Arvutuslikult turvaline infovoog

Teooriapäev Roostal, 16.–17. oktoober 2002

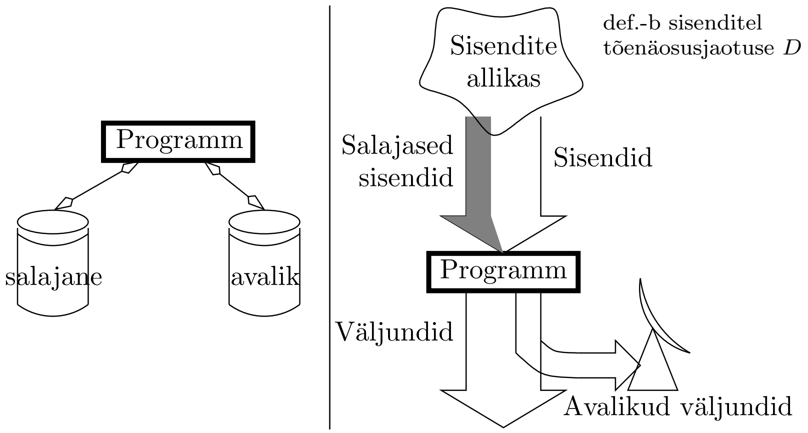
Peeter Laud

Tartu Ülikool
Cybernetica AS

Ettekande ülesehitus

- Probleemi püstitus ja turvalise infovoo definitsioon.
- Vaadeldav programmeerimiskeel.
  - Süntaks. (lihtne imperatiivne keel primitiivse operatsiooniga „krüptimine“)
  - Krüptograafiliste definitsioonide objektid.
  - Semantika.
- Arvutuslikult turvalise infovoo definitsioon.
- Analüüs.
  - Abstraktsiooni olemus.
  - Abstraktne semantika.
  - Vahepeal — turvanõuded krüptimisoperatsiooni semantikale.

Ülesande püstitus



Programmide semantikast

- Vaatame mingis imperatiivses keeles kirjutatud programme.
  - Programmi P *olek* on kujutus tema muutujate hulgast mingisse väärtuste hulka. $\boxed{\mathbf{State} = \mathbf{Var} \to \mathbf{Val}}$
  - Programmi P *semantika* on kujutus, mis teisendab algoleku lõppolekuks. $\boxed{[\![P]\!] = \mathbf{State} \to \mathbf{State}_\perp}$
  - Stohhastilise programmi semantika teisendab algoleku tõenäosusjaotuseks üle lõppolekute. $\boxed{[\![P]\!] = \mathbf{State} \to \mathcal{D}(\mathbf{State}_\perp)}$

Üldine definitsioon

- Olgu antud *salajaste muutujate* hulk $\mathbf{Var}_{\mathrm{S}} \subseteq \mathbf{Var}$ ja *avalike muutujate* hulk $\mathbf{Var}_{\mathrm{P}} \subseteq \mathbf{Var}$. Need defineerivad salajased sisendid ja avalikud väljundid.
- Programmil P on *turvaline infovoog*, kui jaotused
$$\{\!|(S|_{\mathbf{Var}_{\mathrm{S}}}, T|_{\mathbf{Var}_{\mathrm{P}}}) \,:\, S \leftarrow D, T \leftarrow [\![\mathsf{P}]\!](S)|\!\}$$
ja
$$\{\!|(S|_{\mathbf{Var}_{\mathrm{S}}}, T'|_{\mathbf{Var}_{\mathrm{P}}}) \,:\, S, S' \leftarrow D, T' \leftarrow [\![\mathsf{P}]\!](S')|\!\}$$
on mingis mõttes ekvivalentsed.
- Traditsiooniline definitsioon — need kaks jaotust on võrdsed.

Programmeerimiskeele süntaks

$$\begin{array}{lcl} \mathsf{P} & ::= & x := o(x_1, \ldots, x_k) \\ & & x := \mathcal{E}nc(k, y) \\ & & x := \mathcal{G}en() \\ & | & \textit{skip} \\ & | & \mathsf{P}_1; \mathsf{P}_2 \\ & | & \textit{if } b \textit{ then } \mathsf{P}_1 \textit{ else } \mathsf{P}_2 \\ & | & \textit{while } b \textit{ do } \mathsf{P}', \end{array}$$

Siin $x, x_1, \ldots, x_k, k, y, b$ on muutujad, o on mingi aritmeetiline operatsioon (võimalik, et stohhastilise semantikaga).

