

# Reduktsioonid ja turvalisus

Ahto Buldas

## Krüptograafilised primitiivid

Teoreetiline krüptograafia keskendub *mängule*, mis modelleerib mingi süsteemi murdmist. Mängus osalevad:

- *Krüptograafiline primitiiv* – Hulk Turingi masinaid  $B = (B_1, \dots, B_m)$ , mille eesmärk on tagada süsteemile teatud funktsionaalsus (see, mille jaoks süsteem on ehitatud), mis aga ei kuulu otseselt krüptograafia uurimisvaldkonda – krüptograafias on palju olulisemad need omadused, mida süsteemil *ei tohi olla*.
- *Vastane* – Hulk Turingi masinaid  $A = (A_1, \dots, A_\ell)$ , mille eesmärk on primitiiviga fikseeritud viisil (vastavalt *ründestsenaariumile*  $\mathcal{G}$ ) interakteerudes teostada rünne, st saavutada teatud tingimuse  $C$  kehtimine piisavalt suure tõenäosusega  $\Pr[C \mid \mathcal{G}]$  (tingimuse  $C$  kehtimise tõenäosus, arvestades stsenaariumi  $\mathcal{G}$ ), või alternatiivse tähistusviisi korral  $\Pr[\mathcal{G} : C]$ .

## Primitiivi üldine definitsioon

Primitiivi  $B = (B_1, \dots, B_m)$  saab esitada üheainsa arvutatava funktsioonina  $B: \{0, 1\}^* \rightarrow \{0, 1\}^*$ , kui defineerida

$$B(k, x) = B_k(x) .$$

Krüptograafilise primitiivi üldisem definitsioon käsitleb primitiivi kui kõiki-  
de sama tüüpi (ja sama ülesande täitmiseks mõeldud) primitiivide klassi.  
Seega oleks täpsem öelda, et mängus osalevad primitiivi enda asemel  
nende *esindajad*.

Enamasti eeldame, et primitiivid on *efektiivsed*, st nende tööaeg on polü-  
nomiaalne.

## Turvaparameeter

Iga primitiiv kasutab kahte tüüpi mälu:

- *Avalik mälu*, mida ei ole küll võimalik teistel osapooltel (sh vastasel) muuta, kuid mille sisu on loetav kõigile stsenaariumis osalejaile.
- *Privaatmälu*, mille sisu saab lugeda ainult primitiiv (täpsemini, ainult antud primitiivi komponent).

Privaatmälu mahtu (erandjuhtudel ka muid parameetreid) nimetatakse *turvaparameetriks* ja tähistatakse  $s(n)$ . Eeldame, et  $s(n)$  on argumendi  $n$  suhtes monotoonselt kasvav funktsioon, st

$$n_1 \leq n_2 \Rightarrow s(n_1) \leq s(n_2) .$$

Primitiivi turvataset saab alati tõsta, kui võtta kasutusele suurem  $n$ , st kasutada primitiivi kui  $\mathbf{P}$ -pere suurema järjekorranumbriga komponente. Sisuliselt tähendab suurema  $n$  valimine seda, et suurendatakse kasutatava privaadmälu mahtu.

## Aeg-edukus suhe

Intuitiivselt on selge, et mingi primitiiv on seda turvalisem, mida rohkem on vastastel tema murdmiseks vaja arvutusressursse. Võib juhtuda, et ükski vastane, ükskõik kui palju ta selleks aega kulutab, ei suuda murda primitiivi absoluutse kindlusega. Seetõttu tundub loomulik arvestada vajaliku arvutusressursina nn. *aeg-edukus suhet*:

$$\mathbf{R}(s(n)) = \frac{T(n)}{\delta(n)},$$

kus  $\delta(n) = \Pr[\mathcal{G} : C]$  on vastase õnnestumise tõenäosus ja  $T(n)$  on halvima juhu tööaeg.

