \pmod{p}$

Allkirjasta sõnum M

Vali suvaline $k \xleftarrow{\$} \mathbb{Z}_q^*$

$r = (g^k \pmod{p}) \pmod{q}$

$s = (k^{-1}(H(M) + x \cdot r)) \pmod{q}$

$Allkiri = (r, s)$

Kontrolli

$w = s^{-1} \pmod{q}$

$u_1 = H(M) \cdot w \pmod{q}$; $u_2 = r \cdot w \pmod{q}$

$v = (g^{u_1} y^{u_2} \pmod{p}) \pmod{q}$

Tagasta *True* kui $v = r$, vastasel juhul tagasta *False*

Tabel 2: Klassikaline DSA skeem [1, lk 10]

Võtme genereerimine

$PrivaatneVõti \equiv x = (x_1, x_2) \xleftarrow{\$} \mathbb{Z}_q \times \mathbb{Z}_q$

$AvalikVõti \equiv y = g^x$

Allkirjasta sõnum M

Vali suvaline $k \xleftarrow{\$} \mathbb{Z}_q \times \mathbb{Z}_q$

$r = g^k$

$s = k^{-1}(H(M) + x \cdot H(r))$

$Allkiri = (r, s)$

Kontrolli

$v_1 = r^s$

$v_2 = g^{H(M)} \cdot y^{H(r)}$

Tagasta *True* kui $v_1 = v_2$, vastasel juhul tagasta *False*

Tabel 3: Entroopiline DSA skeem [1, lk 10]

Näide 3. Schnorri signatuurskeemi korral on samuti tegu muutujate vahetusega. Klassikalises skeemis valitakse lõplik tsükliline rühm $(G, \cdot)$, mille järk on algarv q, tekitaja on $g \in G$ ja mille korral eeldatakse, et diskreetne logaritmi probleem selle rühma korral on keeruline. Valitakse krüptograafiline räsifunktsioon $H : \{0,1\}^* \mapsto \mathbb{Z}_q$. Entroopilise skeemi korral valitakse lõplik entropoid $\mathbb{E}_{q^2} = (G, \boxplus, \cdot)$, mille järk on q^2, tekitaja on $g \in G$ ja mille korral eeldatakse, et eksponentsiaalsete kongruentside probleem on keeruline. Samuti valitakse krüptograafiline räsifunktsioon $H : \{0,1\}^* \mapsto \mathbb{Z}_q \times \mathbb{Z}_q$. [1, lk 8]

Tabelis 6 on esitatud variant entroopilisest Schnorri signatuurskeemist, mille nimi on SEQUOA [1, lk 8]. 2023. aasta märtsis suudeti aga see skeem murda. Rünne seisneb eksponentsiaalsete kongruentside probleemi taandamisel diskreetse logaritmi probleemile, mida on võimalik kvantarvutiga kergesti lahendada. Seetõttu

ei saa väita, et diskreetse logaritmi probleemi entroopiline teisendus on tegelikult postkvant-turvaline [3]

Võtme genereerimine

$PrivaatneVõti \equiv x \xleftarrow{\$} \mathbb{Z}_q^*, \quad AvalikVõti \equiv y = g^x$

Allkirjasta sõnum M

Vali suvaline $k \xleftarrow{\$} \mathbb{Z}_q^*$

$r = g^k$

$e = H(r||M)$

$s = k - xe$

$Allkiri = (s, e)$

Kontrolli

$r_v = g^s y^e$

$e_v = H(r_v||M)$

Tagasta *True* kui $e_v = e$, vastasel juhul tagasta *False*

Tabel 4: Klassikaline Schnorri signatuurskeem [1, lk 9]

Võtme genereerimine

$PrivaatneVõti \equiv x = (x_1, x_2) \xleftarrow{\$} \mathbb{Z}_q \times \mathbb{Z}_q,$

