Ühissalastusest

Käesolevas tekstis on kasutatud järgmisi algebra mõisteid: jäägiklassikorpus, polünoom, polünoomi aste, polünoomi väärtus kohal c, polünoomi juur, Lagrange'i interpolatsioonivalem.

1 Sissejuhatus

Tänapäeva maailmas on teatud tundlikku infot (näiteks tuumarelvade kasutamiseks vajalik info, teatud pangakontod või krüptosüsteemide salajased võtmed), millele ligipääs tagatakse ainult väga valitud seltskonnale. Kui see seltskond on liiga väike, siis on oht, et ligipääsukood läheb kogemata kaotsi või hävib. Kui aga koodi teavad liiga paljud, siis on oht, et see lekib neile, kes ei peaks seda teadma. Ühissalastusskeemid pakuvad lahendust seda tüüpi probleemile. Need tagavad, et salajane info oleks kaitstud, aga samas neil kel vaja oleks võimalik sellele ligi pääseda.

Ühissalastusskeemide idee on selline, et ligipääsukood s — nimetagem seda edasises saladuseks või salasõnaks — jagatakse teatud viisil osadeks ning igale kasutajale antakse üks osa nii, et iga piisavalt suurte volitustega kasutajate hulk suudab saladuse osade järgi taastada, aga ükski teine kasutajate hulk seda ei suuda.

Formaalsemalt: me eeldame, et ühissalastusskeemi kasutajate hulk on $U = \{1, 2, \ldots, n\}$ ning ühissalastust aitab läbi viia diiler D (see ei pea olema tingimata inimene, võib olla ka arvuti). Eeldame, et diiler teab saladust. Skeemi puhul on fikseeritud volitatud koalitsioonide hulk Γ, mis koosneb hulga U mingitest alamhulkadest ja rahuldab tingimust

$$X \in \Gamma \text{ ja } X \subseteq Y \Longrightarrow Y \in \Gamma.$$

Näide 1 Ajakirja Times Magazine 1992. aasta 4. mai numbris väidetakse, et Nõukogude Liidus olevat olnud realiseeritud järgmine ühissalastusskeem. Riigi kolmel tähtsamal tegelasel — presidendil (keda kutsuti NLKP Keskkomitee peasekretäriks), peaministril ja kaitseministril — oli igaühel niinimetatud tuumakohver ja mistahes kaks neist kolmest oleks saanud tuumaraketid teele saata. Üksinda ei oleks keegi neist kolmest seda teha saanud.

Sellise skeemi puhul $U = \{1, 2, 3\}$ ja $\Gamma = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Seega on antud olukorras kõik kasutajad võrdse tähtsusega. Kui aga $\Gamma = \{\{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$, siis näeme, et siin on kasutaja 1 teistest tähtsam, ilma temata ei saa saladust teada. Samas ei ole ta ka kõikvõimas — ta peab ühendama jõud veel vähemalt ühe kasutajaga.

Näide 2 Vaatleme olukorda, kus pangas on vaja teha suuremahuline ülekanne teise panka. Ei ole mõistlik jätta sellises olukorras otsustamine ainult ühe inimese õlule. Mõistlik oleks

näiteks korraldada asi nii, et sellise otsuse tegemiseks on vaja kas a) kolme vanemtelleri, b) kahe asepresidendi või c) kahe vanemtelleri ja ühe asepresidendi nõusolekut.

Näide 3 ÜRO julgeolekunõukogu koosneb viiest alalisest liikmest ja kümnest mittealalisest liikmest. Otsuse vastuvõtmiseks on vaja kõigi viie alalise liikme nõusolekut ja veel vähemalt nelja mittealalise liikme nõusolekut.

Ühissalastusskeeme on palju erinevaid, aga enamus neist kasutab mingit sorti algebrat või arvuteooriat. Me tutvustame neist ühte lihtsamat — Shamiri ühissalastusskeemi. Enne seda on vaja tutvuda ühe klassikalise tulemusega polünoomide kohta.

