Tüübisüsteem arvutuslikult turvalise infovoo jaoks

Peeter Laud

(koostöös Varmo Venega)

Krüptosüsteemi turvalisusest

Sümmeetrilise krüptosüsteemi $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ turvalisus:

- Keskkond genereerib võtme $k \leftarrow \mathcal{K}$ ja salajase biti $b \in_R \{0,1\}$.
- Ründaja $\mathcal{A}$ töötab.
  - Võib esitada keskkonnale päringuid $x \in \{0,1\}^*$.
  - Keskkond leiab $y = \mathcal{E}(k, x; random)$, vastab y.
    - Kirjutame $y \leftarrow \mathcal{E}(k, x)$.
- $\mathcal{A}$ väljastab kaks ühepikkust teadet m_0 ja m_1.
- Keskkond leiab $y \leftarrow \mathcal{E}(k, m_b)$, annab y ründajale.
- Ründaja töötab (võib esitada päringuid...).
- Ründaja väljastab $b^* \in \{0,1\}$.
- Ründaja eelis: $\mathbf{Adv}_{\mathcal{A}}^{\text{IND-CPA}} = |\Pr[b = b^*] - 1/2|$.

Krüptosüsteemi turvalisusest

- $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ on (τ, ε)-turvaline, kui $\mathbf{Adv}_{\mathcal{A}} \leq \varepsilon$ iga $\mathcal{A}$ jaoks, mis teeb ülimalt τ sammu.
  - Loeme, et iga päring keskkonnale võtab ühe sammu.
- Arvutusvõimsuse kasvades on τ sammu mingil hetkel tehtav.
  - (τ, ε)-turvalisus pole siis enam piisav.
- Kas siis disainime uue krüptosüsteemi?
- Oleks hea, kui süsteemil oleks mingi turvaparameeter $\eta \in \mathbb{N}$, mida suurendades süsteemi turvalisus suureneb.
  - η on ilmselt kuidagi seotud võtmepikkusega.
- $\mathcal{K}$, $\mathcal{E}$ ja $\mathcal{D}$ saavad täiendava argumendi η.
- Kuidas peaksid τ ja ε η-st sõltuma?

Asümptootiline turvalisus

- Ründaja $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ eelis $\mathbf{Adv}_{\mathcal{A}}^{\text{IND-CPA}}(\eta) = |\Pr[b = b^*] - 1/2|$, kus
  - $k \leftarrow \mathcal{K}(\eta)$, $b \in_R \{0, 1\}$,
  - $(m_0, m_1, state) \leftarrow \mathcal{A}_1^{\mathcal{E}(\eta,k,\cdot)}(\eta)$,
  - $y \leftarrow \mathcal{E}(\eta, k, m_b)$, $b^* \leftarrow \mathcal{A}_2^{\mathcal{E}(\eta,k,\cdot)}(\eta, y, state)$.
- $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ on IND-CPA-turvaline, kui iga polünomiaalses ajas töötava $\mathcal{A}$ jaoks on $\mathbf{Adv}_{\mathcal{A}}^{\text{IND-CPA}}$ kaduvväike.
  - Max. sammude arv on funktsioon η-st.
- Funktsioon $f : \mathbb{N} \to \mathbb{R}$ on kaduvväike kui $f = o(1/p)$ iga positiivsete kordajatega polünoomi p jaoks.

Samaväärne turvadefinitsioon

- Keskkond genereerib $k \leftarrow \mathcal{K}(\eta)$ ja $b \in_R \{0,1\}$.
- $\mathcal{A}(\eta)$ töötab (pol. ajas). Seejuures võib esitada keskkonnale päringuid $x \in \{0,1\}^*$.
  - Kui $b = 0$, siis keskkond leiab $y \leftarrow \mathcal{E}(\eta, k, x)$ ja tagastab y.
  - Kui $b = 1$, siis keskkond leiab $y \leftarrow \mathcal{E}(\eta, k, \mathbf{0}^{|x|})$ ja tagastab y.
- $\mathcal{A}$ üritab b-d ära arvata.
- $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ on IND-CPA-turvaline, kui kõigi pol. ajas töötavate ründajate jaoks on nende b äraarvamise eelis kaduvväike.

Võtme identiteet

- Kui meil on süsteemis mitu erinevat võtit, siis me võime tahta varjata, millise võtmega mingi šiffertekst loodud on.
- Katse: $k \leftarrow \mathcal{K}(\eta)$, $k' \leftarrow \mathcal{K}(\eta)$, $b \in_R \{0,1\}$.
- $\mathcal{A}(\eta)$ töötab. Lubatud päringud: $(x,s) \in \{0,1\}^* \times \{1,2\}$. Päringuvastus y leitakse järgmiselt:

$$y \leftarrow \begin{cases} \mathcal{E}(\eta,k,x), & b=0 \ \& \ s=1 \\ \mathcal{E}(\eta,k',x), & b=0 \ \& \ s=2 \\ \mathcal{E}(\eta,k,\mathbf{0}^{|x|}), & b=1 \ . \end{cases}$$

- $\mathcal{A}$ üritab b-d ära arvata. Kui eelis kõigi $\mathcal{A}$-de jaoks kaduvväike, siis on $(\mathcal{K},\mathcal{E},\mathcal{D})$ IND-CPA-turvaline ja varjab võtme identiteeti.

Avateksti pikkus

- Me võime tahta ka avateksti pikkust varjata. See on saavutatav kõigi avatekstide polsterdamisega mingi pikkuseni $\ell(\eta)$.
- Katse: nagu eelmiselgi kilel. y leitakse järgmiselt:

$$y \leftarrow \begin{cases} \mathcal{E}(\eta, k, x), & b = 0 \ \& \ s = 1 \\ \mathcal{E}(\eta, k', x), & b = 0 \ \& \ s = 2 \\ \mathcal{E}(\eta, k, \mathbf{0}^{\ell(\eta)}), & b = 1 \ . \end{cases}$$

- Kui kõigi pol. ajas töötavate ründajate jaoks on b äraarvamise eelis kaduvväike, siis on $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ IND-CPA-turvaline ja varjab võtme identiteeti ning avateksti pikkust.
  - Seda omadust nimetame tüüp-0 turvalisuseks.

Tõenäosusjaotuste perede eristamatus

- Olgu $\mathcal{D}(X)$ kõigi tõenäosusjaotuste hulk üle hulga X.
- Olgu $D_\eta, D'_\eta \in \mathcal{D}(\{0,1\}^*)$, kus $\eta \in \mathbb{N}$.
- Olgu $\mathcal{A}$ mingi ründaja. Vaatame järgmist katset:
  - $b \in_R \{0,1\}$. Kui $b = 0$, siis $x \leftarrow D_\eta$, muidu $x \leftarrow D'_\eta$.
  - $b^* \leftarrow \mathcal{A}(\eta, x)$.
- Kui $|\Pr[b = b^*] - 1/2|$ on kaduvväike iga pol. ajas töötava ründaja $\mathcal{A}$ jaoks, siis ütleme, et D ja D' on (arvutuslikult) eristamatud. Tähistame $D \approx D'$.
- Arvutuslik eristamatus on krüptograafiline vaste võrdsusele. Muuhulgas on $\approx$ ekvivalentsiseos.

Uurimisobjekt

- Uurime (arvuti)süsteeme, mis peavad rahuldama teatud turvaomadusi ka teatud rünnete all.
- Antud töös uurime ainult konfidentsiaalsust ja passiivseid ründeid.
- S.t. ründaja näeb süsteemi väljundeid ja üritab selle põhjal salajaste sisendite kohta midagi teada saada.
- Süsteemi käitumist võib kirjeldada mingi programmiga.
- Me uurime seda programmi. Eeldame, et tema tekst on antud.

Probleemikirjeldus

- Antud programm. Ta saab mingid sisendid ja produtseerib mingid väljundid.
- Mõned väljundid tehakse avalikuks. Mõned sisendid on salajased.
- Tahame, et salajased sisendid avalikke väljundeid märgatavalt ei mõjutaks.
- Programm võib kasutada sümmeetrilist šifreerimist.
- Lubame märkamatut mõjutamist, näiteks salajaste sisendite šifreerimist.

