Matemaatika ja eID

Kalev Pihl

Elektrooniline identiteet

- Definitsioon:
  - Lahendus, mille abil tõendada enda identiteeti üle Interneti
- Eeldus:
  - Inimene ei ole ise võimeline arvutuslikult millegi unikaalsega hakkama saama!
- Lahendus:
  - Inimesele antakse tehniline vidin, mis teeb tema eest midagi arvutuslikult „unikaalset“
- Mure:
  - Elutsüklite lahusus

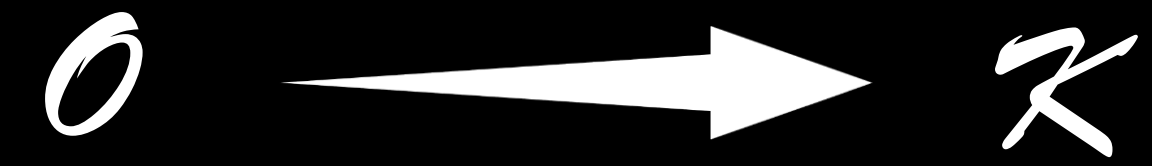
Elektrooniline allkiri

- Definitsioon
  - Isiku seostamise viis allkirjastatud andmetega
- Eeldus:
  - Inimene ei ole võimeline end andmetega seostama
- Lahendus:
  - Andmed seostatakse „isiku“ toiminguga tehnika poolt
- Mure:
  - Otsene kontakt andmetega puudub!

Ühesuunalised funktsioonid

- Funktsioon *f* on ühesuunaline, kui tema arvutamiseks on olemas polünomiaalses ajas töötav algoritm ja mille korral suvaline polünomiaalses ajas töötav tõenäosuslik algoritm F suudab leida kujutisele vastava originaali vääga väikese tõenäosusega.

- Keegi ei tea kas ühesuunalised funktsioonid on olemas!