2 Lagrange'i interpolatsioonivalem

Lagrange'i interpolatsioonivalem annab vastuse küsimusele: kuidas taastada polünoom, kui on teada selle polünoomi väärtused teatud punktides.

Teoreem 1 *Olgu K korpus, $n \in \mathbb{N}$, $c_0, c_1, \ldots, c_n, b_0, b_1, \ldots, b_n \in K$, kusjuures $c_0, c_1, \ldots, c_n$ on paarikaupa erinevad. Siis leidub üheselt määratud polünoom $f(X) \in K[X]$ nii, et* $\deg(f(X)) \leq n$ *ja*

$$f(c_i) = b_i$$

iga $i \in \{0, 1, \ldots, n\}$ korral.

Tõestus. Vajalike omadustega polünoom on

$$f(X) = \sum_{i=0}^{n} b_i \frac{(X - c_0) \ldots (X - c_{i-1})(X - c_{i+1}) \ldots (X - c_n)}{(c_i - c_0) \ldots (c_i - c_{i-1})(c_i - c_{i+1}) \ldots (c_i - c_n)}. \tag{1}$$

Siin valemis liidetava $b_i \frac{g(X)}{d_i}$ all mõeldakse polünoomi $b_i d_i^{-1} g(X)$. Tänu eeldusele, et $c_0, c_1, \ldots, c_n$ on paarikaupa erinevad, on

$$d_i = (c_i - c_0) \ldots (c_i - c_{i-1})(c_i - c_{i+1}) \ldots (c_i - c_n)$$

nullist erinev element korpuses K, sest korpuses ei ole nullitegureid. Seega on elemendil d_i olemas pöördelement. Lihtne on näha, et $f(c_i) = b_i$ iga $i \in \{0, 1, \ldots, n\}$ korral.

Veendume, et polünoom $f(X)$ on üheselt määratud. Oletame, et ka polünoom $g(X) \in K[X]$ on selline, et $\deg(g(X)) \leq n$ ja $g(c_i) = b_i$ iga $i \in \{0, 1, \ldots, n\}$ korral. Siis $\deg(f(X) - g(X)) \leq n$ ja

$$f(c_i) - g(c_i) = b_i - b_i = 0.$$

See tähendab, et $c_0, c_1, \ldots, c_n$ on polünoomi $f(X) - g(X)$ juured. Samas nullist erineva polünoomi juurte koguarv ei saa ületada polünoomi astet (vt. [3], lause 7.1.9). See tähendab, et $f(X) - g(X)$ on nullpolünoom ja seega $f(X) = g(X)$. ■

Järeldus 1 *Olgu K korpus, $n \in \mathbb{N}$, $c_0, c_1, \ldots, c_{n-1}, b_0, b_1, \ldots, b_{n-1} \in K$, kusjuures $c_0, c_1, \ldots, c_{n-1}$ on paarikaupa erinevad ja ükski neist ei ole 0. Siis iga $t \in K$ jaoks leidub üheselt määratud polünoom $f(X) \in K[X]$ nii, et* $\deg(f(X)) \leq n$*, selle polünoomi vabaliige on t ja*

$$f(c_i) = b_i$$

iga $i \in \{0, 1, \ldots, n-1\}$ korral.

Tõestus. Polünoomi vabaliige on tema väärtus kohal 0. Võttes $c_n = 0$, $b_n = t$ ning rakendades teoreemi 1 saame polünoomi $f(X)$, mille korral $f(0) = t$ ning ka ülejäänud tingimused on täidetud. ■

Valemit (1) kutsutakse **Lagrange'i interpolatsioonivalemiks**.

3 Shamiri ühissalastusskeem

Olgu meie saladus esitatud mingi naturaalarvuna s. Valime algarvu p, mis on piisavalt suur. Vaatleme saladust s korpuse $\mathbb{Z}_p$ elemendina. Kuna p on piisavalt suur, siis ei ole ohtu, et pahatahtlik tegelane suudaks ära arvata, mis see s on.