Programmid

$$
\begin{array}{rcl}
\mathsf{P} & ::= & x := o(x_1, \ldots, x_k) \\
& | & \mathit{skip} \\
& | & \mathsf{P}_1; \mathsf{P}_2 \\
& | & \mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2 \\
& | & \mathit{while}\ b\ \mathit{do}\ \mathsf{P}_1
\end{array}
$$

- Olgu $\mathbf{Var}$ muutujate hulk. Olgu $\mathbf{Var}_{\mathrm{S}} \subseteq \mathbf{Var}$ alguses salajaste muutujate hulk ja $\mathbf{Var}_{\mathrm{P}} \subseteq \mathbf{Var}$ lõpuks avalikustatavate muutujate hulk.
- o võib olla $\mathcal{E}nc$, $\mathcal{G}en$ või mõni teine operatsioon.
  - $\mathcal{G}en$ (nullaarne) — loob uue võtme;
  - $\mathcal{E}nc$ (binaarne) — sümmeetriline šifreerimine;
  - dešifreerimine ei vaja eraldi käsitlemist.

Semantika

- Programmi olek on hulgast $\mathbf{State} = \mathbf{Var} \to \mathbf{Val}$.
- $\mathbf{Val}$ — väärtuste hulk. Meil $\mathbf{Val} = \{0,1\}^*$.
- Iga k-aarse operatsiooni o jaoks olgu fikseeritud tema semantika $[\![o]\!] : \mathbf{Val}^k \to \mathcal{D}(\mathbf{Val})$.
- programmikonfiguratsioon on paar (veel jooksutada jäänud) programmist ja programmiolekust.
  - Töö lõpetanud programmi konfiguratsiooniks on lihtsalt üks programmiolek.
- Programmi semantika seab programmikonfiguratsioonide paaridele vastavusse tõenäosuse, et ühe sammuga minnakse esimesest konfiguratsioonist teise.
  - Kirjutame $C_1 \xrightarrow{p} C_2$.

Relatsioon $\longrightarrow$

$$\langle x := o(x_1, \ldots, x_k), S\rangle \xrightarrow{p} S[x \mapsto v] \text{ kus } p = [\![o]\!](S(x_1), \ldots, S(x_k))(v)$$

$$\langle skip, S\rangle \xrightarrow{1} S \qquad \frac{\langle \mathsf{P}_1, S\rangle \xrightarrow{p} S'}{\langle \mathsf{P}_1; \mathsf{P}_2, S\rangle \xrightarrow{p} \langle \mathsf{P}_2, S'\rangle} \qquad \frac{\langle \mathsf{P}_1, S\rangle \xrightarrow{p} \langle \mathsf{P}'_1, S'\rangle}{\langle \mathsf{P}_1; \mathsf{P}_2, S\rangle \xrightarrow{p} \langle \mathsf{P}'_1; \mathsf{P}_2, S'\rangle}$$

$$\frac{S(b) = \mathsf{true}}{\langle \mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2, S\rangle \xrightarrow{1} \langle \mathsf{P}_1, S\rangle}$$

$$\frac{S(b) = \mathsf{false}}{\langle \mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2, S\rangle \xrightarrow{1} \langle \mathsf{P}_2, S\rangle}$$

$$\frac{S(b) = \mathsf{true}}{\langle \mathit{while}\ b\ \mathit{do}\ \mathsf{P}_1, S\rangle \xrightarrow{1} \langle \mathsf{P}_1; \mathit{while}\ b\ \mathit{do}\ \mathsf{P}_1, S\rangle}$$

$$\frac{S(b) = \mathsf{false}}{\langle \mathit{while}\ b\ \mathit{do}\ \mathsf{P}_1, S\rangle \xrightarrow{1} S}$$

Programmijooksud

- Programmijooks R on järjend kujul
  $C_0 \xrightarrow{p_1} C_1 \xrightarrow{p_2} \dots \xrightarrow{p_n} C_n$, kus
  - $C_0, \dots, C_{n-1}$ on programmikonfiguratsioonid;
  - C_n on programmiolek;
- Programmijooksu tõenäosus $\Pr[R] = \prod_{i=1}^{n} p_i$.
- Olgu $\mathbf{R}_n(C)$ kõigi programmijooksude hulk, mis algavad konfiguratsioonist C ja mille pikkus on ülimalt n.
- Olgu $\mathbf{R}_n(C; S)$ kõigi programmijooksude hulk, mis algavad konfiguratsioonist C, lõppevad olekus S ja mille pikkus on ülimalt n.

Programmi töö tulemus

- Olgu $\mathbf{State}_\perp = \mathbf{State} \dot\cup \{\perp\}$. Siin $\perp$ tähistab mittetermineerumist.
- Olgu P programm ja S_0 programmikonfiguratsioon. Siis $D = [\![P]\!](S_0) \in \mathcal{D}(\mathbf{State}_\perp)$, kus iga $S \in \mathbf{State}$ jaoks

$$D(S) = \sum_{R \in \mathbf{R}_\infty(\langle P, S_0 \rangle; S)} \Pr[R] \ .$$

ja $D(\perp)$ on võrdne ülejäänud osaga tõenäosusest.

$\mathcal{G}en$ ja $\mathcal{E}nc$ semantika

- Olgu $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ tüüp-0 turvaline.
- Tahame võtta $[\![\mathcal{G}en]\!] = \mathcal{K}$ ja $[\![\mathcal{E}nc]\!] = \mathcal{E}$.
- Mis saab turvaparameetrist η?

$\mathcal{G}en$ ja $\mathcal{E}nc$ semantika

- Olgu $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ tüüp-0 turvaline.
- Tahame võtta $[\![\mathcal{G}en]\!] = \mathcal{K}$ ja $[\![\mathcal{E}nc]\!] = \mathcal{E}$.
- Mis saab turvaparameetrist η?
- Lisandub igale poole.
- Meil on $[\![o]\!]_\eta$, $\xrightarrow[\eta]{}$, $R_{\eta,n}(C)$, $[\![P]\!]_n$.

Turvadefinitsioon

- Ründaja näeb
  - $\mathbf{Var}_{\mathrm{P}}$-sse kuuluvate muutujate lõppväärtusi;
  - programmi tööaega (või mittetermineerumist).
- Turvadefinitsioonis tahame me arvestada lõppväärtustega, aga mitte tööajaga.
  - Kui tahaks tööaega ka arvesse võtta, siis võib programmi lisada operatsioonide arvu loenduri ja selle lõpuks väljastada.
- Olgu $D_\eta \in \mathcal{D}(\mathbf{State})$ programmi sisendite jaotus. Programmil P on arvutuslikult turvaline infovoog (sisendite jaotuse D jaoks), kui

$$\{\!|(S_\eta|_{\mathbf{Var}_{\mathrm{S}}}, S'_\eta|_{\mathbf{Var}_{\mathrm{P}}}) \;:\; S_\eta \leftarrow D_\eta, S'_\eta \leftarrow [\![P]\!]_\eta(S_\eta)|\!\}_\eta \approx$$

$$\{\!|(S_\eta|_{\mathbf{Var}_{\mathrm{S}}}, S'_\eta|_{\mathbf{Var}_{\mathrm{P}}}) \;:\; S_\eta, S''_\eta \leftarrow D_\eta, S'_\eta \leftarrow [\![P]\!]_\eta(S''_\eta)|\!\}_\eta$$

Programmi tööaeg

- Mis siis saab, kui $[\![P]\!]_\eta(S_\eta)$-st valitakse $\perp$?
- Ütleme, et programm P töötab oodatult polünomiaalses ajas, kui leiduvad
  - polünoom q,
  - kaduvväike funktsioon α,

  nii et iga $S \in \mathbf{State}$ jaoks oleks

$$\sum_{R \in \mathbf{R}_{\eta,q(\eta)}(\langle P,S \rangle)} \Pr[R] \geq 1 - \alpha(\eta) \quad .$$

- Siis võime lugeda, et $[\![P]\!]_\eta : \mathbf{State} \to \mathcal{D}(\mathbf{State})$.
- Uurime ainult oodatult polünomiaalses ajas töötavaid programme.

