Matemaatilisi pildikesi infoturbest

MTMM.00.324 Sissejuhatus matemaatika erialasse

Peeter Laud

peeter.laud@cyber.ee

05.12.2013

Ajaloost

- Kaamasuutra, 1. osa, 3. peatükk
  - 64 vajalikku oskust igaühele
    - 45. Sõrmedekeele abil rääkimine [tõlk. Linnart Mäll, 1989]
    - 45. *The art of understanding writing in cypher, and the writing of words in a peculiar way* [tõlk. Richard F. Burton jt., 1883]
- Caesari šiffer
  - A→D, B→E,...,W→Z,X→A,Y→B,Z→C
  - RQ PHHOGLY WHLG VLLQ NRKDWD

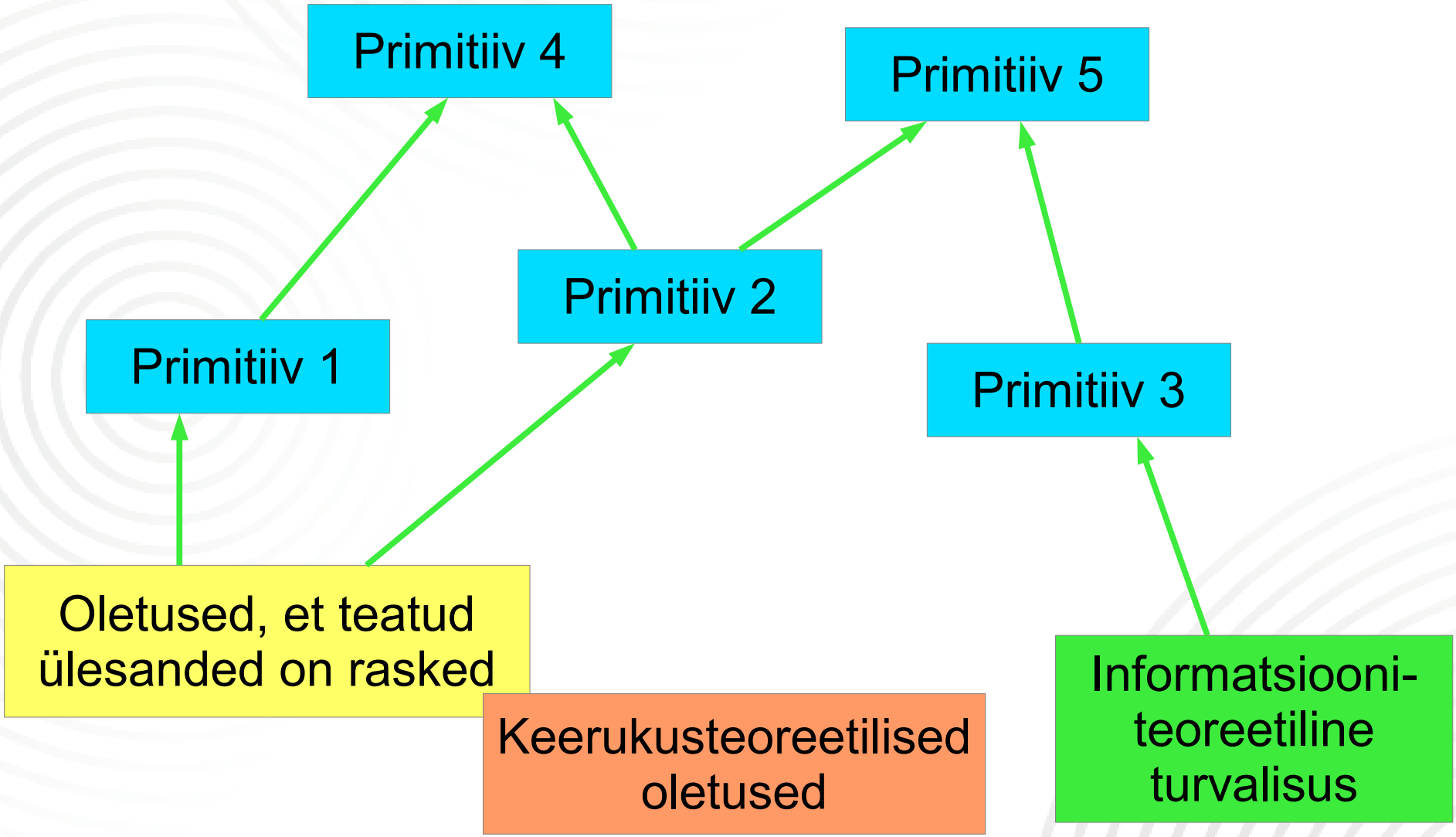
Turvalisus

- Funktsionaalsus – süsteemi omadus teha seda, mida me tahame, et ta teeks
- Turvalisus – süsteemi omadus mitte teha seda, mida me ei taha, et ta teeks
  - Väljalülitatud arvuti on kõige turvalisem
- Krüptograafia – matemaatilised meetodid süsteemide turvalisuse tagamiseks
- Funktsionaalsuse ja turvalisuse samaaegne saavutamine on huvitav ülesanne

