Ühissalastusskeemid

Helger Lipmaa

13. november 1997. a.

1 Sissejuhatus

Ühissalastusskeemid on mitme osapoolega võtmekehtestusprotokollid, mille vajadus tuleb esile teatud erilistes situatsioonides, nagu näiteks:

1. Pangas on šeif, mida avatakse korra päevas. Pangal on selle jaoks palgatud kolm vanemtellerit. Avamist ei usaldata ühelegi tellerile individuaalselt; šeifi avamise juures peab kohal olema vähemalt kaks tellerit.
2. Notariaalkontoris allkirjastatakse dokumente. Vastavalt dokumentide olulisusele peab iga dokumendi all olema ühe, kahe või kolme notari allkirjad. Vastasel juhul ei loeta dokumenti kehtivaks.
3. Nõukogude ajal oli NSV Liidus kolm nö "tuumaportfell," mille nupule vajutamine oleks valla päästnud tuumasõja. Kõrgema turvalisuse tagamiseks oli ka siin rakendatud nö kaks-kolmest süsteem: sõjategevus aktiviseerus ainult kahe nupu samaaegsel vajutamisel.

Hoopis erinev näide on vajadus teha krüptograafilistest võtmetest tagavarakoopiaid. Mida suurem arv koopiaid tehakse, seda tõenäolisemalt tulevad võtmed avalikuks. Mida vähem koopiaid tehakse, seda tõenäolisemalt võtmed kaduma lähevad.

Ühissalastusskeemid on välja töötatud usaldatavuse tõstmiseks ilma täiendava riski lisandumiseta. Samuti adresseerivad ü.s.s.-id olukordi, kus on vaja jagada kriitiliste operatsioonide teostamise usaldust ja/või vastutust.

Ühissalastusskeemideks klassifitseeruvad ka **ühisvastutusskeemid**, kus on vajalik ühe või enama osapoole osasid mingi kriitilise tegevuse sooritamiseks (saladus võimaldab tegevust alustada, samas võib ka saladuse taastamist ennast defineerida 'tegevuseks').

Tähistame kõigi osapoolte hulka $\mathcal{P}$, kusjuures $|\mathcal{P}| = w$ ning $\mathcal{P} := \{P_i : 1 \leq i \leq w\}$. Ü.s.s-id saavad sisendiks **saladuse** ning "jagavad" selle **osadeks** (*share*), mis jaotatakse osapoolte vahel nii, et ainult osapoolte hulga **autoriseeritud alamhulkade** saladuste ühendamisel saadakse kätte algne saladus. Tähistame kõikide saladuste hulka $\mathcal{K}$ ning kõikide osade hulka $\mathcal{S}$. Saladuse ehk võtme K väärtuse valib tavaliselt välja spetsiaalne osapool, keda nimetatakse **jagajaks** (*dealer*). Jagajat tähistame D. Eeldame, et $D \notin \mathcal{P}$. Jagaja jaotab ka saladuse osadeks ning toimetab osad osapooltele turvaliselt kohale. Osade ühendamiseks on võimalikud erinevad protokollid (osapooled saavad füüsiliselt kokku; osad saadetakse edasi usaldatavale instantsile).

Kõikide autoriseeritud hulkade hulka Γ nimetatakse **pääsustruktuuriks** (*access structure*); $\Gamma \subseteq 2^{\mathcal{P}}$.

Definitsioon 1.1 *Hulga $\mathcal{Q}$ alamhulkade süsteemi $\mathcal{R} \subseteq \mathcal{Q}$, mis rahuldab järgmist tingimust:*

$$X \in \mathcal{R} \wedge X \subseteq Y \supset Y \subset \mathcal{R}$$

nimetatakse hulga $\mathcal{Q}$ ***ideaaliks****.*

On selge, et suvaline pääsustruktuur on hulga $2^{\mathcal{P}}$ ideaal.