Programmi sisendite jaotus

- $\mathbf{Var}_{\mathrm{S}}$-i kuuluvate muutujate algväärtused on salajased.
- Aga teiste muutujate algväärtused?
- D võib olla selline, et teiste muutujate algväärtustest saab leida $\mathbf{Var}_{\mathrm{S}}$-i kuuluvate muutujate algväärtusi.
- Selliseid D-sid me ei uuri.
- Nõuame, et

$$\{\!|(S_\eta|_{\mathbf{Var}_{\mathrm{S}}}, S_\eta|_{\mathbf{Var}\setminus\mathbf{Var}_{\mathrm{S}}}) \;:\; S_\eta \leftarrow D_\eta|\!\} \approx$$
$$\{\!|(S_\eta|_{\mathbf{Var}_{\mathrm{S}}}, S'_\eta|_{\mathbf{Var}\setminus\mathbf{Var}_{\mathrm{S}}}) \;:\; S_\eta, S'_\eta \leftarrow D_\eta|\!\}$$

- Nõuame ka, et D oleks polünomiaalses ajas konstrueeritav — leidub selline pol. ajas töötav algoritm $\mathcal{D}$, et $\mathcal{D}(\eta)$ väljundi jaotus oleks D_η.

Tüübid

- Tüüpimine γ seab igale muutujale vastavusse mingi tüübi.
- Tüübid kirjeldavad informatsiooni, mis sinna muutujasse võib voolata. Samuti kirjeldavad nad, kas see muutuja on kasutatav šifreerimisvõtmena.
  - S.t. tüüp $\gamma(x)$ on paar $\langle \gamma_I(x), \gamma_U(x) \rangle$.
- Tüüpide hulk on järjestatud, leiduvad ülemised rajad.
- Tüüpide hierarhias kõrgemale minek tähendab sõltuvust rohkemast informatsioonist.
- Programmi tekstist tuletatud tüüpimisreeglid seavad tüüpimistele kitsendusi — mitte iga tüüpimine pole korrektne.

Korrektsusteoreem

- Tüüpide hierarhias leidub tüüp h, mis vastab salajasele informatsioonile.
- Teoreem: Kui programmil P leidub selline korrektne tüüpimine γ, et
  - $\gamma_I(x) \geq h$ iga $x \in \mathbf{Var}_{\mathrm{S}}$ jaoks,
  - $\bigvee_{x \in \mathbf{Var}_{\mathrm{P}}} \gamma_I(x) \not\geq h$,

  siis on programmil P arvutuslikult turvaline infovoog.

nformatsioonitüübid — esmased saladuse

- Olgu $\mathcal{G}$ kõigi võtmegenereerimiste hulk programmis P.
  - $\mathcal{G}$ on nende programmipunktide hulk P-s, kus esineb operaator $\mathcal{G}en$.
  - Edaspidi tähistame $\mathcal{G}$ elemente naturaalarvudega.
- Esmased saladused: $\mathcal{T}_0 = \{h\} \dot{\cup} \mathcal{G}$.
  - $\gamma_I(x) \geq h$ tähendab, et x-st võib ehk leida midagi salajaste sisendite kohta.
  - $\gamma_I(x) \geq g \in \mathcal{G}$ tähendab, et x-st võib ehk leida midagi mõne võtme kohta, mis on genereeritud punktis g.
  - Paneme tähele, et tüübisüsteem ei suuda vahet teha erinevatel võtmetel, mis on samas punktis genereeritud :(

Informatsioonitüübid

- $\mathfrak{T}_1 = \{t_N \,:\, t \in \mathfrak{T}_0, N \subseteq \mathcal{G}\}$.
- $\gamma_I(x) \geq t_N$ tähendab, et x-st võib ehk leida informatsiooni tüüpi t, kui meil oleks võtmed, mis on genereeritud punktides N (mõni võti igast punktist).
- Järjestus: $t_N \leq t'_{N'}$, kui $t = t'$ ja $N \supseteq N'$.
- $\mathfrak{T}_2 = \mathcal{P}(\mathfrak{T}_1)$. $\mathfrak{T}_2$, kus osad elemendid on samastatud, ongi informatsioonitüüpide hulk.
- $\gamma_I(x) \geq T \in \mathfrak{T}_2$ tähendab, et iga $t_N \in T$ jaoks võib ehk x-st leida informatsiooni, mis vastab t_N-le.
- Järjestus: $T \leq U$, kui $\forall t_N \in T\ \exists t'_{N'} \in U$: $t_N \leq t'_{N'}$.
- Kui $T \leq U$ ja $U \leq T$, siis loeme T ja U samaks.

Dekrüptimine $\mathcal{T}_2$-s

- Olgu $T \in \mathcal{T}_2$ ja $g \in \mathcal{G}$. Olgu $t_{\{g\}}, g_\emptyset \in T$ ja $g \in N$.
- S.t. muutujast tüüpi T võiks leida informatsiooni, mis vastab t-le, kui meil oleks võti, mis on genereeritud punktis g.
- Aga selline võti on meil olemas.
- Seega võib T-st leida informatsiooni, mis vastab t-le. S.t. T ja $T \cup \{t_\emptyset\}$ võib samaks lugeda.
- Üldjuhul: kui $t_N, g_\emptyset \in T$, siis T on sama, mis $T \cup \{t_{N \setminus \{g\}}\}$.

Krüptimistsüklid

- Olgu $k \leftarrow \mathcal{K}(\eta)$ ja $y \leftarrow \mathcal{E}(\eta, k, k)$. Kas y-st on leitav k?
- Tüüp-0 turvalisuse definitsioon ei ütle, et ei ole.
- S.t. kui $T \in \mathcal{T}_2$ ja $g_{\{g\}} \in T$, siis T on sama, mis $T \cup \{g_\emptyset\}$.
- Üldisemalt, iga $T \in \mathcal{T}_2$ defineerib teatud suunatud graafi tipuhulgaga $\mathcal{G}$.
- Kaared: kui $g_N \in T$ ja $g' \in N$, siis on kaar g'-st g-sse.
- Selle graafi suunatud tsüklitest võib olla võimalik kasulikku informatsiooni leida.
- See peab kajastuma ekvivalentsis, millega $\mathcal{T}_2$-e faktoriseeritakse.
  - Iga $\mathcal{T}_2$-e element on ekvivalentne mõne elemendiga, mis on vähemalt sama suur kui tema, ja mille graafis pole suunatud tsükleid.

$T \in \mathcal{T}_2$-st leitavad võtmed

- Olgu $I \subseteq \mathcal{G}$ suurim selline hulk, mis rahuldab järgmist tingimust:

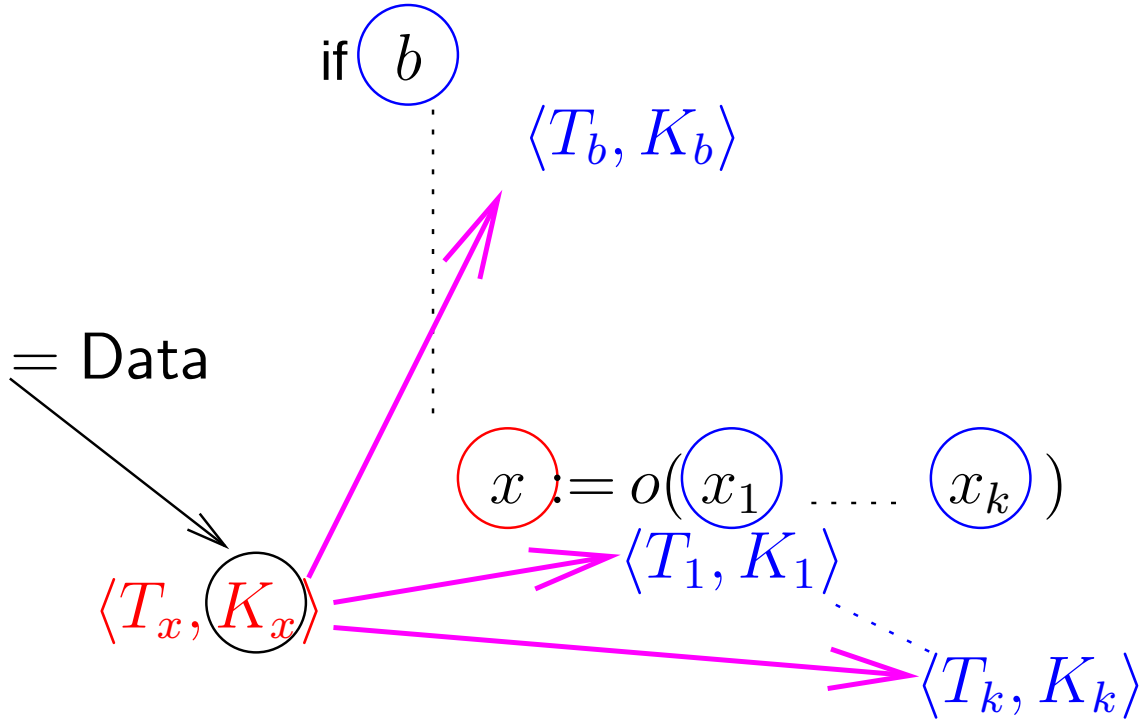
$$\forall g \in \mathcal{G} : \Big(\big(\forall t_N \in T : t \neq g \vee N \not\subseteq I \big) \Rightarrow g \notin I \Big)$$

- I leidmiseks initsialiseerime $I = \mathcal{G}$ ja siis hakkame I-st võtmeid kustutama.
- I on kõigi nende võtmete hulk, mis võib ehk T-st leitav olla.
- T on samaväärne tüübiga $\{g_\emptyset : g \in I\} \cup \{t_{N \setminus I} : t_N \in T\}$.

Kasutustüübid

- $\gamma_U(x)$ näitab, kas x on võtmena kasutatav, ning kui jah, siis kus x loodud võib olla.
- Tüübid:
  - Data — ei ole võti;
  - Key_N, kus $N \subseteq \mathcal{G}$ — võti, mis on loodud ühes punktidest N.
- Kogu muutujatüüp on mingi $\langle T, K \rangle$.
- Järjestus:
  - $\langle T, \mathsf{Data} \rangle \leq \langle T', \mathsf{Data} \rangle$, kui $T \leq T'$.
  - $\langle T, \mathsf{Key}_N \rangle \leq \langle T', \mathsf{Key}_{N'} \rangle$, kui $T \leq T'$ ja $N \subseteq N'$.
  - $\langle T, \mathsf{Key}_N \rangle \leq \langle T', \mathsf{Data} \rangle$, kui $T \vee \{g_\emptyset : g \in N\} \leq T'$.

Kitsendused: üldine omistamine



- Siin $\rightarrow$ tähendab $\geq$.
- Järgnevatel slaididel on toodud erijuhud, mis panevad tüüpide peale nõrgemad tingimused.

Üldine omistamine

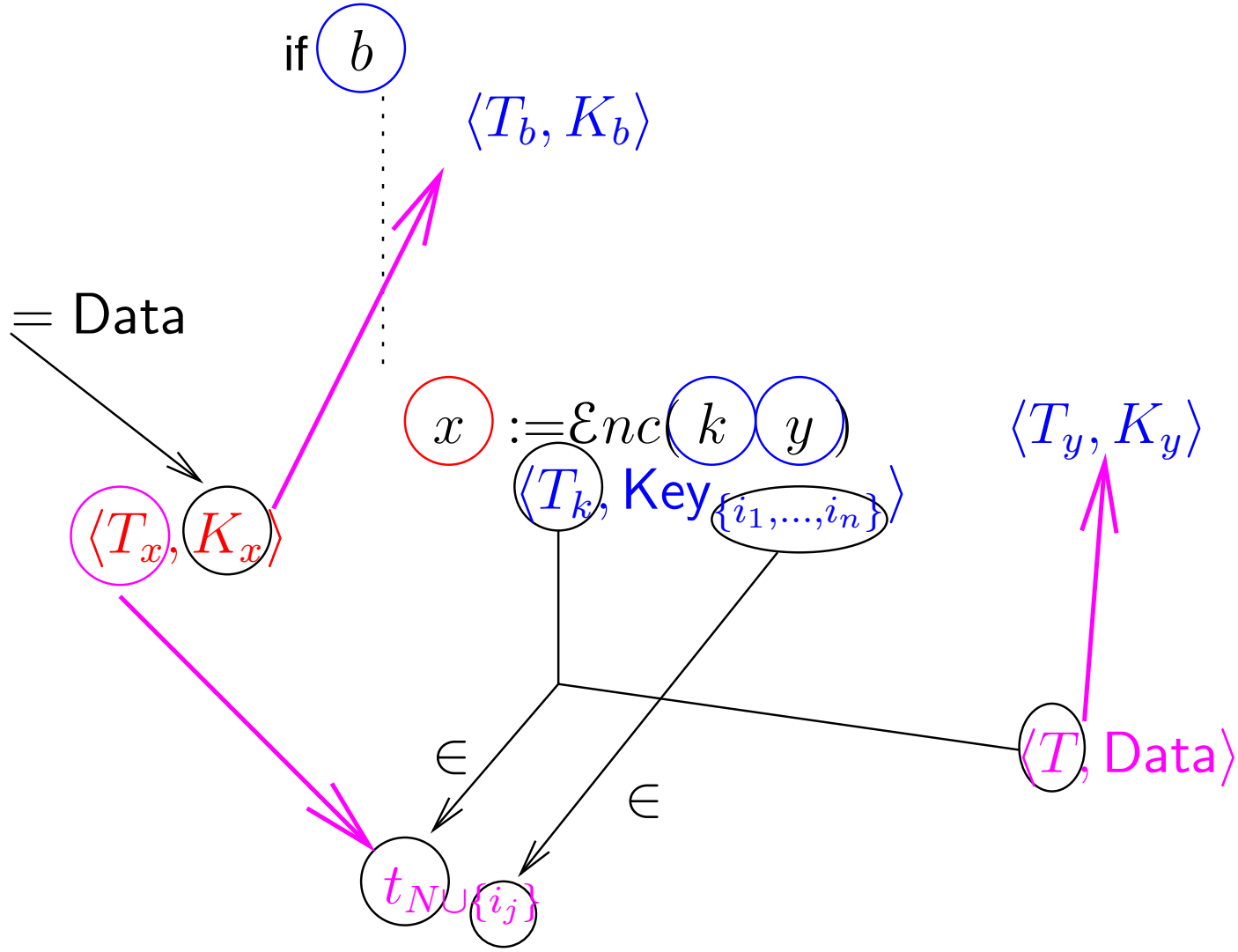
$if\ b\ \ldots\ x := o(x_1, \ldots, x_k)\ \ldots$