Turvaomadusi

- konfidentsiaalsus
  - salajastest andmetest süsteemi käitumine nähtavalt ei sõltu
- terviklus
  - süsteem ei lähe olekusse, kuhu me ei taha, et ta läheks
- käideldavus (funktsionaalsus)
- teenusetõkestusrünnete taluvus
- salgamise vääramine
- jälgitavus / jälitatavus
- tõestamatus
- anonüümsus
- ...

Krüptograafiliste turvagarantiide olemusest

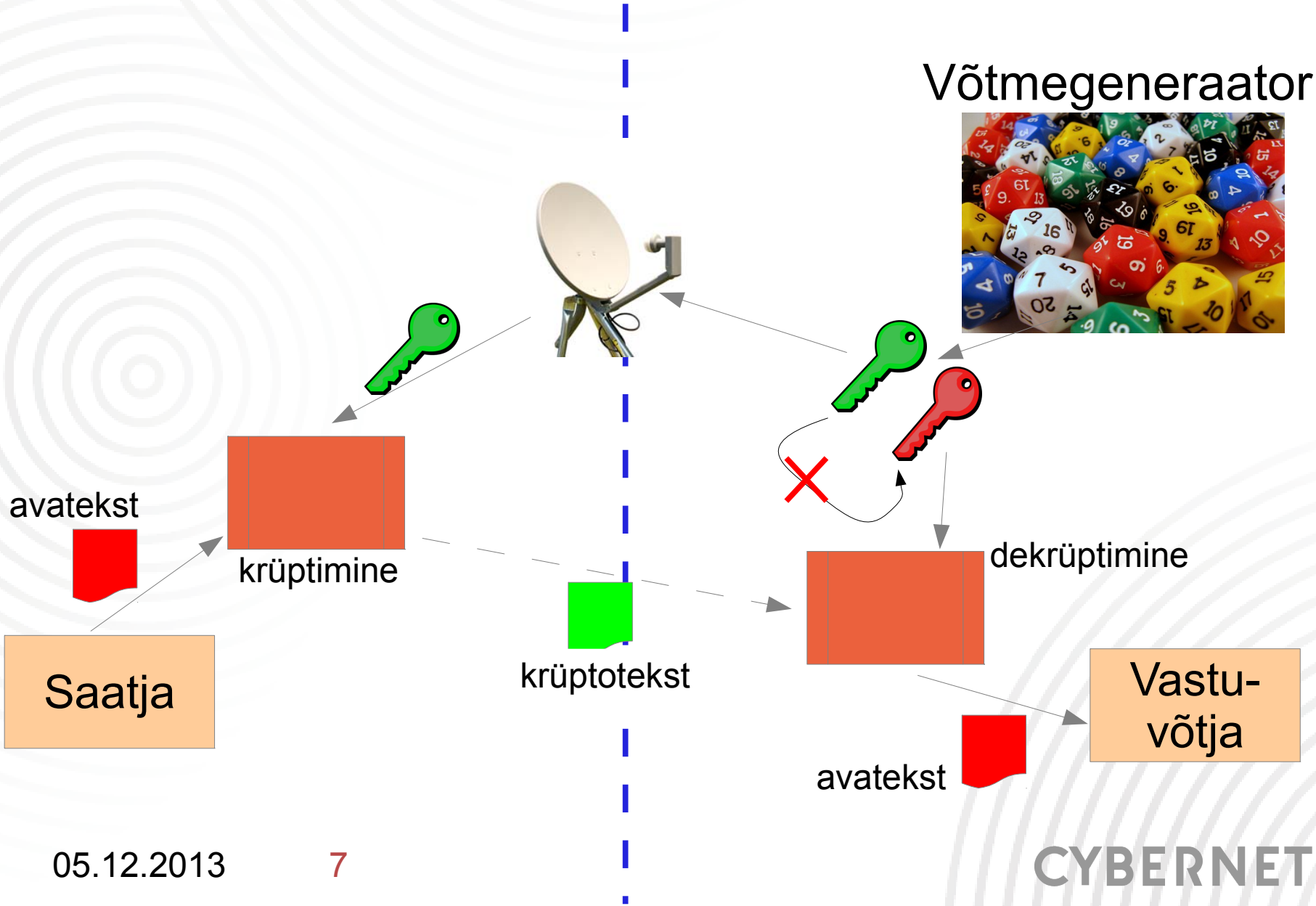


CYBERNETICA

Konfidentsiaalsusprimitiive

- Krüptimine
  - sümmeetrilised krüptosüsteemid
  - asümmeetrilised krüptosüsteemid
- Ühissalastusskeemid
- Turvalised ühisarvutused
- ...