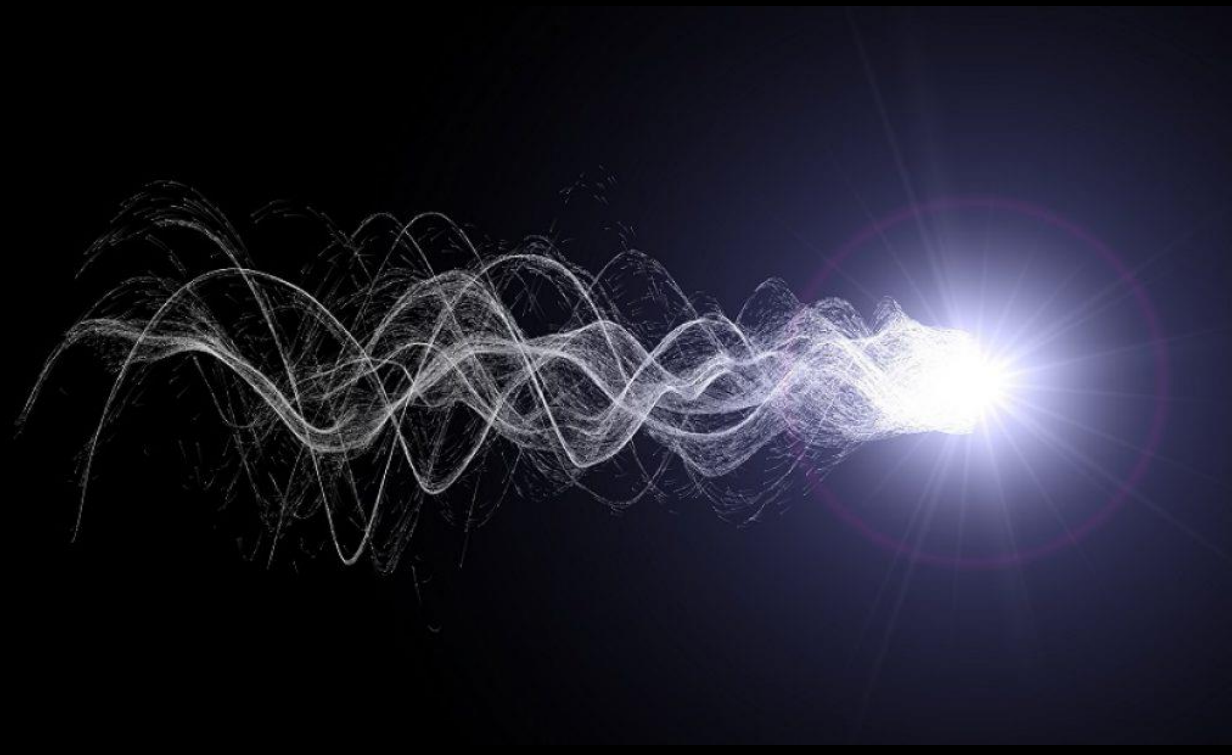


Sobivad funktsioonid ja kvantarvuti

Seni probleemid, millest saab ühesuunalise funktsiooni

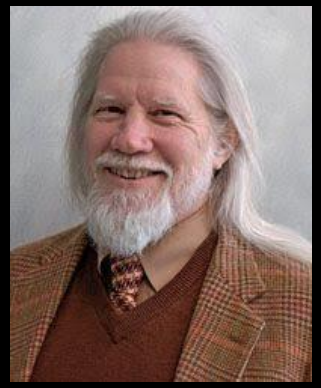
- Faktoriseerimine
- Diskreetse logaritmi lahendamine

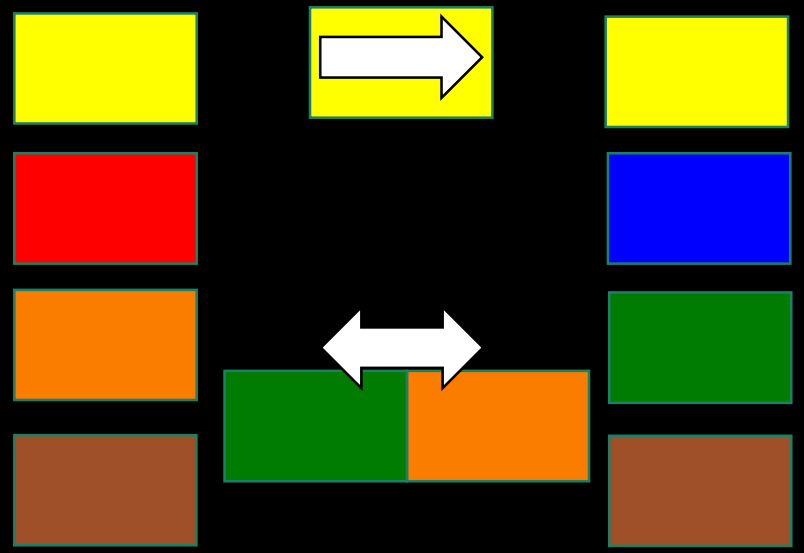
On tegelikult BQP-klassi probleemid

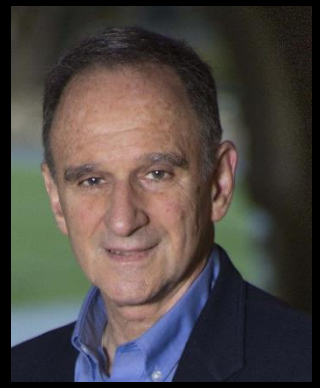


Diffie-Hellmani mõte

- Alusidee: värvide lahutamine algosadeks on keeruline, aga kokku segamine mitte! Värvide segamise järjekord pole oluline.







RSA

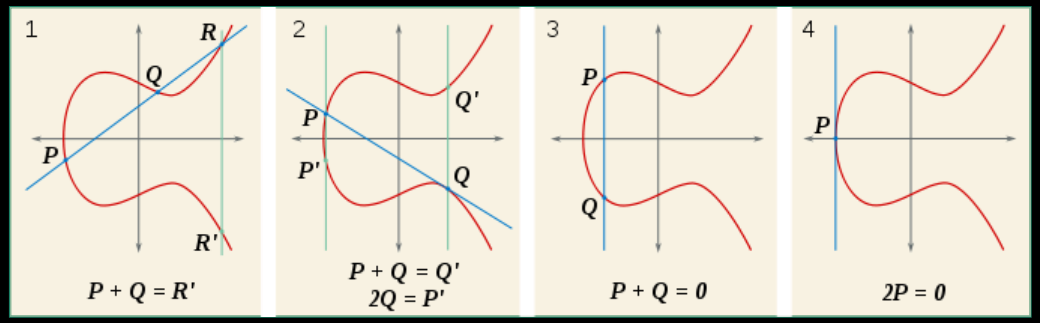
- Alusidee: Korrutamine on kiire, aga arvude faktoriseerimine, ehk algarvulisteks teguriteks jaotamine on keeruline.
- Võtmepaari loomine:
  - p ja q on valitud juhuslikud algarvud
  - n=pq (n pikkus on võtmepikkus)
  - Arvuta t=(p-1)(q-1) – tulemust ei avaldata
  - Vali e ja leia d nii, et $d \cdot e \equiv 1 \pmod{t}$
- Avalik võti: e, n
- Isiklik/privaat/salajane võti: d, n