Definitsioon 1.2 *Pääsustruktuuri $\Gamma \subseteq 2^{\mathcal{P}}$ realiseeriv* ***täielik ühissalastusskeem*** *on meetod saladuse K jagamiseks w osapoole vahel nii, et järgmised kaks omadust oleksid rahuldatud:*

1. *Suvalise autoriseeritud alamhulga $B \subseteq \mathcal{P}$ osade ühendamisel saadavast informatsioonist piisab saladuse K kindlaks määramiseks.*
2. *Ühegi mitteautoriseeritud alamhulga $B \not\subseteq \mathcal{P}$ osade ühendamisel saadavast informatsioonist ei piisa saladuse K kindlaks määramiseks.*

Järgnevas näitame, et hulga $2^{\mathcal{P}}$ suvalise ideaali realiseerimiseks leidub täielik ühissalastusskeem, st et hulga $2^{\mathcal{P}}$ suvalist ideaali võib vaadelda pääsustruktuurina.

2 Shamiri läviskeem

Definitsioon 2.1 *Olgu antud osapoolte hulk $\mathcal{P}$. Olgu t ja w positiivsed täisarvud, $t \leq w$. (t, w)-**läviskeem** on meetod, mis realiseerib pääsustruktuuri $\Gamma := \{B \subseteq \mathcal{P} \colon |B| \geq t\}$.*

Näited 1 ja 3 vastavad (2,3) läviskeemidele. Vaatleme järgnevalt Shamiri meetodit (t, w)-läviskeemi realiseerimiseks. Siin $\mathcal{K} = \mathcal{S} = \mathbb{Z}_p$, kus $p > w + 1$. Shamiri läviskeemis konstrueerib jagaja juhusliku polünoomi ülimalt $(t-1)$-järgu polünoomi $a(x)$, mille vabaliikmeks on saladus K. Igale osapoolele P_i antakse selle polünoomi üks punkt (x_i, y_i).

Algoritm 2.2 (Shamiri (t, w)-läviskeem, [Sha79])

Initsialiseerimine.

- *D valib w erinevat elementi $x_1, \ldots, x_w$ hulgast $\mathbb{Z}_p^*$. D edastab osapoolele P_i väärtuse x_i, $\forall i$.*

Saladuse $K \in \mathbb{Z}_p$ distributeerimine.

1. *D genereerib $t - 1$ juhuarvu $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$.*
2. *Olgu $a(x) := K + \sum_{j=1}^{t-1} a_j x_j \pmod p$. Igale osapoolele P_i edastatakse osa $y_i := a(x_i)$.*

2.1 Andmete ühendamine

Osapoolte hulk $B = \{P_1, \dots, P_t\}$, rekonstrueerib saladuse, kasutades polünoomide interpoleerimisel põhinevaid meetodeid.

Esimene meetod. Osapooled teavad, et $y_i = a(x_i)$, $i \le t$, kus $a(x) \in \mathbb{Z}_p[x]$ on D poolt valitud salastatud polünoom. Kuna polünoomi $a(x)$ järk on ülimalt $t-1$, siis $a(x) = a_0 + a_1 x + \dots + a_{t-1} x^{t-1}$, kus kordajad $a_1, \dots, a_{t-1}$ on salastatud elemendid hulgast $\mathbb{Z}_p$ ning $a_0 = K$. Kuna $y_i = a(x_i)$, teavad kokkutulnud t lineaarvõrrandit üle t muutuja $a_0, \dots, a_{t-1}$ (aritmeetika toimub ringis $\mathbb{Z}_p$). Juhul kui võrrandid on lineaarselt sõltumatud, leidub saadud võrrandisüsteemil ühene lahend $(\tilde{a}_0, \dots, \tilde{a}_{t-1})$, kus $\tilde{a}_0 = K$.

Lemma 2.3 *Saadud lineaarvõrrandisüsteemil on alati ühene lahend.*

Tõestus 2.4 *Lineaarvõrrandi maatrikskuju on järgmine:*

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \dots & x_t^{t-1} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}. \tag{1}$$

Kordajate maatriks A on Vandemonde maatriks, mille determinant saadakse valemist

$$\det A = \prod_{1 \le j < k \le t} (x_k - x_j) \pmod p.$$

Kuna kõik x_i-d on erinevad, siis $\det A \ne 0 \pmod p$ *ja järelikult on sel süsteemil ühene lahend* $\pmod p$.