Asümmeetrilised krüptosüsteemid



CYBERNETICA

RSA krüptosüsteem

p=103 ja q=127
n=103·127 = 13081
$\varphi(n)$=12852
e=79
d=3091
m=5678
c=7425

- Vali kaks algarvu p ja q
- Olgu n=pq
- Olgu $\varphi(n)$=(p–1)(q–1)
- Vali e∈{1…n-1}, nii et SÜT(e, $\varphi(n)$) = 1
- Olgu d∈{1…n-1} selline, et de *mod* $\varphi(n)$ = 1
- Avalik võti: (n,e). Salajane võti: (n,d)
  - p, q ja $\varphi(n)$ hoia salajas või hävita
- Avatekst m∈{1…n-1}. Krüptotekst $c = m^e$ *mod* n
- Kui krüptotekst on c, siis avatekst on c^d *mod* n

RSA turvalisusest

- Tegelikult on p ja q u. 300-kohalised arvud
  - n on u. 600-kohaline (2048 bitti)
  - vahetulemused on u. 1200-kohalised
- Arvatakse, et nii suurte arvude tegurdamine on keeruline
- RSA turvalisus põhineb arvust n arvude p ja q leidmise raskusel
  - Ei ole teada viisi dešifreerimiseks, mis p-d ja q-d ei vaja

Kas RSA töötab?

- $n=pq$, $\varphi(n)=(p-1)(q-1)$,
- SÜT(e, $\varphi(n)$) = 1, $de \bmod \varphi(n) = 1$
- Kas $(m^e)^d = m$?
- Leidub k, nii et $de = k\varphi(n) + 1$
- Edaspidi näitame, et:
  - kui SÜT(a,n)=1, siis $a^{\varphi(n)} \bmod n = 1$
- $m^{ed} \equiv m^{k\varphi(n)+1} \equiv m^{k\varphi(n)}.m \equiv (m^{\varphi(n)})^k.m \equiv m \pmod n$
  - kui SÜT(m,n)=1

Arvuteooria mõisteid

- Jaguvus
- Kongruentsid
- Jäägiklassiringid
- Suurim ühistegur
- Laiendatud Eukleidese algoritm
- Pööratavus *mod* n
- Euleri φ-funktsioon

Kuidas suuri täisarve tegurdada?

- Olgu $n=pq$
- Olgu $x, y \in \{1, \ldots, n-1\}$ sellised, et
  - $x^2 \equiv y^2 \pmod{n}$
  - $x \not\equiv \pm y \pmod{n}$
- Siis $kn = x^2 - y^2 = (x-y)(x+y)$
  - x-y ja x+y omavad n-ga mittetriviaalset ühistegurit
- Tegurdamiseks otsime sobivat paari (x, y)

Ruutsõel (1. samm)

- Olgu $\mathcal{B}$ mingite väikeste algarvude hulk
- Otsime arve x, mille korral arvu x^2 *mod* n kõik algtegurid on $\mathcal{B}$-s
  - See on tõenäolisem, kui x on pisut suurem kui $\sqrt{n}$
  - Jätame algtegurduse ka meelde

$$\mathcal{B} = \{p_1, \ldots, p_k\}$$

$$\begin{array}{l|l} x_1 \to e_{11}, \ldots, e_{1k} & x_1^2 \equiv p_1^{e_{11}} \cdots p_k^{e_{1k}} \pmod{n} \\ x_2 \to e_{21}, \ldots, e_{2k} & x_2^2 \equiv p_1^{e_{21}} \cdots p_k^{e_{2k}} \pmod{n} \\ \vdots \to \vdots & \vdots \\ x_m \to e_{m1}, \ldots, e_{mk} & x_m^2 \equiv p_1^{e_{m1}} \cdots p_k^{e_{mk}} \pmod{n} \end{array}$$

Ruutsõel (2. samm)

- Leiame indeksid $i_1,\ldots,i_r$ nii, et iga j jaoks $e_{i_1,j} + e_{i_2,j} + \cdots + e_{i_r,j}$ on paarisarv.
- Siis

$$(x_{i_1} \cdots x_{i_r})^2 \equiv \left(\prod_{j=1}^{k} p_j^{\frac{e_{i_1,j}+\cdots+e_{i_r,j}}{2}} \right)^2 \pmod{n}$$

- Loodetavasti need kaks ruututõstetud arvu pole võrdsed ega teineteise vastandarvud
- Indeksid leiame lineaarvõrrandisüsteemist