Aeg-edukus suhte sobilikkuse kasuks räägib ka järgmine tähelepanek. Olgu A vastane tööajaga  $T(n)$ , mis murrab primitiivi B edukusega  $\delta(n)$ . Olgu

$t(n) < T(n)$ . Defineerime vastase  $A'$ , mis käitub järgmiselt:

- Tõenäosusega  $\frac{t(n)}{T(n)}$  käitub vastane  $A'$  samuti nagu vastane  $A$ ;
- Tõenäosusega  $1 - \frac{t(n)}{T(n)}$  ei tee vastane midagi ja väljastab mingi konstandi (näiteks  $0^n$ ).

Eeldades, et suhe  $\frac{t(n)}{T(n)}$  on arvutatav ajaga  $T(n)$ , on vastase  $A'$  keskmine tööaeg on

$$T'(n) = t(n) + \frac{t(n)}{T(n)} \cdot T(n) + \left(1 - \frac{t(n)}{T(n)}\right) \cdot 0 = \mathcal{O}(t(n))$$

ja tema õnnestumise tõenäosus on  $\delta'(n) = \frac{t(n)}{T(n)} \cdot \delta(n)$ , millest tulenevalt

$$\mathbf{R}(s(n)) = \frac{T'(n)}{\delta'(n)} = \frac{\mathcal{O}(t(n))}{\frac{t(n)}{T(n)} \cdot \delta(n)} = \mathcal{O}\left(\frac{T(n)}{\delta(n)}\right) = \mathcal{O}(\mathbf{R}'(s'(n))).$$

See tähendab, et uue vastase aeg-edukus suhe erineb esialgsest ainult konstantse võrdeteguri poolest.

## Turvalisus ja tõestatav turvalisus

*Def:* Ütleme, et primitiiv  $B$  on  *$S(n)$ -turvaline*, kui iga vastase  $A$  aeg-educus suhe  $R(s(n)) \geq S(n)$ .

Teoreetilise krüptograafia üks peamisi ülesandeid on konstrueerida ühest krüptograafilisest primitiivist  $B$  teisi primitiive  $B'$  ja tõestada, et saadav konstruktsioon  $B'$  on piisavalt turvaline, eeldades, et  $B$  on turvaline. Selleks, et anda piisavalt täpne matemaatiline kirjeldus sellistele konstruktsioonidele, on vaja defineerida *oraakliga vastase* mõiste.

## Oraakliga vastased

Oraakliga vastaseks  $S$  nimetatakse polünomiaalses ajas töötavat algoritmi (Turingi masinat), mis ei ole täielikult defineeritud selles mõttes, et tema kood sisaldab oraakli väljakutseid – eraldi käsked, mille täitmiseks kasutatakse funktsioone, mille kirjeldus ei kuulu algoritmi  $S$  kirjelduse juurde.

Eeldame, et välised funktsioonid, mida  $S$  välja kutsub on koodis kuidagi tähistatud (näiteks märgendatud arvudega  $1, 2, \dots$ ), nii et oleks võimalik aru saada, millal kutsutakse välja ühte ja sama funktsiooni.

Tähistus  $S^A$ , kus  $A = (A_1, \dots, A_\ell)$  on mingi vastane, tähendab algoritmi, mis saadakse siis, kui algoritmis  $S$  kasutatud oraakliväljakutseid täidetakse vastase  $A$  komponentide  $A_1, \dots, A_\ell$  abil, kusjuures eeldatakse, et märgendiga  $i$  oraakliväljakutseid täidetakse algoritmi  $A_i$  abil. Vastase  $S^A = S^{A_1, \dots, A_\ell}$  tööaja arvutamisel arvestatakse ka oraakliväljakutsete täitmiseks kulunud aegu, st Turingi masinate  $A_i$  tööaegu.

## Reduktsioonid

**Def.:** Ütleme, et  $S$  on polünomiaalne oraakliga vastane, kui sellest, et  $A_1, \dots, A_\ell$  on polünomiaalses ajas töötavad Turingi masinad, järeldub, et ka  $S^{A_1, \dots, A_\ell}$  tööaeg on polünomiaalne.