„Sama olemine“ krüptograafias (1/2)

- Kaks tõenäosusjaotust $D^{(0)}, D^{(1)}$ on „samad“, kui suvalise polünomiaalses ajas töötava algoritmi $\mathcal{A}$ jaoks
$$\Pr[b^* = b \,:\, b \in_{\mathrm{R}} \{0,1\}, x \leftarrow D^{(b)}, b^* \leftarrow \mathcal{A}(x)] = \frac{1}{2} + \alpha,$$
kus α on „kaduvväike“.
- Polünomiaalne mille suhtes? Mida tähendab kaduvväike?
- Keerukusteoreetilised omaduste definitsioonid on tavaliselt mitte objektide, vaid objektide *perede* (indekseeritud *turvalisusparameetriga* $n \in \mathbb{N}$) jaoks.

„Sama olemine“ krüptograafias (2/2)

- Jaotuste pered $D^{(0)}$ ja $D^{(1)}$ on *arvutuslikult eristamatud*, kui iga n-i suhtes polünomiaalses ajas töötava algoritmi $\mathcal{A}$ jaoks
$$\Pr[b^* = b \,:\, b \in_{\mathrm{R}} \{0,1\}, x \leftarrow D_n^{(b)}, b^* \leftarrow \mathcal{A}(n, x)] = \frac{1}{2} + \alpha(n),$$
kus α on kaduvväike. Tähistame $D^{(0)} \approx D^{(1)}$.
- α on *kaduvväike*, kui iga polünoomi q jaoks on $\alpha(n)$ asümptootiliselt väiksem kui $1/|q(n)|$.

Näide: Funktsioonide pere H, kus $H_n : \{0,1\}^* \to \{0,1\}^{\ell(n)}$, on (tugevalt) kollisioonivaba, kui iga pol. ajas töötava algoritmi $\mathcal{A}$ jaoks
$$\Pr[x \neq y \wedge H_n(x) = H_n(y) \,:\, (x, y) \leftarrow \mathcal{A}(n)]$$
on kaduvväike (kui funktsioon n-st).

Semantika

Lisame turvalisusparameetri:

- $\mathbf{State}_n = \mathbf{Var} \to \mathbf{Val}_n$, $\mathbf{Val}_n$ on mingi bitijadade hulk;
- $[\![\mathsf{P}]\!] : \prod_{n \in \mathbb{N}} \mathbf{State}_n \to \mathcal{D}(\mathbf{State}_{n\perp})$.

Semantika defineeritud induktiivselt üle programmi süntaksi.

$$[\![x := o(x_1, \ldots, x_k)]\!]_n(S_n) := \{\!|S_n[x \mapsto v] \,:\, v \leftarrow [\![o]\!]_n(S_n(x_1), \ldots, S_n(x_k))|\!\}$$

$$[\![\mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2]\!]_n(S_n) := \begin{cases} [\![\mathsf{P}_1]\!]_n(S_n), & \text{kui } S_n(b) = \mathsf{true} \\ [\![\mathsf{P}_2]\!]_n(S_n), & \text{kui } S_n(b) = \mathsf{false} \end{cases}$$

$$[\![\mathit{while}\ b\ \mathit{do}\ \mathsf{P}']\!] = [\![\mathit{if}\ b\ \mathit{then}\ \big(\mathsf{P}'; \mathit{while}\ b\ \mathit{do}\ \mathsf{P}'\big)\ \mathit{else}\ \mathit{skip}]\!]$$

$[\![\mathit{skip}]\!]$ on „samasusteisendus“. $[\![\mathsf{P}_1; \mathsf{P}_2]\!]$ on $[\![\mathsf{P}_2]\!]$ ja $[\![\mathsf{P}_1]\!]$ „kompositsioon“.