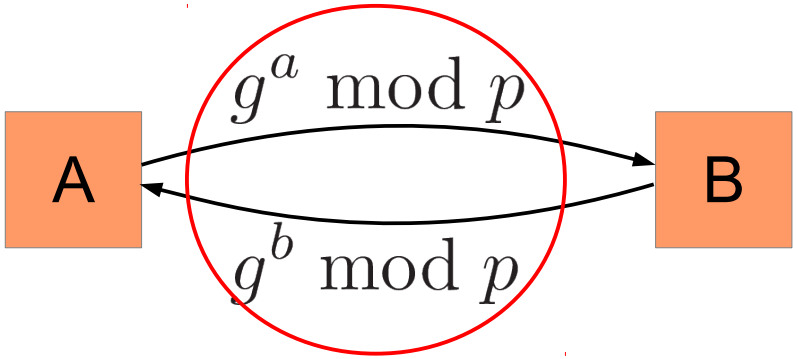
Diffie-Hellmani võtmevahetus

Olgu p suur algarv ja g rühma $\mathbb{Z}_p^*$ *moodustaja*

$$\{1, g, g^2, \ldots, g^{p-2}\} = \mathbb{Z}_p^*$$

$a \xleftarrow{R} \{1, \ldots, p-1\}$

$K = (g^b)^a \bmod p$



$b \xleftarrow{R} \{1, \ldots, p-1\}$

$K = (g^a)^b \bmod p$

ründaja vaade

CYBERNETICA

DH võtmevahetuse turvalisus

- Diskreetse logaritmi probleem:
  - Antud g, h, p, leia a nii, et $g^a \equiv h \pmod{p}$
- Arvatavalt keeruline, kui p on suur
  - ja rahuldab veel mõningaid omadusi
- Diffie-Hellmani probleem:
  - Antud p ning g, g^a, g^b, leia g^{ab} (kõik astmed *mod* p)
- Ei ole teada DH probleemi lahendamisviise, mis ei viiks diskreetse logaritmi lahendamiseni

ElGamal-i krüptosüsteem

- Genereeri arvud p, g, a
  - p ja g võivad olla ka standardis fikseeritud
- Olgu h=g^a mod p
- Avalik võti: (g,h,p). Salajane võti: a (ja g,h,p)
- Avatekst: $m \in \{1 \ldots p\text{-}1\}$.
  - Krüptotekst: (g^r, mh^r), kus r on juhuslik
- Et dekrüptida (c_1,c_2): arvuta $c_2 c_1^{-a}$
- Kõik arvutused on *mod* p

Turvataandus ElGamal → DH

- Oletame, et suudame ElGamali murda
- Lahendame DH probleemi (p,g,g',g'') nii:
  - Siin $g'=g^a$ ja $g''=g^b$, kus a ja b on tundmatud
- Olgu ElG avalik võti (p,g,$(g'')^{-1}$), krüptotekst (g',1)
- Murrame ja saame avateksti x
- See rahuldab: $(g', 1) = (g^a, x \cdot (g^{-b})^a) = (g^a, x \cdot g^{-ab})$
- Seega $x=g^{ab}$

Kuidas arvutada diskreetset logaritmi?

- Geneerilised algoritmid
  - Ajakulu proportsionaalne suurusega $\sqrt{n}$, kus n on rühma elementide arv.
  - Liiga aeglased, kui n on u. 256-bitine
- $\mathbb{Z}_p$-spetsiifilised algoritmid
  - Keerukus sarnane tegurdamise algoritmidele

Elliptilised kõverad

- Punktihulk tasandil, mis rahuldab võrrandit

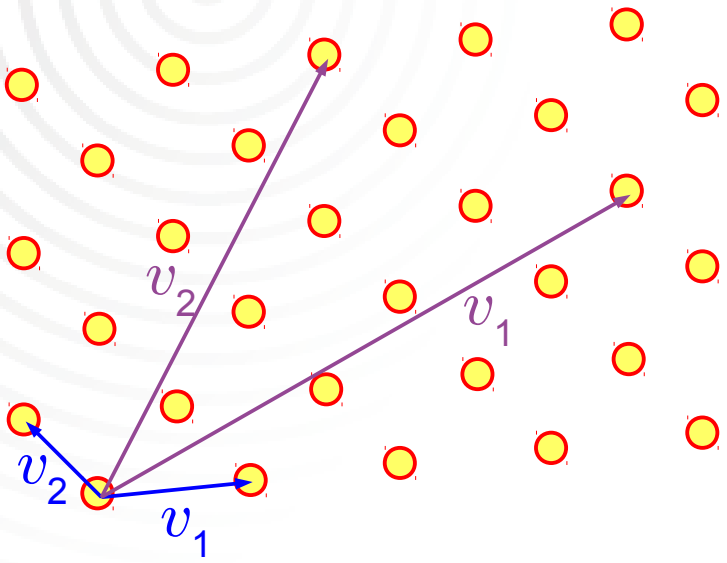
$$y^2 = x^3 + ax + b$$

- Lisaks „punkt lõpmatuses“: O.
- Neil punktidel on defineeritav üks binaarne tehe
  - Selle tehte suhtes on tegemist rühmaga
- Vaatame neid operatsioone üle lõpliku korpuse
- Selle rühma diskreetsete logaritmide jaoks pole teada geneerilisest paremaid algoritme