Reduktsiooniks primitiivilt  $\mathcal{B}_1$  primitiivile  $\mathcal{B}_2$  nimetetakse oraakliga Turingi masinate paari  $(P, S)$ , nii et kehtivad järgmised kaks eeldust:

- **Konstruktsioon** – kui  $f \in \mathcal{B}_1$ , siis  $P^f \in \mathcal{B}_2$ .
- **Garantii** – Kui  $A$  murrab primitiivi  $P^f$  aeg-edukus suhtega  $\mathbf{R}_2(s_2(n))$ , siis oraakliga vastane  $S^{A, f}$  murrab primitiivi  $f$  aeg-edukus suhtega  $\mathbf{R}_1(s_1(n))$ .

## Reduktsiooni tüübid

Reduktsioon on seda väärtuslikum (st tema poolt antav garantii kindlam), mida väiksem on suhe  $r_1(n) = \mathbf{R}_1(s_1(n))$  suhtega  $r_2(n) = \mathbf{R}_2(s_2(n))$  võrreldes, st mida aeglasemalt kasvab funktsioon

$$r_1(n) = \Phi[r_2(n)] .$$

Garantii lihtsustatult: Kui konstrueeritud primitiiv  $B_2$  oleks murtav ressursiga  $r_2(n)$ , siis oleks lähteprimitiiv murtav ressursiga  $r_1(n)$ .

Võib juhtuda, et me teame lähteprimitiivi kohta, et see on  $S_1(n)$ -turvaline. Kui  $\Phi$  on monotoonselt kasvav funktsioon, siis eelduste tõttu kehtivast võrratusest  $r_1(n) \geq S_1(n)$  järeldeb, et konstrueeritud primitiiv  $B_2$  on vähemalt  $\Phi^{-1}[S_1(n)]$ -turvaline.

## Reduktsiooni efektiivsusklassid

Vastavalt funktsiooni  $\Phi$  iseloomule on mõistlik eristada järgmisi reduktsiooni tüüpe:

- *Lineaarne* reduktsioon –  $r_1(n) = n^{\mathcal{O}(1)} \cdot r_2(n)$ .
- *Polünoomiaalne* reduktsioon –  $r_1(n) = n^{\mathcal{O}(1)} \cdot (r_2(n))^{\mathcal{O}(1)}$ .
- *Nõrk* reduktsioon –  $r_1(n) = n^{\mathcal{O}(1)} \cdot [r_2(n^{\mathcal{O}(1)})]^{\mathcal{O}(1)}$ .

## Efektiivsus: näide

Et paremini aru saada reduktsiooni tüüpide poolt antavatest garantiidest, kujutame ette, et meil on antud reduktsioon primitiivilt  $B_1$  primitiivile  $B_2$ , ja me soovime selle reduktsiooni abil saada primitiivi  $B_2$  esindajat, mis on  $2^{n/2}$ -turvaline. Kui turvaline peab seljuhul olema lähteprimitiiv  $B_1$ ? Kui reduktsioon on:

- *lineaarne*, siis peab lähteprimitiiv olema  $n^{\mathcal{O}(1)} \cdot 2^{n/2} = 2^{\frac{n}{2} + \mathcal{O}(\log n)}$ -turvaline,
- *polünomiaalne*, siis lähteprimitiiv peab olema  $2^{\mathcal{O}(n)}$ -turvaline
- *nõrk*, siis lähteprimitiiv peab olema juba  $2^{n^{\mathcal{O}(1)}}$ -turvaline.

Näiteks kui lähteprimitiiv kujutab endast mingit krüpteerimisalgoritmi, mis kasutab  $n$ -bitist salajast võtit, siis seda algoritmi on alati võimalik murda ajas  $n^{\mathcal{O}(1)} \cdot 2^n$ , mistõttu juba polünomiaalne reduktsioon (rääkimata nõrgast reduktsioonist) võib olla praktika seisukohalt väärtusetu.