$$\gamma(x) \geq \gamma(x_i)$$

$$\gamma(x) \geq \gamma(b)$$

$$\gamma_U(x) = \mathsf{Data}$$

Šifreerimised



Šifreerimised

$if\ b\ \ldots\ x := \mathcal{E}nc(k, y)\ \ldots$

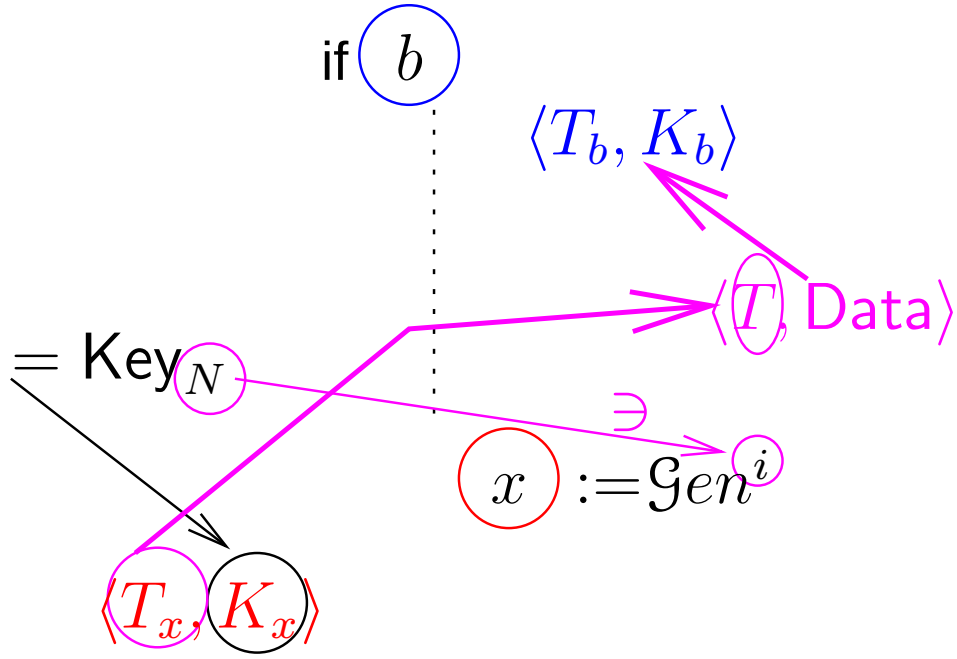
Olgu $\gamma(x) = \langle T_x, K_x \rangle$, $\gamma(k) = \langle T_k, \mathsf{Key}_N \rangle$, $\gamma(y) \leq \langle T_y, \mathsf{Data} \rangle$, $\gamma(b) \leq \langle T_b, \mathsf{Data} \rangle$.

$$K_x = \mathsf{Data}$$

$$T_x \geq T_b$$

$$T_x \geq \{t_{M \cup \{g\}} \ : \ t_M \in T_y \cup T_k, g \in N\}$$

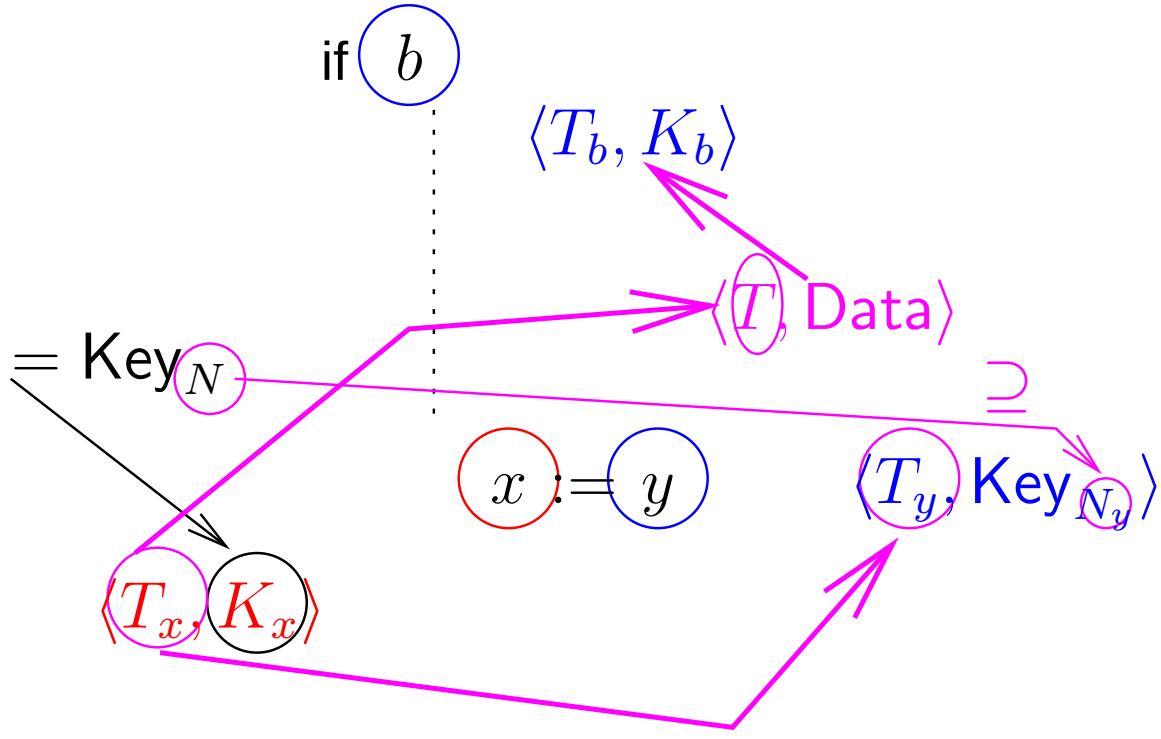
Võtmegenereerimised



$$T_x \geq T \quad \text{kus} \quad \langle T, \mathsf{Data} \rangle \geq \gamma(b)$$

$$K_x = \mathsf{Key}_N \quad \text{ja} \quad i \in N$$

Ühe võtme teisele omistamised



$$\gamma(x) \geq \gamma(y)$$

$$T_x \geq T \quad \text{kus} \quad \langle T, \text{Data} \rangle \geq \gamma(b)$$

Korrektsuse teoreem

- Olgu $\mathbf{Var}_\mathrm{I} \subseteq \mathbf{Var}$ kõigi sisendmuutujate hulk, s.t. selliste muutujate, mille algväärtust võidakse programmis kasutada.
- Kui P-l on korrektne tüüpimine γ, nii et
  - $\gamma(x) \geq \langle \{h_\emptyset\}, \mathsf{Data} \rangle$ kõigi $x \in \mathbf{Var}_\mathrm{S}$ jaoks,
  - $\gamma(x) \geq \langle \emptyset, \mathsf{Data} \rangle$ kõigi $x \in \mathbf{Var}_\mathrm{P} \cup \mathbf{Var}_\mathrm{I}$ jaoks,
  - $\bigvee_{x \in \mathbf{Var}_\mathrm{P}} \gamma_I(x) \not\geq \{h_\emptyset\}$,

  siis on P-l arvutuslikult turvaline infovoog.
- S.t. programmi sisendid ja avalikud väljundid ei tohi olla võtmed.
  - Võtmed sisenditeks — lisa programmi ette vastavad võtmegenereerimised.
  - Võtmed avalikeks väljunditeks — omista teisele muutujale.

Näide

$k := \mathcal{G}en^1$

$if\ b\ then$

$\quad k' := k$

$\quad y := \mathcal{G}en^2$

$else$

$\quad k' := \mathcal{G}en^3$

$\quad y := \mathcal{G}en^4$

$z := o(y)$

$x := \mathcal{E}nc(k', z)$

$u := \mathcal{E}nc(k, z)$

Näide

$k := \mathcal{G}en^1$

if b *then*

  $k' := k$

  $y := \mathcal{G}en^2$

else

  $k' := \mathcal{G}en^3$

  $y := \mathcal{G}en^4$

$z := o(y)$

$x := \mathcal{E}nc(k', z)$

$u := \mathcal{E}nc(k, z)$

$b : \langle \{h_\emptyset\}, \mathsf{Data} \rangle$

$k : \langle \emptyset, \mathsf{Key}_{\{1\}} \rangle$

$k' : \langle \{h_\emptyset\}, \mathsf{Key}_{\{1,3\}} \rangle$

$y : \langle \{h_\emptyset\}, \mathsf{Key}_{\{2,4\}} \rangle$

$z : \langle \{h_\emptyset, 2_\emptyset, 4_\emptyset\}, \mathsf{Data} \rangle$

$x : \langle \{h_{\{1\}}, h_{\{3\}}, 2_{\{1\}}, 2_{\{3\}}, 4_{\{1\}}, 4_{\{3\}}\}, \mathsf{Data} \rangle$