Vaatleme juhtu, kus $|B| < t$. Toimides nagu ennegi, saavad kogunenud osapooled $t-1$ võrrandist koosneva lineaarvõrrandisüsteemi üle t muutuja. Sel juhul on lahendite ruum ühemõõtmeline, st iga a_0-i väärtuse $\tilde{a}_0$ jaoks leidub üks vektori $(a_1, \dots, a_{t-1})$ väärtus $(\tilde{a}_1, \dots, \tilde{a}_{t-1})$, nii et $(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_{t-1})$ on lineaarvõrrandisüsteemi 1 lahendiks. Järelikult ei saa osapooled antud juhul mingit täiendavat informatsiooni saladuse K kohta.

Teine meetod. Polünoomi $a(x)$ väärtuste arvutamiseks on olemas lihtsam meetod, mis kasutab Lagrange'i interpolatsioonivalemit:

$$a(x) = \sum_{j=1}^{t} y_j \prod_{1 \le k \le t, k \ne j} \frac{x - x_k}{x_j - x_k}.$$

On kerge veenduda, et saadud $(t-1)$-järku polünoom on sama, mis algne $a(x)$ ($a(x_i) = y_i$ suvalise $1 \le i \le t-1$ korral; kuna polünoom on $(t-1)$-järku, siis määravad tema väärtused $t-1$ erineval kohal täielikult polünoomi). t osapoolest koosnev rühm leiab $a(x)$-i väärtuse Lagrange' interpolatsioonivalemi abil üheselt. Samas ei ole neil vaja teada tervet polünoomi $a(x)$, vaid ainult väärtust

Algoritm 2.5

1. *D valib salaja, juhuslikult ja sõltumatult hulgast* $\mathbb{Z}_m$ $t-1$ *elementi* $y_1, \ldots,$ y_{t-1}.
2. *D arvutab* $y_t := K - \sum_{i=1}^{t-1} y_i \pmod{m}$.
3. *D saadab osapoolele* P_i, $1 \leq i \leq t$, *osa* y_i.

Joonis 1: (t, t)-läviskeem üle hulga $\mathbb{Z}_m$

$K = a(0)$. Saladuse K saab teada järgmisest valemist:

$$K := \sum_{j=1}^{t} y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_k - x_j}.$$

Defineerides

$$b_j := \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_k - x_j}$$

(paneme tähele, et väärtused b_j saab eelnevalt välja arvutada ning nad ei pruugi olla salastatud), saame

$$K := \sum_{j=1}^{t} b_j y_j,$$

seega on saladus t osa lineaarne kombinatsioon.

2.2 (t, t)-läviskeem

(t, t)-läviskeemis $\mathcal{K} = \mathcal{S} = \mathbb{Z}_m$,täiesti suvalise positiivse m-i väärtuse jaoks (m ei pea olema algarv ning m ei pea olema suurem kui t). Jagaja tükeldab võtme $K \in \mathbb{Z}_m$ joonisel 1 toodud algoritmi kohaselt.

Osapooled $P_1, \ldots, P_t$ leiavad võtme K valemist

$$K = \sum_{i=1}^{t} y_i \pmod{m}.$$

Esimesed $t-1$ osapoolt ei suuda omaette saladust arvutada, kuna nad teavad $t-1$ sõltumatut juhuslikku väärtust. Vaatleme (i.ü.k.) juhtu, kus $B = \{P_2, \ldots, P_t\}$. Need osapooled teavad koos osasid $y_2, \ldots, y_{t-1}$ ning $K - \sum_{i=1}^{t-1} y_i$. Osasid liites saadakse kätte $K - y_1$. Kuna aga osapooled ei tea väärtust y_1, siis ei suuda nad leida ka väärtust K. Seega on tegu (t, t)-läviskeemiga.

3 Üldised pääsustruktuurid

Vaatleme üldjuhtu, kus Γ on hulga $2^{\mathcal{P}}$ suvaline ideaal, olukorras, kus me ei piira autoriseerimata osapoolte arvutuslikku võimsust (st teoreetilist turvalisust).

Hulka $B \in \Gamma$ nimetatakse **minimaalseks autoriseeritud hulgaks**, kui $A \subset B \supset A \notin \Gamma$. Pääsustruktuuri Γ minimaalsete autoriseeritud alamhulkade hulka tähistatakse Γ_0 ning nimetatakse hulga Γ **baasiks**. Siis

$$\Gamma = \{C \subseteq \mathcal{P} \colon B \subseteq C, B \in \Gamma_0\}.$$

Ütleme, et Γ on hulga Γ_0 **sulund** ning kirjutame $\Gamma := \mathrm{cl}\,\Gamma_0$.