Arvutuslikult turvaline infovoog

- Vaatame ainult programme, mis töötavad polünomiaalses ajas.
- Programmil P on *(arvutuslikult) turvaline infovoog*, kui jaotuste pered

$$\{\!|(S_n|_{\mathbf{Var}_\mathrm{S}}, T_n|_{\mathbf{Var}_\mathrm{P}}) \,:\, S_n \leftarrow D_n, T_n \leftarrow [\![\mathsf{P}]\!]_n(S_n)|\!\}_{n \in \mathbb{N}}$$

ja

$$\{\!|(S_n|_{\mathbf{Var}_\mathrm{S}}, T'_n|_{\mathbf{Var}_\mathrm{P}}) \,:\, S_n, S'_n \leftarrow D_n, T'_n \leftarrow [\![\mathsf{P}]\!]_n(S'_n)|\!\}_{n \in \mathbb{N}}$$

on *arvutuslikult eristamatud.*

Analüüsi eesmärk

- Antud
  - programmi P tekst,
  - muutujate hulgad $\mathbf{Var}_\mathrm{S}$ ja $\mathbf{Var}_\mathrm{P}$,
  - sisendite jaotuse D kirjeldus,

  leida, kas P-l on arvutuslikult turvaline infovoog.
- See on ilmselt mittearvutatav.
- Lubame programmianalüüsil eksida, aga ainult ühele, „ohutule“ poole:
  - Kui analüüs ütleb: „infovoog on turvaline“, siis on P-l turvaline infovoog.
  - Kui P-l ei ole turvaline infovoog, siis analüüs ütleb :„infovoog ei ole turvaline“.
  - Lubatud on juht, kus P-l on turvaline infovoog ja analüüs ütleb: „infovoog ei ole turvaline“.

Abstraktsioon

- $[\![\mathsf{P}]\!]$ on vaadeldav kui hulga $\prod_{n \in \mathbb{N}} \mathcal{D}(\mathbf{State}_n)$ teisendus. Me tahame abstraheerida selle hulga elemente.
- Olgu $X, Y \subseteq \mathbf{Var}$. X on *sõltumatu* Y-st jaotuses D, kui

$$\{\!|(S_n|_X, S_n|_Y) \,:\, S_n \leftarrow D_n|\!\}_{n \in \mathbb{N}} \approx \{\!|(S_n|_X, S'_n|_Y) \,:\, S_n, S'_n \leftarrow D_n|\!\}_{n \in \mathbb{N}}.$$

- D-d abstraheerib hulga $\mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$ selline alamhulk, mis sisaldab (ülimalt) kõik sellised paarid (X, Y), et X on jaotuses D Y-st sõltumatu.
- Kui P ei muuda hulga $\mathbf{Var}_\mathrm{S}$ elementide väärtusi, siis P-l on turvaline infovoog $\Leftrightarrow$ $\mathbf{Var}_\mathrm{S}$ on sõltumatu $\mathbf{Var}_\mathrm{P}$-st jaotuses $[\![\mathsf{P}]\!](D)$.
- Programmi P analüüs (tähist. $\langle\!\langle \mathsf{P} \rangle\!\rangle$) on hulga $\mathcal{P}(\mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var}))$ teisendus. Ta kujutab D abstraktsiooni (mingiks) $[\![\mathsf{P}]\!](D)$ abstraktsiooniks.

Abstraktne semantika — omistamine

Olgu $\mathsf{P} \equiv x := o(x_1, \ldots, x_k)$.

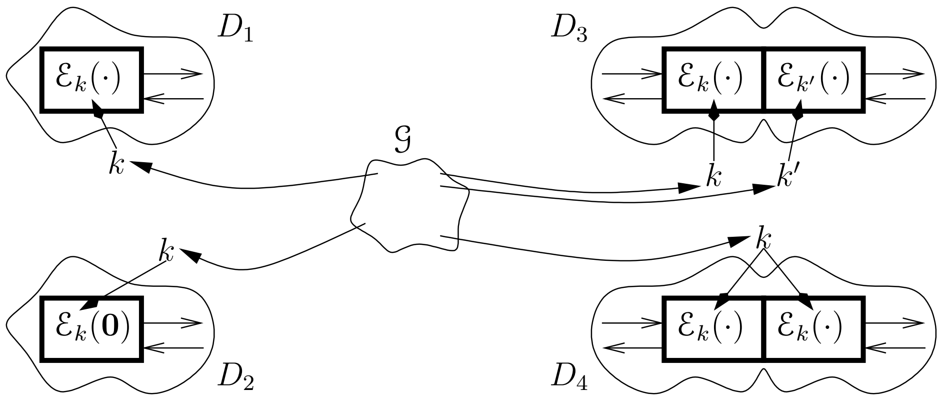
- Olgu $\mathcal{X} \subseteq \mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$. Me võime eeldada, et $\mathcal{X}$ on sümmeetriline ja *monotoonne*:
  - kui $(X, Y) \in \mathcal{X}$, $X' \subseteq X$ ja $Y' \subseteq Y$, siis $(X', Y') \in \mathcal{X}$