(Arvu)võred

- Olgu $v_1,\ldots,v_n$ lineaarselt sõltumatud vektorid $\mathbb{R}^n$-s
- Nende poolt määratud võre on punktihulk

$$\{a_1v_1 + \cdots + a_nv_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}$$



võre baas: $v_1,\ldots,v_n$

Baas ei ole unikaalne

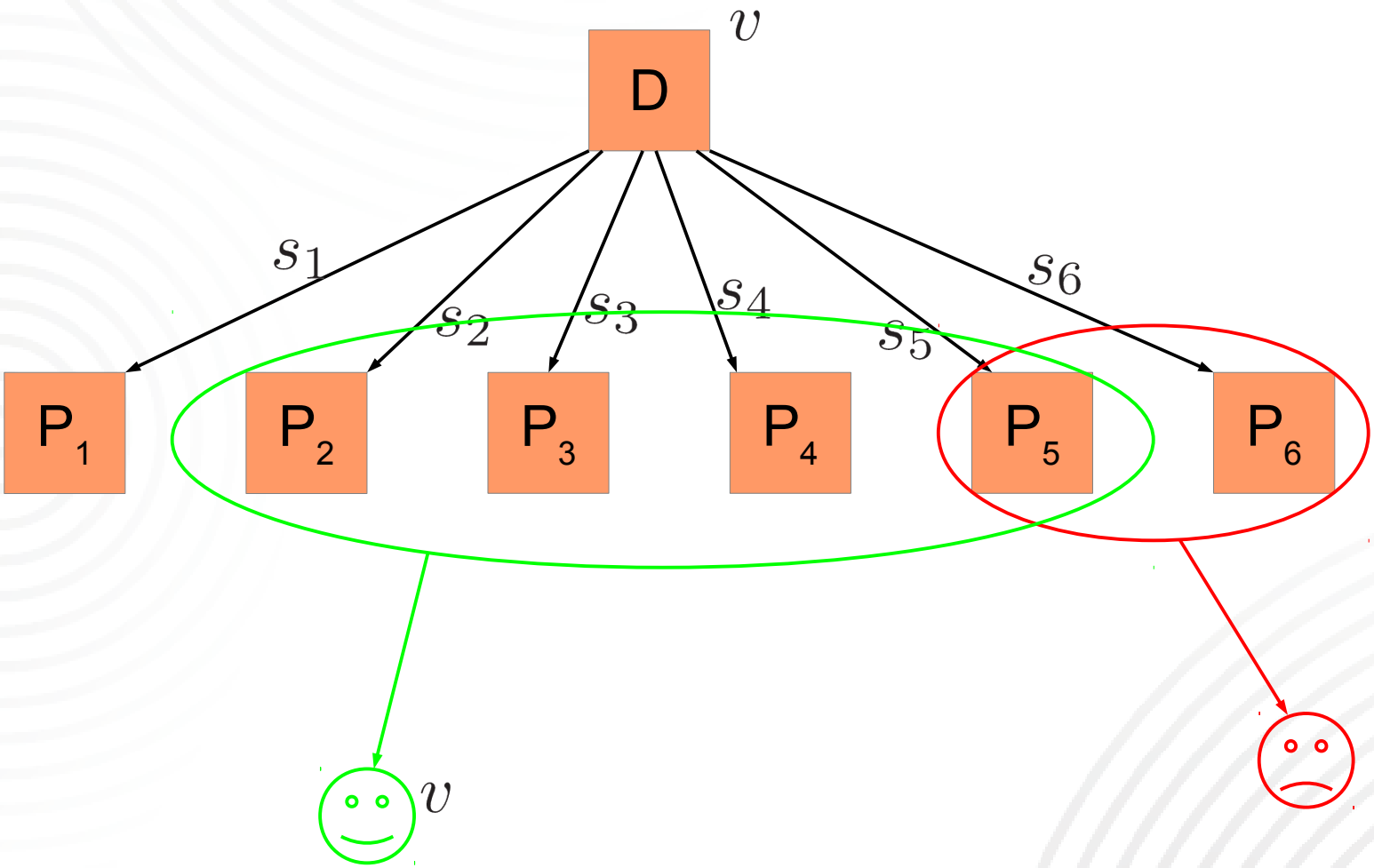
Raskeid probleeme võredes

- Leia lühim nullist erinev vektor võres
- Leia antud vektorile ($\mathbb{R}^n$-st) lähim vektor võres
- Tegemist on arvatavalt raskete probleemidega, kui baas on „ebamugav“
- „Mugavas“ baasis on vektorid peaaegu ortogonaalsed