$u : \langle \{h_{\{1\}}, 2_{\{1\}}, 4_{\{1\}}\}, \mathsf{Data} \rangle$

Teine näide

$k := \mathcal{G}en^1$

$x := \mathcal{E}nc(k, y)$

$g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$

$while\ g\ do$

$\quad x := \mathcal{E}nc(k, y)$

$\quad g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$

Teine näide

$k := \mathcal{G}en^1$

$x := \mathcal{E}nc(k, y)$

$g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$

while g *do*

$x := \mathcal{E}nc(k, y)$

$g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$

s:$\langle \{h_\emptyset\}, \mathsf{Data} \rangle$

y:$\langle \emptyset, \mathsf{Data} \rangle$

k:$\langle \emptyset, \mathsf{Key}_{\{1\}} \rangle$

g:$\langle \{h_\emptyset\}, \mathsf{Data} \rangle$

x:$\langle \{h_\emptyset\}, \mathsf{Data} \rangle$

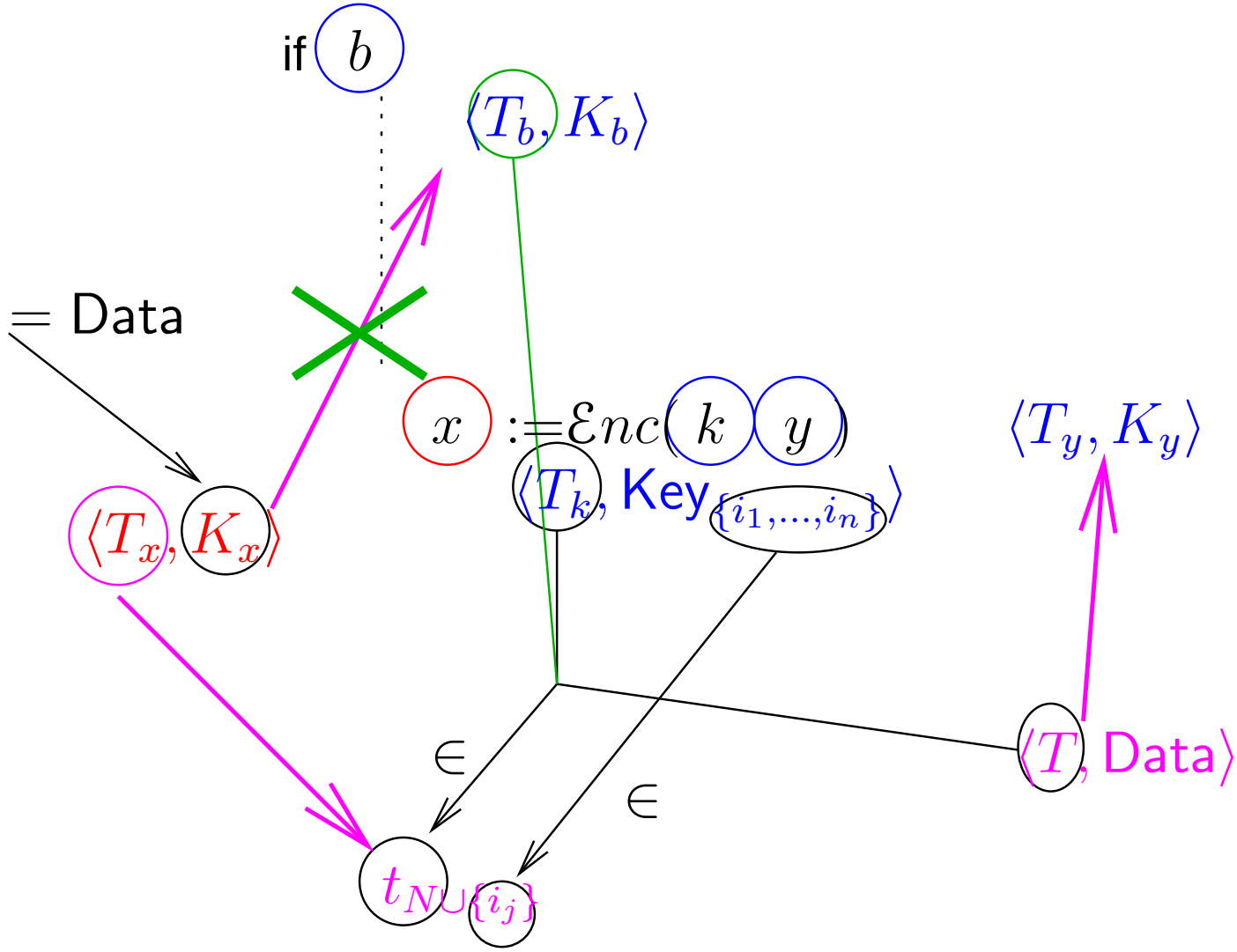
Teine näide

$k := \mathcal{G}en^1$
$x := \mathcal{E}nc(k, y)$
$g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$
$while\ g\ do$
  $x := \mathcal{E}nc(k, y)$
  $g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$

s:$\langle\{h_\emptyset\}, \mathsf{Data}\rangle$
y:$\langle\emptyset, \mathsf{Data}\rangle$
k:$\langle\emptyset, \mathsf{Key}_{\{1\}}\rangle$
g:$\langle\{h_\emptyset\}, \mathsf{Data}\rangle$
x:$\langle\{h_\emptyset\}, \mathsf{Data}\rangle$

Kui tsüklitingimusest (g) tuletatav informatsioon ka šiffertekstidest (x) tuletatava informatsiooni sisse šifreeritult läheks, siis...

Šifreerimised



Teine näide

$k := \mathcal{G}en^1$
$x := \mathcal{E}nc(k, y)$
$g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$
$while\ g\ do$
  $x := \mathcal{E}nc(k, y)$
  $g := (\mathsf{lsb}_{10}(s) \neq \mathsf{lsb}_{10}(x))$

s:$\langle\{h_\emptyset\}, \mathsf{Data}\rangle$
y:$\langle\emptyset, \mathsf{Data}\rangle$
k:$\langle\emptyset, \mathsf{Key}_{\{1\}}\rangle$
g:$\langle\{h_\emptyset\}, \mathsf{Data}\rangle$
x:$\langle\{h_{\{1\}}\}, \mathsf{Data}\rangle$

Kui tsüklitingimusest (g) tuletatav informatsioon ka šiffertekstidest (x) tuletatava informatsiooni sisse šifreeritult läheks, siis...

Tõestuse idee

- Näitame, et leidub programm P', nii et
  - P'-i muutujate hulk on $\mathbf{Var}'$; $\mathbf{Var}_{\mathrm{S}} \cup \mathbf{Var}_{\mathrm{P}} \subseteq \mathbf{Var}'$.
  - P'-i sisendmuutujate hulk on $\mathbf{Var}_{\mathrm{I}}{}' \subseteq \mathbf{Var}_{\mathrm{I}}$.
  - P' ei kasuta $\mathbf{Var}_{\mathrm{S}}$-i kuuluvaid muutujaid.
  - P' töötab oodatult pol. ajas.
  - Iga pol. ajas konstrueeritava $D_\eta \in \mathcal{D}(\mathbf{State})$ jaoks

$$\{\!|(S_\eta|_{\mathbf{Var}_{\mathrm{S}}}, S'_\eta|_{\mathbf{Var}_{\mathrm{P}}}) \;:\; S_\eta \leftarrow D_\eta, S'_\eta \leftarrow [\![P]\!]_\eta(S_\eta)|\!\} \approx$$
$$\{\!|(S_\eta|_{\mathbf{Var}_{\mathrm{S}}}, S'_\eta|_{\mathbf{Var}_{\mathrm{P}}}) \;:\; S_\eta \leftarrow D_\eta, S'_\eta \leftarrow [\![P']\!]_\eta(S_\eta)|\!\} \quad .$$

  S.t. $\mathbf{Var}_{\mathrm{P}}$-s olevate muutujate lõppväärtused on võimalik sama hästi kui välja arvutada ilma $\mathbf{Var}_{\mathrm{S}}$-s olevate muutujate väärtusi lugemata.
- P' leitakse P-d teisendades.

Teisendused

- Kahte sorti teisendusi:
  - Need, mis vastavad ühe oraakli asendamisele teisega, kus oraaklid on tüüp-0 turvalisuse tõestusest.
    - Muudab $[\![P]\!]$-d, aga ainult eristamatult.
    - Vaja, et P oleks kujul, kus oraakli kasutamise piisavus ilmne oleks.
    - Toome sisse uue operatsiooni, mille semantikaks on keskkonna pakutava oraakli kasutamine.
  - Need, mis $[\![P]\!]$-d üldse ei muuda.
    - Vajalikud programmi sellisele kujule viimiseks, kus esimest sorti teisendusi kasutada saab.