  kuna sõltumatus on sümmeetriline ja monotoonne.
- Olgu $(X, Y) \in \mathcal{X}$.
  - Kui $x \notin X \cup Y$, siis $(X, Y) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.
  - Kui $x \notin X$ ja $x_1, \ldots, x_k \in Y$, siis $(X, Y \cup \{x\}) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.
- $\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$ on sümmeetriline ja monotoonne.

Turvanõuded krüptimisprimitiivile

Krüptimisprimitiiv $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ on

- *kordust varjav*, kui D_1 ja D_2 on eristamatud;
- *võtmete samasust varjav*, kui D_3 ja D_4 on eristamatud.



Virtuaalsed elemendid hulgas Var

- Peale operatsiooni $x := \mathcal{E}nc(k, y)$ on hulgad $\{x\}$ ja $\{k\}$ sõltuvad.
- Peale operatsiooni $l := k + 1$ on hulgad $\{l\}$ ja $\{k\}$ sõltuvad.
- Need sõltuvused on „erinevat laadi“.
- Kui $k \in \mathbf{Var}$, siis olgu $[k]_\mathcal{E}$ selline objekt, et kui $S_n \in \mathbf{State}_n$, siis $S_n([k]_\mathcal{E})$ tähistab musta kasti, mis krüptib võtmega $S_n(k)$.
- Ka objektide $[k]_\mathcal{E}$ jaoks on defineeritud sõltumatus.
- $\{x\}$ ja $\{[k]_\mathcal{E}\}$ on sõltumatud. $\{l\}$ ja $\{[k]_\mathcal{E}\}$ on sõltuvad.
- Me „lisame“ objektid $[k]_\mathcal{E}$ hulka $\mathbf{Var}$.

Abstraktsioon — võtmed

- Meil on vaja teada, millised muutujad on võtmetena kasutatavad.
- Täiendame jaotuste pere D abstraktsiooni: lisame selliste muutujate $x \in \mathbf{Var}$ hulga, kus

$$\{\!| S_n([x]_\mathcal{E}) : S_n \leftarrow D_n |\!\}_{n \in \mathbb{N}} \approx \{\!| \mathcal{E}(n, k, \cdot) : k \leftarrow \mathcal{G}(n) |\!\}_{n \in \mathbb{N}} .$$

- Abstraktne väärtus $\mathcal{X}$ on paar $(\mathcal{X}_\mathrm{s}, \mathcal{X}_\mathrm{v})$, kus
  - $\mathcal{X}_\mathrm{s} \subseteq \mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$.
  - $\mathcal{X}_\mathrm{v} \subseteq \mathbf{Var}$.
- Olgu $\mathcal{F}(\mathbf{Var}) = \mathcal{P}(\mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})) \times \mathcal{P}(\mathbf{Var})$.

Olgu $P \equiv x := o(x_1, \ldots, x_k)$. Olgu $\mathcal{X} \in \mathcal{F}(\mathbf{Var})$.

- $x \in [\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})]_\mathrm{v}$ parajasti siis, kui
  - o on $\mathcal{G}en$ või
  - $P \equiv x := y$ ja $y \in \mathcal{X}_\mathrm{v}$.
- $y \in [\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})]_\mathrm{v}$ parajasti siis, kui $y \in \mathcal{X}_\mathrm{v}$.

Abstraktne semantika — krüptimine

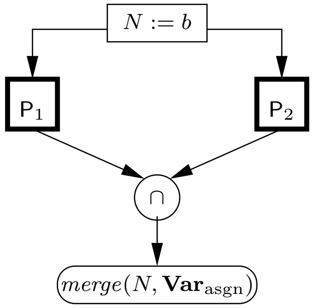
Olgu $\mathcal{X} \in \mathcal{F}(\mathbf{Var})$ ja $(X, Y) \in \mathcal{X}_\mathrm{s}$.