Krüptosüsteem (üldiselt)

- Avalik võti: „ebamugav baas“
- Salajane võti: „mugav baas“
- Lubatud teated: vektorid, mis on piisavalt lühikesed võrreldes võre punktide vahelise kaugusega
- Krüptimine: vali suvaline punkt võres, lisa sellele teade
- Dekrüptimine: leia krüptotekstile lähim punkt, lahuta see krüptotekstist

Ühissalastusskeemid



CYBERNETICA

Shamiri ühissalastusskeem

- (n,t)-läviturvalisus
  - n osapoolt, kellel on saladuse tükk (osak)
  - Saladuse leidmiseks on tarvis vähemalt t osapoolt
- Saladus v on $\mathbb{Z}_p$ element
- Jagamiseks genereeri $a_1, \ldots, a_{t-1} \xleftarrow{R} \mathbb{Z}_p$
- Olgu $f(x) = v + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$
- P_i osak on $f(i)$
- Rekonstruktsioon: t-st punktist piisab, et leida polünoomi kordajad

Polünoomid

- $f:\mathbb{F}\rightarrow\mathbb{F}$, $f(x)=a_0+a_1x+\ldots+a_tx^t$, $a_i\in\mathbb{F}$
  - $t=\deg(f)$ on polünoomi aste
- v on f-i juur, kui $f(v)=0$
- Kui $\mathbb{F}$ on korpus, siis f-l on ülimalt $\deg(f)$ juurt
  - Kui kaks ülimalt t-nda astme polünoomi on võrdsed vähemalt $(t+1)$-s punktis, siis need polünoomid on võrdsed igal pool
- Polünoome saab liita, korrutada, jäägiga jagada, ühistegureid leida, ...

Polünoomide interpoleerimine

- **Teoreem**. Leidub täpselt üks ülimalt t-1 astme polünoom f, mis läbib punkte $(x_1,y_1),\ldots,(x_t,y_t)$
  - Punktid $x_1,\ldots,x_t$ on kõik erinevad
  - x_i,y_i on korpuse $\mathbb{F}$ elemendid
- **Tõestus.** (Lagrange'i interpolatsioonivalem)

$$f(x) = \sum_{j=1}^{t} y_j \prod_{k \neq j} \frac{x - x_k}{x_j - x_k}$$

  - Ühesus järeldub eelmisel slaidil olnust

Rekonstruktsioon Shamiri skeemis

- Tegelikult huvitab meid ainult $f(0)$
- Kui osapoolte $i_1, \ldots, i_t$ osakud on $s_{i_1}, \ldots, s_{i_t}$, siis

$$v = \sum_{j=1}^{t} s_{i_j} \prod_{k \neq j} \frac{i_k}{i_k - i_j}$$

- Paneme tähele, et v on osakute lineaarkombinatsioon

Shamiri skeemi turvalisus

- Kui meil on olemas t-1 osakut, siis võime v-ks võtta ükskõik, millise väärtuse
  - Leidub ülimalt t-nda astme polünoom, mis on kooskõlas nende t-1 osaku ja valitud v väärtusega
  - Iga v väärtuse jaoks on ühepalju polünoome
- Sama siis, kui meil on veel vähem osakuid
- Infoteoreetiline turvalisus

Veaparanduskoodid

- Mis siis, kui mõni osapooltest rekonstrueerimisel valetab? Kas saab parandada?
- (n,k,d)-veaparanduskood üle hulga X:
  - kujutus $C: X^k \rightarrow X^n$
  - nii et $C(x)$ ja $C(x')$ erinevad vähemalt d positsioonis
- (n,k,d)-veaparanduskoodi abil saab parandada suvalised (d-1)/2 viga