Olgu meil n kasutajat, kes tahaks, et saladus oleks osadeks jagatud nii, et mistahes k kasutajat, kus $k < n$, saaks saladuse teada, aga ükski kasutajate hulk, kus on alla k inimese, ei saaks saladust teada. Iisraeli krüptograaf Adi Shamir (sündinud 1952) on selleks pakkunud välja järgmise elegantse meetodi.

Diiler

1. genereerib k juhuslikku elementi $s_0, s_1, \ldots, s_{k-1} \in \mathbb{Z}_p$ ja võtab saladuseks s elemendi s_0;
2. moodustab polünoomi

$$f(X) = s_0 + s_1X + s_2X^2 + \ldots + s_{k-1}X^{k-1} \in \mathbb{Z}_p[X];$$

3. iga $i \in \{1, 2, \ldots, n\}$ korral arvutab polünoomi $f(X)$ väärtuse kohal i ning annab kasutajale i tema "osa" $f(i) =: b_i$. (Kui olla päris täpne, siis arvutakse küll $f(\bar{i})$.) Praktikas võib seda osa säilitada arvupaarina $(i, f(i))$ mingil elektroonilisel kaardil.

Kui nüüd k kasutajat ühendavad oma andmed, siis nad suudavad Lagrange'i interpolatsioonivalemi abil taastada polünoomi $f(X)$ ja saada teada selle vabaliime $s_0 = s$. Samas $k-1$ kasutajal ei ole absoluutselt mingit infot s kohta. Seda ütleb järeldus 1: $k-1$ kasutaja andmete põhjal saab konstrueerida mistahes vabaliikmega polünoomi.

Näide 4 Ühe firma juhatuses on neli liiget. Firma põhikirja järgi on igal kolmikul neist lubatud teha tehinguid välismaal olevat pangakontot kasutades. Firma kasutab selleks ühissalastusskeemi, kus saladuseks on korpuse $\mathbb{Z}_7$ element. Süsteemi administraator annab igale juhatuse liikmele välja elektroonilise kaardi vajaliku infoga.

Oletame, et kolm liiget soovivad teha ülekande mainitud kontolt. Nende käes olevatel kaartidel on paarid

$$(1, 3), \quad (2, 0), \quad (4, 6).$$

Näitame, kuidas antud olukorras saavad nad leida vajaliku salasõna.

Nad otsivad polünoomi $f(X) = s_0 + s_1X + s_2X^2 \in \mathbb{Z}_7[X]$, mis rahuldaks tingimusi

$$f(1) = 3, \quad f(2) = 0, \quad f(4) = 6.$$

Kasutades Lagrange'i interpolatsioonivalemit saavad nad, et

$$\begin{aligned} f(X) &= 3\frac{(X-2)(X-4)}{(1-2)(1-4)} + 6\frac{(X-1)(X-2)}{(4-1)(4-2)} = 3\frac{(X+5)(X+3)}{3} + 6\frac{(X+6)(X+5)}{6} \\ &= (X^2 + X + 1) + (X^2 + 4X + 2) = 2X^2 + 5X + 3. \end{aligned}$$

Siit nad näevad, et vabaliige (ja seega salasõna) on 3.

Kes soovib Shamiri ühissalastusskeemi kohta põhjalikumalt lugeda, võib tutvuda Dan Bogdanovi poolt koostatud tekstiga [2]. Käesolev tekst on koostatud Valdis Laane poolt 2017. aastal tuginedes Arkadii Slinko raamatule [1].

Viited

[1] A. Slinko, *Algebra for Applications*, Springer, 2015.

[2] D. Bogdanov, *Foundations and properties of Shamirs secret sharing scheme*, https://pdfs.semanticscholar.org/540b/faa26cfafde5be79aadde37cb79f9d2daf76.pdf , 2007.

[3] M. Kilp, Algebra I, Tartu, 1998.