Teisendamise näide

$k := \mathcal{G}en^1$

if b *then*

$\quad l := k$

$\quad y := \mathcal{G}en^2$

else

$\quad l := \mathcal{G}en^3$

$\quad y := \mathcal{G}en^4$

$x := \mathcal{E}nc(l, y)$

$z := \mathcal{E}nc(y, s)$

$b : \langle \{h\}, \mathsf{Data} \rangle \quad s : \langle \{h\}, \mathsf{Data} \rangle$

$k : \langle \emptyset, \mathsf{Key}_1 \rangle$

$l : \langle \{h\}, \mathsf{Key}_{1,3} \rangle \quad y : \langle \{h\}, \mathsf{Key}_{2,4} \rangle$

$x : \langle \{h_1, h_3, 2_1, 2_3, 4_1, 4_3\}, \mathsf{Data} \rangle$

$z : \langle \{h_2, h_4\}, \mathsf{Data} \rangle$

$\mathrm{P} : \{h_1, h_2, h_3, h_4, 2_1, 2_3, 4_1, 4_3\}$

Eraldame võtmegenereerimised

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$\quad l^{(t)} := k^{(t)}; l_1 := k_1$

$\quad y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$\quad l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$\quad y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$\quad v := y_2$

else

$\quad v := y_4$

$x := \mathcal{CE}nc(l^{(t)} \| 1, l_1, v | 3, l_3, v)$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

$b : \langle \{h\}, \mathsf{Data} \rangle$ $\quad s : \langle \{h\}, \mathsf{Data} \rangle$

$k^{(t)} : \langle \emptyset, \mathsf{Data} \rangle$ $\quad k_1 : \langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)} : \langle \{h\}, \mathsf{Data} \rangle$

$l_1 : \langle \{h\}, \mathsf{Key}_1 \rangle$ $\quad l_3 : \langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)} : \langle \{h\}, \mathsf{Data} \rangle$

$y_2 : \langle \{h\}, \mathsf{Key}_2 \rangle$ $\quad y_4 : \langle \{h\}, \mathsf{Key}_4 \rangle$

$v : \langle \{h, 2, 4\}, \mathsf{Data} \rangle$

$x : \langle \{h_1, h_3, 2_1, 2_3, 4_1, 4_3\}, \mathsf{Data} \rangle$

$z : \langle \{h_2, h_4\}, \mathsf{Data} \rangle$

$\mathrm{P} : \{h_1, h_2, h_3, h_4, 2_1, 2_3, 4_1, 4_3\}$

Mida tähendab $[\![P]\!]$ mittemuutmine?

- Olgu $(S, \to)$ mingi tõenäosuslik olekuautomaat. S.t.
  - S on mingi hulk.
    - Näiteks programmikonfiguratsioonid.
  - $\to$ on funktsioon S-st $\mathcal{D}(S)$-i.
    - $\Pr[s \to s']$ tähistagu suurust $\to (s)(s')$.
    - $\Pr[s \to S']$ tähistagu suurust $\sum_{s' \in S'} \Pr[s \to s']$.
- $\sim \in \mathrm{Eqv}\ S$ on tõenäosuslik bisimulatsioon, kui $s \sim s'$-st järeldub iga $t \in S$ jaoks $\sum_{t' \sim t} \Pr[s \to t'] = \sum_{t' \sim t} \Pr[s' \to t']$ ehk $\Pr[s \to [t]_\sim] = \Pr[s' \to [t]_\sim]$.
- S.t. kui süsteem alustab üks kord tööd s-st ja teine kord s'-st, siis nad läbivad sünkroonis $\sim$-i ekvivalentsiklasse.

Mittesünkroonne läbimine

- Olgu $\sim \in \mathrm{Eqv}\ S$. Olgu $A, B \in S/\sim$ ja $s \in A$. Olgu $\mathbf{P}(s, A, B)$ tõenäosus, et süsteem, alustades tööd s-st teeb null või rohkem sammu hulgas A ja seejärel läheb hulka B.
- $\sim$ on nõrk tõenäosuslik bisimulatsioon kui $\mathbf{P}(s, A, B) = \mathbf{P}(s', A, B)$ kõigi $A, B \in S/\sim$ ja $s, s' \in A$ jaoks.
- Kui me võrdleme kahte süsteemi, $(S, \rightarrow)$ ja $(T, \Rightarrow)$ algolekutega s_0 ja t_0, siis moodustame nende ühendi $(S \dot\cup T, \rightarrow \dot\cup \Rightarrow)$ ja otsime sobivat (nõrka) bisimulatsiooni, mis seob s_0-i ja t_0-i.
- Bisimulatsioon on sobiv, kui ta eraldab konfiguratsioonid, kus avalikel muutujatel on erinevad väärtused.

Lisame võtme $0^{\ell(\eta)}$ šifreerimiseks

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$l^{(t)} := k^{(t)}; l_1 := k_1$

$y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$v := y_2$

else

$v := y_4$

$x := \mathcal{CE}nc(l^{(t)} \| 1, l_1, v | 3, l_3, v)$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \{h, 2, 4\}, \mathsf{Data} \rangle$

x : $\langle \{h_1, h_3, 2_1, 2_3, 4_1, 4_3\}, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_1, h_2, h_3, h_4, 2_1, 2_3, 4_1, 4_3\}$

Leiame töödeldava võtmegenereerimise

- Meil oli $\gamma_I(\mathbf{Var}_\mathrm{P}) = \{h_1, h_2, h_3, h_4, 2_1, 2_3, 4_1, 4_3\}$.
- See sisaldab veel h-d.
- Leiame mingi $g \in \mathcal{G}$, mis esineb seal ainult võtme kohal.
  - Need on 1 ja 3, olgu valitud 1.
- Kustutame programmist kõik muutujad, mille tüübis 1 esineb andmete kohal.
  - Kustutame kõik laused, kus neid loetakse või kirjutatakse.
- Antud juhul ei tee see kustutamine midagi.

Tüüp-0 turvalisus paljude võtmetega

- Olgu $\mathcal{O}$ oraakel, mis võtab kaks argumenti.
  - Päringu (l, x) peale kontrollib $\mathcal{O}$, kas tal on salvestatud paar (l, k_l).
    - Kui ei, siis genereerib uue võtme k_l ja salvestab (l, k_l).
  - $\mathcal{O}$ leiab $y \leftarrow \mathcal{E}(k_l, y)$ ja tagastab y.
- Olgu $\mathcal{O}'$ oraakel, mis võtab kaks argumenti.
  - Töö alguses genereerib $\mathcal{O}'$ võtme k.
  - Päringu peale leiab ta $y \leftarrow \mathcal{E}(k, \mathbf{0}^{\ell(n)})$ ja tagastab y.
- $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ on tüüp-0 turvaline $\Leftrightarrow \mathcal{O} \approx \mathcal{O}'$.