3.1 Monotoonsete Boole'i skeemide konstruktsioon

Toome järgmiselt Benaloh ja Leichteri ([BL90]) üldise konstruktsiooni suvalise monotoonse pääsustruktuuri realiseerimiseks täieliku ühissalastusskeemi abil, mis koosneb kahest sammust:

1. Konstrueeritakse antud pääsustruktuuri ära tundev monotoonne Boole'i skeem.

2. Konstrueeritakse esimesel sammul ehitatud Boole'i skeemi kirjeldusest lähtuvalt ühissalastusskeem.

Olgu antud w kahendsisendiga $x_1, \ldots, x_w$ (mis vastavad w-le osapoolele $P_1, \ldots, P_w$) Boole'i skeem $\mathbf{C}$ ning üks kahendväljund y. Boole'i skeemi, mis koosneb vaid $\wedge$- ning $\vee$-elementidest, nimetatakse **monotoonseks Boole'i skeemiks** (monotoonne, kuna sisendite muutmine 0-st 1-ks ei muuda kunagi väljundit 1-st 0-ks). Suvalisel elemendil võib olla kuitahes palju sisendeid, kuid vaid üks väljund. Boole'i skeemi elementide arvu nimetatakse selle skeemi **skeemkeerukuseks**.

Defineerime

$$B(x_1, \ldots, x_w) = \{P_i \colon x_i = 1\}$$

(hulga $\mathcal{P}$ alamhulk, mis vastab tõestele sisenditele). Monotoonse Boole'i skeemi korral defineerime talle vastava pääsustruktuuri

$$\Gamma(\mathbf{C}) := \{B(x_1, \ldots, x_w) \colon \mathbf{C}(x_1, \ldots, x_w) = 1\},$$

kus $\mathbf{C}(x_1, \ldots, x_w)$ tähistab skeemi $\mathbf{C}$ väljundit sisendi $(x_1, \ldots, x_w)$ korral. Kuna skeem $\mathbf{C}$ on monotoone, siis on $\Gamma(\mathbf{C})$ hulga $2^{\mathcal{P}}$ ideaal. On lihtne aru saada, et selliste monotoonsete Boole'i skeemide ning monotoonsete Boole'i valemite (valemite, mis sisaldavad tehteid $\wedge$ ja $\vee$, aga ei sisalda eitusi) vahel on olemas üksühene seos.

Vaatleme nüüd suvalist pääsustruktuuri Γ (tuletame meelde, et Γ on hulga $2^{\mathcal{P}}$ ideaal). Ehitame monotoonse Boole'i skeemi $\mathbf{C}$, mille korral $\Gamma(\mathbf{C}) = \Gamma$, järgmiselt. Olgu Γ_0 — pääsustruktuuri Γ baas. Konstrueerime disjunktiivsel normaalkujul oleva lausearvutusvalemi

$$\bigvee_{B\in\Gamma_0} (\bigwedge_{P_i\in B} P_i).$$

Näide 3.1 *Näiteks kui* $\Gamma_0 = \{\{P_1, P_2, P_3\}, \{P_2, P_4\}, \{P_1, P_4\}\}$*, saame valemi* $(P_1 \wedge P_2 \wedge P_3) \vee (P_2 \wedge P_4) \vee (P_1 \wedge P_4)$.

Suvalisele lausele Boole'i valemis vastab $\wedge$-element vastavas Boole'i skeemis; lauseid siduvale disjunktsioonile vastab $\vee$-element. Seega on Boole'i skeemi elementide arv $|\Gamma_0| + 1$.

Olgu **C** suvaline pääsustruktuuri Γ ära tundev monotoonne ühissalastusskeem. Järgnevalt toome algoritmi, mis võimaldab jagajal D konstrueerida pääsustruktuuri Γ realiseeriva ühissalastusskeemi. Konstrueeritavas ühissalastusskeemis kasutatakse ehitusplokina joonisel 1 toodud (t, t)-läviskeeme (st et $\mathcal{K} = \mathbb{Z}_m$, kus $m \in \mathbb{Z}^+$).