Shamiri skeem kui veaparanduskood

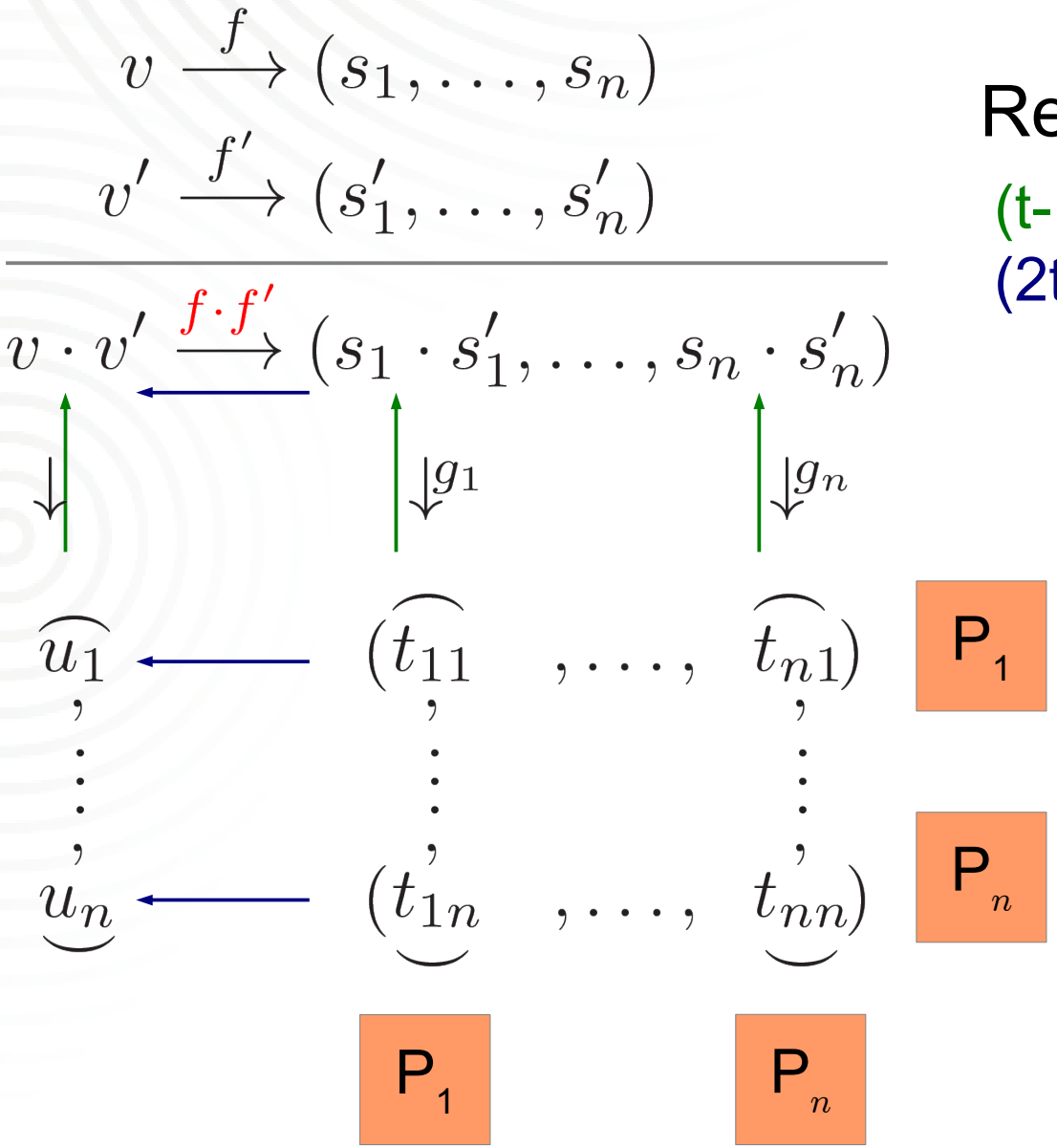
- (n,t)-ühissalastusskeemis
  - $(v,a_1,...,a_{t-1}) \rightarrow (f(1),...,f(n))$
  - Erinevad f-id on võrdsed ülimalt $(t$-1)-s punktis
- Seega on meil $(n,t,n-t+1)$-veaparanduskood
  - Parandada saab kuni $(n-t)/2$ viga
- Parandamiseks on olemas efektiivne algoritm
  - Shamiri ühissalastusskeem on põhimõtteliselt sama, mis Reed-Solomoni veaparanduskood

Turvalised ühisarvutused

Ühissalastatud väärtustega saab arvutada:

$$\frac{v \xrightarrow{f} (s_1, \ldots, s_n) \qquad v' \xrightarrow{f'} (s'_1, \ldots, s'_n)}{v + v' \xrightarrow{f+f'} (s_1 + s'_1, \ldots, s_n + s'_n)}$$

Turvalised ühisarvutused



Rekonstruktsioon:

(t-1)-astme polünoomide
(2t-2)-astme polünoomide

Need lineaar-kombinatsioonid kommuteeruvad

$$n \geq 2t - 1$$

CYBERNETICA

Infoturve Cyberneticas

- Turvalised ühisarvutused (sharemind.cyber.ee)
- Krüptoprotokollide teooria ja praktika
  - X-tee, e-valimised, turvaanalüüsid, ...
  - PKI, ajatembeldus, ID-kaardindus
- Heterogeensete süsteemide turvaanalüüsi teooria
  - ... ja praktika (infosüsteemide audit)
- Krüptograafia keerukusteoreetilised alused