$AvalikVõti \equiv y = g^x$

Allkirjasta sõnum M

Vali suvaline $k \xleftarrow{\$} \mathbb{Z}_q \times \mathbb{Z}_q$

$r = g^k$

$e = H(r||M)$

$s = k - xe$

$Allkiri = (s, e)$

Kontrolli

$r_v = g^s y^e$

$e_v = H(r_v||M)$

Tagasta *True* kui $e_v = e$, vastasel juhul tagasta *False*

Tabel 5: Entroopiline Schnorri signatuurskeem [1, lk 9]

Võtme genereerimine

$PrivaatneVõti \equiv x = (x_1, x_2) \xleftarrow{\$} \mathbb{Z}_q \times \mathbb{Z}_q$,

$AvalikVõti \equiv y = g^x$

Allkirjasta sõnum M

Olgu $k = (k_1, k_2) \leftarrow H(rand||PrivaatneVõti||M)$,

kus $rand \xleftarrow{\$} \{0,1\}^n$ on vähemalt vähemalt n

juhuslikult genereeritud biti jada.

$r = g^k$

$e = H(r||AvalikVõti||M)$

$s = k - xe$

$Allkiri = (s, e)$

Kontrolli

$r_v = g^s y^e$

$e_v = H(r_v||AvalikVõti||M)$

Tagasta *True* kui $e_v = e$, vastasel juhul tagasta *False*

Tabel 6: SEQUOA signatuurskeem

3.3 Rünnakud entroopiliselt teisendatud diskreetse logaritmi probleemi vastu

Esitame algoritmid, mille abil saab lihtsustatud eksponentsiaalsete kongruentside probleemi lahendada. Nende põhjal väitis artikli [1] autor, et entroopiliselt teisendatud diskreetse logaritmi probleem on postkvant-turvaline, aga, nagu sai märgitud näites 3, siis tegelikkuses suudab kvantarvuti seda efektiivselt lahendada.

Lemma 4. [1, lk 6] *Olgu g entropoidi $\mathbb{E}_{q^2}$ tekitaja ja olgu $y \in G$ selline, et see on lahend võrrandile $y = g^{x_1} \boxplus g^{x_2}$ mingi $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$ korral. Antud võrrandile*

on võimalik leida lahend (x_1, x_2) *deterministliku algoritmiga, mille halvim keerukus on* $O(q^{3/2}(\log q))$.

Tõestus. Arvutame iga $x_2 \in \{0, 1, \ldots, q-1\}$ korral $y \boxminus g^{x_2}$ ja proovime leida täisarvu x_1 nii, et $g^{x_1} = y \boxminus g^{x_2}$. Selle leidmiseks on võimalik kasutada Baby-Step Giant-Step deterministliku algoritmi [7], mille ajaline keerukus on halvimal juhul $O(q^{1/2}(\log q))$. Siin juhul see algoritm tagastab vastava lahendi või leiab, et arvu x_2 korral ei leidu lahendit x_1. Lisades juurde aja, mis kulub kõikide arvude x_2 läbi vaatamiseks, saame halvimaks ajaliseks keerukuseks $O(q \cdot q^{1/2}(\log q)) = O(q^{3/2}(\log q))$. □

Järeldus 1. [1, lk 6, 7] *Leidub randomiseeritud algoritm võrrandi* $y = g^{x_1} \boxplus g^{x_2}$ *lahendi leidmiseks, mis teeb* $O(q_\nu^{5/2})$ *rühma tehet, kus* $q = q_1 \ldots q_\nu$ *(järjestatud kasvavalt) ja suurim algtegur* $q_\nu > q^{1/2}$.