Algoritmi töö käigus omistatakse Boole'i skeemi **C** igale juhtmele W mingi väärtus $f(W) \in \mathcal{K}$. Algselt omistatakse skeemi **C** väljundjuhtmele W_{out} väärtus K. Algoritmi itereeritakse seni, kuni igale juhtmele on lõpuks omistatud mingi väärtus. Töö lõpus antakse igale osapoolele P_i nimistu väärtustest $f(W)$, kus W on Boole'i skeemi sisendjuhe, mille sisendiks on x_i. Algoritm on toodud joonisel 2.

Näide 3.3 *Vaatleme eelnevalt toodud näidet*

$$\Gamma_0 = \{\{P_1, P_2, P_3\}, \{P_2, P_4\}, \{P_1, P_4\}\}.$$

Olgu saladuseks K. Vastav Boole'i skeem on toodud joonisel 3. Algoritm annab väljundjuhtmele väärtuseks K. $\vee$-elemendi sisendjuhtmete väärtuseks on ka K.

Vaatleme nüüd näiteks vasakpoolseimat $\wedge$-elementi. Elemendi väljundjuhtme väärtus on K, sisendeid on 3. Seega genereeritakse kaks juhuslikku arvu a ning a', sisendjuhtmete väärtused on vastavalt a, a' ning $K - a - a'$. Analoogiliselt genereeritakse juhuarvud b ja c.

Algoritmi lõpus antakse osapoolele P_1 osa $\{a, c\}$, osapoolele P_2 osa $\{a', b\}$, osapoolele P_3 osa $\{K - a - a'\}$ ning osapoolele P_4 osa $\{K - b, K - c\}$.

Näitame, et saadud skeem on täielik. Esiteks, $\{P_1, P_2, P_3\}$ leiab K, kuna teab väärtusi a, a' ja $K - a - a'$. Hulk $\{P_2, P_4\}$ leiab K, kuna teab väärtusi b ja $K - b$. Hulk $\{P_1, P_4\}$ leiab K, kuna teab väärtusi c ja $K - c$; seega kõik Γ_0 hulgad leiavad K.

Olgu B mingi maksimaalne autoriseerimata alamhulk; näitame, et B ei leia K-d. Maksimaalseteks autoriseerimata alamhulkadeks on järgmised hulgad:

1. *$B = \{x_1, x_2\}$. Siin hulk B teab suurusi a, a', b ja c, mis on kõik juhuslikud suurused ja millest ei leki informatsiooni võtme K kohta.*

2. *$B = \{x_1, x_3\}$. Siin hulk B teab suurusi a, c, $K - a - a'$ ehk samaväärselt, B teab suurusi a, c, $K - a'$. Siin kaks esimest suurust on juhuslikud, kolmas aga K miinus juhuslik arv.*