- Kui $\mathsf{P} \equiv x := \mathcal{G}en()$, siis $(X \cup \{[x]_\mathcal{E}\}, Y \cup \{[x]_\mathcal{E}\}) \in [\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})]_\mathrm{s}$.
- Kui $\mathsf{P} \equiv x := \mathcal{E}nc(k, y)$, siis kehtivad:
  - Kui
    - $k \in \mathcal{X}_\mathrm{v}$,
    - $(\{[k]_\mathcal{E}\}, X \cup Y \cup \{y\}) \in \mathcal{X}_\mathrm{s}$,

    siis $(X, Y \cup \{x\}) \in [\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})]_\mathrm{s}$.
  - Kui $(X, Y \cup \{[k]_\mathcal{E}, y\}) \in \mathcal{X}_\mathrm{s}$, siis $(X, Y \cup \{x\}) \in [\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})]_\mathrm{s}$.

Abstraktne semantika — hargnemised (1/2)

Olgu $\mathsf{P} \equiv$ *if* b *then* P_1 *else* P_2



- N — uus muutuja
- $\mathbf{Var}_\mathrm{asgn} \subseteq \mathbf{Var}$ — muutujad, millele omistatakse P_1-s või P_2-s.

Abstraktne semantika — hargnemised (2/2)

Olgu $\mathcal{X} \in \mathcal{F}(\mathbf{Var})$. Tähistame $\mathcal{Y} = \langle\!\langle merge(N, \mathbf{Var}_\mathrm{asgn}) \rangle\!\rangle(\mathcal{X})$.

- Kui $(X, Y \cup \{N\}) \in \mathcal{X}_\mathrm{s}$ ja $X \perp \mathbf{Var}_\mathrm{asgn}$, siis $(X, Y) \in \mathcal{Y}_\mathrm{s}$.
- Olgu $X \perp \mathbf{Var}_\mathrm{asgn}$, $Y \perp \mathbf{Var}_\mathrm{asgn}$. Olgu $K_X, K_Y, K_{XY} \subseteq \mathcal{X}_\mathrm{v}$, nii et $K_X \perp K_Y \perp K_{XY} \perp K_X$. Kui
  - $(X, Y) \in \mathcal{X}_\mathrm{s}$,
  - $([K_X]_\mathcal{E} \cup [K_Y]_\mathcal{E} \cup [K_{XY}]_\mathcal{E}, X \cup Y \cup \{N\}) \in \mathcal{X}_\mathrm{s}$,
  - $[K_X]_\mathcal{E} \cup [K_Y]_\mathcal{E} \cup [K_{XY}]_\mathcal{E}$ elemendid on kõik üksteisest sõltumatud,
  - iga $[K_{XY}]_\mathcal{E}$ element on iseendast sõltumatu,

  siis $(X \cup [K_X]_\mathcal{E} \cup [K_{XY}]_\mathcal{E}, Y \cup [K_Y]_\mathcal{E} \cup [K_{XY}]_\mathcal{E}) \in \mathcal{Y}_\mathrm{s}$.
- Olgu $k \in \mathcal{X}_\mathrm{v}$. Siis $k \in \mathcal{Y}_\mathrm{v}$, kui $k \notin \mathbf{Var}_\mathrm{asgn}$ või $(\{[k]_\mathcal{E}\}, \{N\}) \in \mathcal{X}_\mathrm{s}$.

Abstraktne semantika — muud

- $\langle\!\langle skip \rangle\!\rangle$ on samasusteisendus.
- $\langle\!\langle \mathsf{P}_1; \mathsf{P}_2 \rangle\!\rangle := \langle\!\langle \mathsf{P}_2 \rangle\!\rangle \circ \langle\!\langle \mathsf{P}_1 \rangle\!\rangle$.
- $\langle\!\langle$ *while* b *do* $\mathsf{P} \rangle\!\rangle = \langle\!\langle$ *if* b *then* P *else* *skip* $\rangle\!\rangle^*$, kus

$$f^* := \bigcap_{n \in \mathbb{N}} \underbrace{f \circ f \circ \cdots \circ f}_{n} \ .$$