Võtmed 1 & 0 $\Rightarrow$ oraaklikutsed

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$\quad l^{(t)} := k^{(t)}; l_1 := k_1$

$\quad y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$\quad l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$\quad y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$\quad v := y_2$

else

$\quad v := y_4$

$x := \mathcal{CE}nc(l^{(t)} \| 1, l_1, v \,|3, l_3, v)$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s|4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \{h, 2, 4\}, \mathsf{Data} \rangle$

x : $\langle \{h_1, h_3, 2_1, 2_3, 4_1, 4_3\}, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_1, h_2, h_3, h_4, 2_1, 2_3, 4_1, 4_3\}$

Oraaklikutsed $\Rightarrow \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$\quad l^{(t)} := k^{(t)}; l_1 := k_1$

$\quad y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$\quad l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$\quad y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$\quad v := y_2$

else

$\quad v := y_4$

$x := \mathcal{CE}nc(l^{(t)} \| 1, \mathfrak{k}, \mathbf{0}^{\ell(\eta)} | 3, l_3, v)$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \{h, 2, 4\}, \mathsf{Data} \rangle$

x : $\langle \{h_0, h_3, 2_3, 4_3\}, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_0, h_2, h_3, h_4, 2_3, 4_3\}$

Töödeldav võtmegenereerimine

- $\gamma_I(\mathbf{Var}_{\mathrm{P}})$-s esinevad ainult võtmetena 0 ja 3.
- 0-i ei vali, seega võtame 3-e.
  - Teisenduste jooksul rahuldab $T = \gamma_I(\mathbf{Var}_{\mathrm{P}})$ invarianti, et kui $t_{N \dot{\cup} \{0\}} \in T$, siis leidub $g \notin N$ nii, et ka $t_{N \cup \{g\}} \in T$.
  - Seega on alati võimalik valida 0-st erinev võtmegenereerimise koht.
- 3 ei esine ühegi muutuja tüübis andmete kohal. Seega ei pea midagi kustutama.

Võtmed 3 & 0 $\Rightarrow$ oraaklikutsed

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$l^{(t)} := k^{(t)}; l_1 := k_1$

$y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$v := y_2$

else

$v := y_4$

$x := \mathcal{CE}nc(l^{(t)} \| 1, \mathfrak{k}, \mathbf{0}^{\ell(\eta)} | 3, l_3, v)$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \{h, 2, 4\}, \mathsf{Data} \rangle$

x : $\langle \{h_0, h_3, 2_3, 4_3\}, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_0, h_2, h_3, h_4, 2_3, 4_3\}$

Oraaklikutsed $\Rightarrow \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$\quad l^{(t)} := k^{(t)}; l_1 := k_1$

$\quad y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$\quad l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$\quad y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$\quad v := y_2$

else

$\quad v := y_4$

$x := \mathcal{CE}nc(l^{(t)} \| 1, \mathfrak{k}, \mathbf{0}^{\ell(\eta)} | 3, \mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \{h, 2, 4\}, \mathsf{Data} \rangle$

x : $\langle \{h_0\}, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_0, h_2, h_4\}$

Võrdsete harudega $\mathcal{CE}nc \Rightarrow \mathcal{E}nc$

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$\quad l^{(t)} := k^{(t)}; l_1 := k_1$

$\quad y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$\quad l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$\quad y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$\quad v := y_2$

else

$\quad v := y_4$

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \{h, 2, 4\}, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_2, h_4\}$

Töödeldav võtmegenereerimine

- $\gamma_I(\mathbf{Var}_{\mathrm{P}})$-s esinevad ainult võtmetena 2 ja 4. Valime 2-e.
- 2 esineb andmete koha peal $\gamma(v)$-s.
- Kustutame kõik käsud, kus esineb v.

Andmetes oleva 2-e kustutamine

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

  $l^{(t)} := k^{(t)}; l_1 := k_1$

  $y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

  $l^{(t)} := 3; l_3 := \mathcal{G}en^3$

  $y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

  skip

else

  skip

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \emptyset, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_2, h_4\}$

Võtmed 2 & 0 $\Rightarrow$ oraaklikutsed

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

  $l^{(t)} := k^{(t)}; l_1 := k_1$

  $y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

  $l^{(t)} := 3; l_3 := \mathcal{G}en^3$

  $y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

  skip

else

  skip

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, y_2, s \,|\, 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1 : $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4 : $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \emptyset, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \{h_2, h_4\}, \mathsf{Data} \rangle$

P : $\{h_2, h_4\}$

Oraaklikutsed $\Rightarrow \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

  $l^{(t)} := k^{(t)}; l_1 := k_1$

  $y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

  $l^{(t)} := 3; l_3 := \mathcal{G}en^3$

  $y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

  skip

else

  skip

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, \mathfrak{k}, \mathbf{0}^{\ell(\eta)} | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \emptyset, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \{h_0, h_4\}, \mathsf{Data} \rangle$

P : $\{h_0, h_4\}$

Võtmed 4 & 0 $\Rightarrow$ oraaklikutsed

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

  $l^{(t)} := k^{(t)}; l_1 := k_1$

  $y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

  $l^{(t)} := 3; l_3 := \mathcal{G}en^3$

  $y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

  skip

else

  skip

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, \mathfrak{k}, \mathbf{0}^{\ell(\eta)} | 4, y_4, s)$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1 : $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4 : $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \emptyset, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \{h_0, h_4\}, \mathsf{Data} \rangle$

P : $\{h_0, h_4\}$

Oraaklikutsed $\Rightarrow \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

  $l^{(t)} := k^{(t)}; l_1 := k_1$

  $y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

  $l^{(t)} := 3; l_3 := \mathcal{G}en^3$

  $y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

  skip

else

  skip

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{CE}nc(y^{(t)} \| 2, \mathfrak{k}, \mathbf{0}^{\ell(\eta)} | 4, \mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1: $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

l_1 : $\langle \{h\}, \mathsf{Key}_1 \rangle$ l_3 : $\langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)}$: $\langle \{h\}, \mathsf{Data} \rangle$

y_2 : $\langle \{h\}, \mathsf{Key}_2 \rangle$ y_4: $\langle \{h\}, \mathsf{Key}_4 \rangle$

v : $\langle \emptyset, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \{h_0\}, \mathsf{Data} \rangle$

P : $\{h_0\}$

Võrdsete harudega $\mathcal{CE}nc \Rightarrow \mathcal{E}nc$

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

if b *then*

$\quad l^{(t)} := k^{(t)}; l_1 := k_1$

$\quad y^{(t)} := 2; y_2 := \mathcal{G}en^2$

else

$\quad l^{(t)} := 3; l_3 := \mathcal{G}en^3$

$\quad y^{(t)} := 4; y_4 := \mathcal{G}en^4$

if $y^{(t)} = 2$ *then*

$\quad$ *skip*

else

$\quad$ *skip*

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$b : \langle \{h\}, \mathsf{Data} \rangle$ $\quad s : \langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k} : \langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)} : \langle \emptyset, \mathsf{Data} \rangle$ $\quad k_1 : \langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)} : \langle \{h\}, \mathsf{Data} \rangle$

$l_1 : \langle \{h\}, \mathsf{Key}_1 \rangle$ $\quad l_3 : \langle \{h\}, \mathsf{Key}_3 \rangle$

$y^{(t)} : \langle \{h\}, \mathsf{Data} \rangle$

$y_2 : \langle \{h\}, \mathsf{Key}_2 \rangle$ $\quad y_4 : \langle \{h\}, \mathsf{Key}_4 \rangle$

$v : \langle \emptyset, \mathsf{Data} \rangle$

$x : \langle \emptyset, \mathsf{Data} \rangle$

$z : \langle \emptyset, \mathsf{Data} \rangle$

$\mathrm{P} : \emptyset$

Andmetes oleva h-i kustutamine

$\mathfrak{k} := \mathcal{G}en^0$

$k^{(t)} := 1; k_1 := \mathcal{G}en^1$

$skip$

$skip$

$x := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

$z := \mathcal{E}nc(\mathfrak{k}, \mathbf{0}^{\ell(\eta)})$

b : $\langle \{h\}, \mathsf{Data} \rangle$ s : $\langle \{h\}, \mathsf{Data} \rangle$

$\mathfrak{k}$: $\langle \emptyset, \mathsf{Key}_0 \rangle$

$k^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$ k_1 : $\langle \emptyset, \mathsf{Key}_1 \rangle$

$l^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$

l_1 : $\langle \emptyset, \mathsf{Data} \rangle$ l_3 : $\langle \emptyset, \mathsf{Data} \rangle$

$y^{(t)}$: $\langle \emptyset, \mathsf{Data} \rangle$

y_2 : $\langle \emptyset, \mathsf{Data} \rangle$ y_4 : $\langle \emptyset, \mathsf{Data} \rangle$

v : $\langle \emptyset, \mathsf{Data} \rangle$

x : $\langle \emptyset, \mathsf{Data} \rangle$

z : $\langle \emptyset, \mathsf{Data} \rangle$

P : $\emptyset$