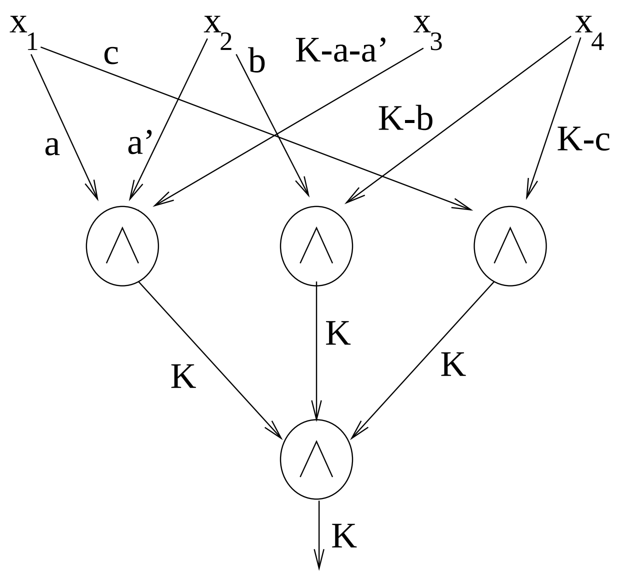
Algoritm 3.2

1. *$f(W_{out}) := K$*
2. ***while*** *leidub juhe W, et $f(W)$ ei ole defineeritud* ***do***
3. *leia element G, mille väljundjuhtmele W_G vastav $f(W_G)$ on defineeritud, kuid $f(W)$ on defineerimata kõigi selle elemendi sisendjuhtmete korral*
4. ***if*** *G on $\vee$-element* ***siis***
5. *$f(W) := f(W_G)$ elemendi G suvalise sisendjuhtme W jaoks*
6. ***else*** *(G on $\wedge$-element)*
7. *Olgu $W_1, \ldots, W_t$ elemendi G sisendjuhtmed*
   Vali hulgast $\mathbb{Z}_m$ (juhuslikult ja sõltumatult) $t-1$ elementi $y_{G,1}, \ldots, y_{G,t-1}$. Olgu

$$y_{G,t} := f(W_G) - \sum_{i=1}^{t-1} y_{G,i} \pmod{m}.$$

8. ***for*** *$1 \leq i \leq t$* ***do***
9. *$f(W_i) = y_{G,i}$*

Joonis 2: Monotoonsete Boole'i skeemide konstruktsioon



Joonis 3: Γ_0-ile vastav Boole'i skeem

3. $\{x_2, x_3\}$. *Analoogiline.*

4. $\{x_3, x_4\}$. *Analoogiline.*

Erinevad pääsustruktuurid saab, kui kasutame erinevaid Boole'i skeeme. Nii näiteks võib disjunktiivsele normaalkujule vastava Boole'i skeemi asemel tarvitada konjunktiivsele normaalkujule vastavat, aga ka suvalist teist, mis realiseerib antud Boole'i valemit.

Teoreem 3.4 *Olgu* $\mathbf{C}$ *mingi monotoonne Boole'i skeem. Monotoonse Boole'i skeemi konstruktsioon tagastab pääsustruktuuri* $\Gamma(\mathbf{C})$ *realiseeriva täieliku ühissalastusskeemi.*

Tõestus 3.5 *Tõestame teoreemi induktsiooniga üle skeemi* $\mathbf{C}$ *elementide arvu. Olgu skeemis* $\mathbf{C}$ *vaid üks element. Kui* $\mathbf{C}$ *on* $\vee$*-element, siis antakse kõigile osavõtjatele võti. See skeem realiseerib pääsustruktuuri, mis koosneb osapoolte kõikidest mittetühjadest alamhulkadest. Kui* $\mathbf{C}$ *on* $\wedge$*-element* t*-sisendiga, siis on antud skeem* (t,t)*-skeem, mis oli antud joonisel 1.*

Oletame nüüd, et täisarvu $j > 1$ *korral tagastab antud konstruktsioon kõikide skeemkeerukusega* $< j$ *Boole'i skeemide puhul ühissalastusskeemi, mis realiseerib* $\Gamma(\mathbf{C})$*. Olgu* $\mathbf{C}$ *suvaline Boole'i skeem skeemkeerukusega* j*. Vaatleme skeemi* $\mathbf{C}$ *viimast, väljund-, elementi* G*.* G *võib olla* $\vee$*-element või* $\wedge$*-element. Olgu* G $\vee$*-element. Tähistame elemendi* G *sisendjuhtmed kui* W_i*,* $1 \leq i \leq t$*. Juhtmed* W_i *on* t *alamskeemi* $\mathbf{C}_i$*,* $1 \leq i \leq t$*, väljundjuhtmeteks. Igale Boole'i skeemile* $\mathbf{C}_i$ *vastab induktsiooni põhjal ühissalastusskeem, mis realiseerib pääsustruktuuri*

$\Gamma(\mathbf{C}_i)$. *Triviaalselt* $\Gamma(\mathbf{C}) = \bigcup_{i=1}^{t} \Gamma(\mathbf{C}_i)$. *Kuna iga sisendjuhtme* W_i *väärtus on* K, *siis realiseerib antud ühissalastusskeem pääsustruktuuri* $\Gamma(\mathbf{C})$.

Juhul, kui G *on* $\wedge$*-element, saame analoogiliselt, et* $\Gamma(\mathbf{C}) = \bigcap_{i=1}^{t} \Gamma(\mathbf{C}_i)$. *Kuna võtit* K *jagatakse* t *sisendjuhtme* W_i *vahel, kasutades* (t,t)*-läviskeemi, saame, et antud ühissalastusskeem realiseerib pääsustruktuuri* $\Gamma(\mathbf{C})$.