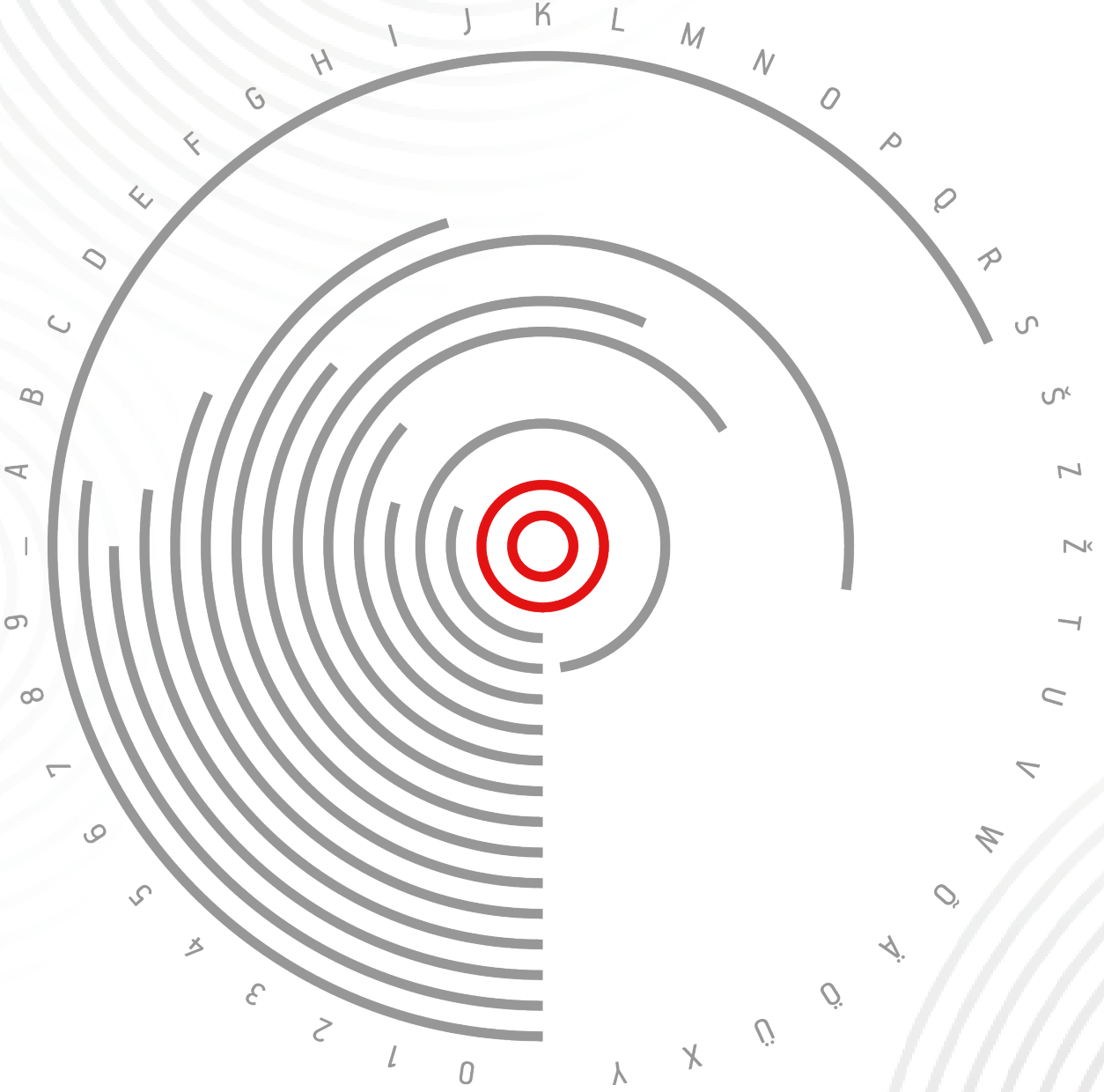
Infoturve Tartu Ülikoolis

- Krüptoprotokollide konstruktsioon
- Krüptoprotokollide analüüsi teooria
- Kvantkrüptograafia
- Krüptograafia teooria

Infoturve Tallinnas

- Küberkaitsega seotud teemad
  - Heterogeensete süsteemide turve (TTÜ)
    - Turvamehhanismide analüüs ja süntees
  - Juriidilised küsimused (CCD CoE)
- Võrgurünnete tuvastamine ja analüüs (CCD CoE)
- Mul ei ole väga head ülevaadet

CYBERNETICA



CYBERNETICA