Tõestus. Asendame Lemma 4 tõestuses Baby-Step Giant-Step algoritmi randomiseeritud algoritmiga, mida kirjeldatakse Victor Shoup' artiklis [9]. See algoritm teeb $\Omega(\sqrt{q_\nu})$ rühma tehet. Seega ajaline keerukus tuleb $O(q \cdot q_\nu^{1/2}) < O(q_\nu^2 \cdot q_\nu^{1/2}) = O(q_\nu^{5/2})$. □

Lemma 5. [1, lk 7] *Olgu* g *entropoidi* $\mathbb{E}_{q^2}$ *tekitaja ja olgu* $y \in G$ *selline, et see on lahend võrrandile* $y = g^{x_1} \boxplus g^{x_2}$ *mingi* $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$ *korral. Antud võrrandile on võimalik leida lahend* (x_1, x_2) *kvantalgoritmiga, mille halvim ajaline keerukus on* $O(q^{1/2}(\log \log q))$.

Tõestus. Arvutame iga $x_2 \in \{0, 1, \ldots, q-1\}$ korral $y \boxminus g^{x_2}$ ja kasutame Shor'i algoritmi (mille kohta saab lugeda artiklist [8]), et leida x_1, mille korral $g^{x_1} = y \boxminus g^{x_2}$, või leida, et sellist elementi x_1 ei saa leida antud x_2 korral. Eeldatav arv kordi enne, kui Shor'i algoritm jõuab lahenduseni, on $O(\log \log q)$. Tähistagu $\mathcal{S}(x_2)$ alamrutiini, mis implementeerib Shor'i algoritmi kvantvõrgu.

Kasutame nüüd Grover'i otsingualgoritmi [2] üle alamrutiini $\mathcal{S}(x_2)$ ja otsinguruumi $x_2 \in \{0, 1, \ldots, q-1\}$. Lõplik keerukus on siis $O(q^{1/2}(\log \log q))$. □

Kokkuvõte

Käesolevas töös esitasime entropoidide ja astmeindeksite baasteooria. Andsime lühikese ülevaate asümmeetrilisest krüptograafiast ja baasprobleemidest, mille alusel asümmeetrilisi skeeme konstrueerida. Kirjeldasime entroopilise teisenduse olemust, tõime näiteid selle toimimisest ja esitasime algoritme teisendatud probleemi lahendamiseks.

Töös sai mainitud, et antud teisendus ei taga tegelikkuses postkvant-turvalisust, seega töö edasiareng oleks analüüsida entropoidi konstruktsiooni ja formuleerida selle põhjal uus algebraline struktuur, millega saaks kvantturvalisust tagada.

Kasutatud allikad

[1] Danilo Gligoroski. *A Transformation for Lifting Discrete Logarithm Based Cryptography to Post-Quantum Cryptography*. Cryptology ePrint Archive, Paper 2023/318. 2023. URL: https://eprint.iacr.org/2023/318.

[2] Lov K Grover. "A fast quantum mechanical algorithm for database search". Teoses: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, lk. 212–219.

[3] *hxp CTF 2022: sequoa writeup*. URL: https://hxp.io/blog/95/.

[4] Jonathan Katz ja Yehuda Lindell. *Introduction to modern cryptography*. CRC Press, Taylor & Francis Group, 2015.

[5] Valdis Laan. *Algebra II loengukonspekt*. Sügis 2022. URL: https://courses.ms.ut.ee/2022/algebra2/fall/Main/Lectures.

[6] Gary L. Mullen ja Daniel Panario. *Handbook of Finite Fields*. Chapman & Hall/CRC, 2013.

[7] Daniel Shanks. *Class number, a theory of factorization, and genera*. 1971. DOI: 10.1090/pspum/020/0316385.

[8] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing* 26.5 (oktoober 1997), lk. 1484–1509.

[9] Victor Shoup. "Lower bounds for discrete logarithms and related problems". *Advances in Cryptology — EUROCRYPT '97* (1997), lk. 256–266. DOI: 10.1007/3-540-69053-0_18.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Brett Johannes Hankewitz,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose "Diskreetse logaritmi probleemi entroopiline teisendus ja selle rakendused", mille juhendajad on Jan Villemson ja Valdis Laan, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaaloman-di ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Brett Johannes Hankewitz
09.05.2023