Suvaline autoriseeritud alamhulk B peab teadma D poolt osade jaotamisel kasutatud Boole'i skeemi ning seda, millistele juhtmetele vastavad millised osad. Järelikult peab see informatsioon olema avalik. Võtme rekonstrueerimise algoritm sisaldab endas Boole'i skeemile vastavat osade kombineerimist, kus $\wedge$-element tähendab sisendite summeerimist $\pmod m$ ning $\vee$-element tähendab suvalise sisendjuhtme väärtuse valikut (eeldades, et kõik need väärtused on võrdsed).

4 Lõpetus

Sõnastame järgnevalt mõned ühissalastusskeemide kohta teadaolevad tulemused.

1. Ühissalastusskeemide rangemas definitsioonis on esitatud nõue, et suvalise autoriseerimata alamhulga B jaoks $p_{\mathcal{K}}(K|f_B) = p_{\mathcal{K}}(K)$, kus f_B on osade jaotus alamhulgale B. St, et teadaolevad osad mitte ainult ei tohi lubada otseselt leida võtit K; nende abil ei tohi muutuda ka B teadmus võtme K esinemistõenäosusest hulgas $\mathcal{K}$.

2. Monotoonsete Boole'i skeemide konstruktsiooni efektiivsus sõltub oluliselt kasutatavast skeemist. Näiteks, (t,w)-läviskeemi jaoks saab konstrueerida Boole'i valemi disjunktiivsele normaalkujule vastava Boole'i skeemi, mille skeemkeerukus on $1+\frac{w}{t}$. Iga osapool saab $\frac{w-1}{t-1}$ elementi hulgast $\mathbb{Z}_m$. Samas Shamiri (t,w)-läviskeemi kasutades saab iga osapool vaid ühe "võtmetüki".

   Olgu $\rho = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}(P_i)|}$, kus $\mathcal{S}(P_i)$ tähistab P_i-le antavate tükkide hulka. Suvalise monotoonse Boole'i skeemi jaoks leidub teda realiseeriv ühissalastusskeem, mille korral $\rho = \max\{1/r_i \colon 1 \leq i \leq w\}$ ning r_i on Boole'i skeemi $\mathbf{C}$ sisendjuhtmete arv, mille sisendiks on x_i.

   Suvalist pääsusstruktuuri Γ realiseeriva täieliku ühissalastusskeemi korral $\rho \leq 1$.

3. Mõningal juhul saab ideaalseid ühissalastusskeeme konstrueerida, kasutades nn Brickelli vektorruumi konstruktsiooni ([Bri89]).

4. Leiduvad teatud "lisaväärtusega" ühissalastusskeemid, üks huvitavamaid neist on juht, kus üks või rohkem autoriseeritud osapooli ja/või jagaja on ebaausad.

Üks huvitavaid ideid on visuaalne krüptograafia ([NS95]), mida kasutatakse piltide jagamiseks ning krüptimiseks. Pilt jagatakse kaheks või enamaks pildiks, millest igaüks sisaldab osa igast lähtepildi pikselist. Iga algpiksel jaotatakse sobiva suurusega alampikseliteks, valides alampikselite värvid nii, et erinevaid osi kandvate kilede teineteise peale asetamisel tunneb silm ära lähtepildi. Sealjuures näib iga osa täiesti juhuslik. Pildi taastamine ei nõua arvutamist (on puhtvisuaalne). Ükski autoriseerimata hulk ei näe (tõestatavalt) mitte midagi kasulikku.

Viited

[BL90] J. Benaloh and J. Leichter. Generalized Secret Sharing Schemes and Monotone Functions. In *Advances on Cryptology — CRYPTO '88*, pages 27–35, 1990. Lecture Notes in Computer Science No. 403.

[Bri89] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9:105–113, 1989.

[NS95] M. Naor and Adi Shamir. Visual Cryptography. In *Proc. EUROCRYPT 94*, pages 1–12. Springer, 1995. Lecture Notes in Computer Science No. 950.

[Sha79] Adi Shamir. How to Share a Secret. *Communications of the ACM*, 22:612–613, 1979.