Krüpteerimine

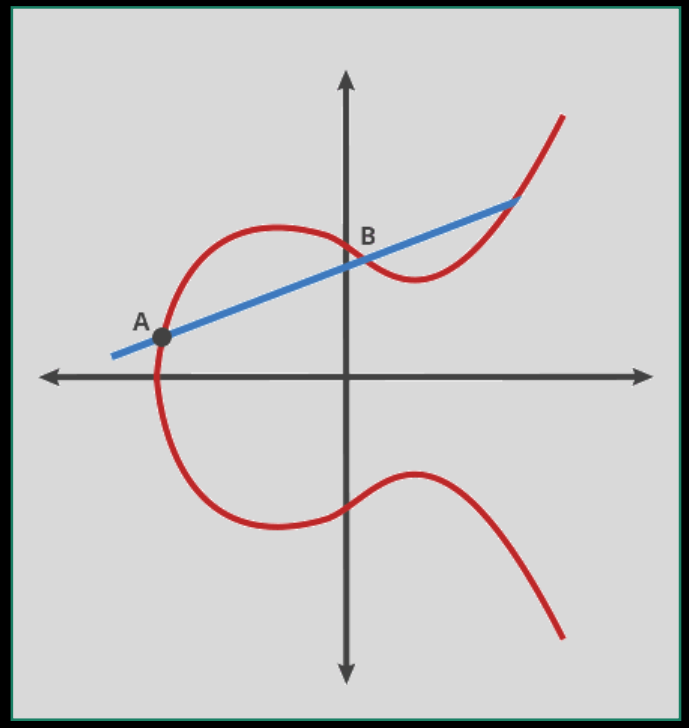
- **Krüpteerimine**
- **C** = $\mathbf{M}^{\mathbf{e}}$ mod **n**
- **Osutub, et kogu eelnev on tore selleks, et dekrüpteerida sõnum alljärgnevalt:**
- $\mathbf{C}^{\mathbf{d}}$ mod **n** = $(\mathbf{M}^{\mathbf{e}})^{\mathbf{d}}$ mod **n**= $\mathbf{M}^{\mathbf{e*d}}$ mod **n** = **M**

ECC

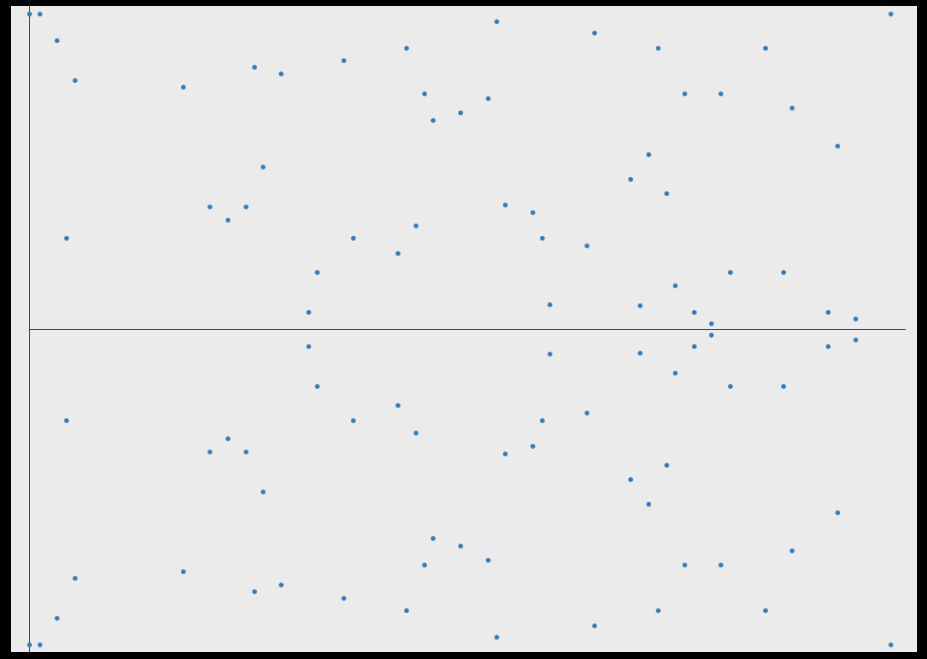
- Alusidee: Diskreetse logaritmi probleem. Elliptilisel kõveral korrutamine on lihtne, jagamine raske.
- Võtmepaari loomine: Skeemis on valitud „kõver“ ja baaspunkt G
  - Avalik võti: Kõvera punkt H = d*G
  - Isiklik/privaat/salajane võti: d



ECC pildid



ECC pildid



ECC krüpteerimine

ECDH
Saladus on S
Alice ja BOB näitel: $S=d_A H_B = d_A (d_B G) = d_B (d_A G) = d_B H_A$

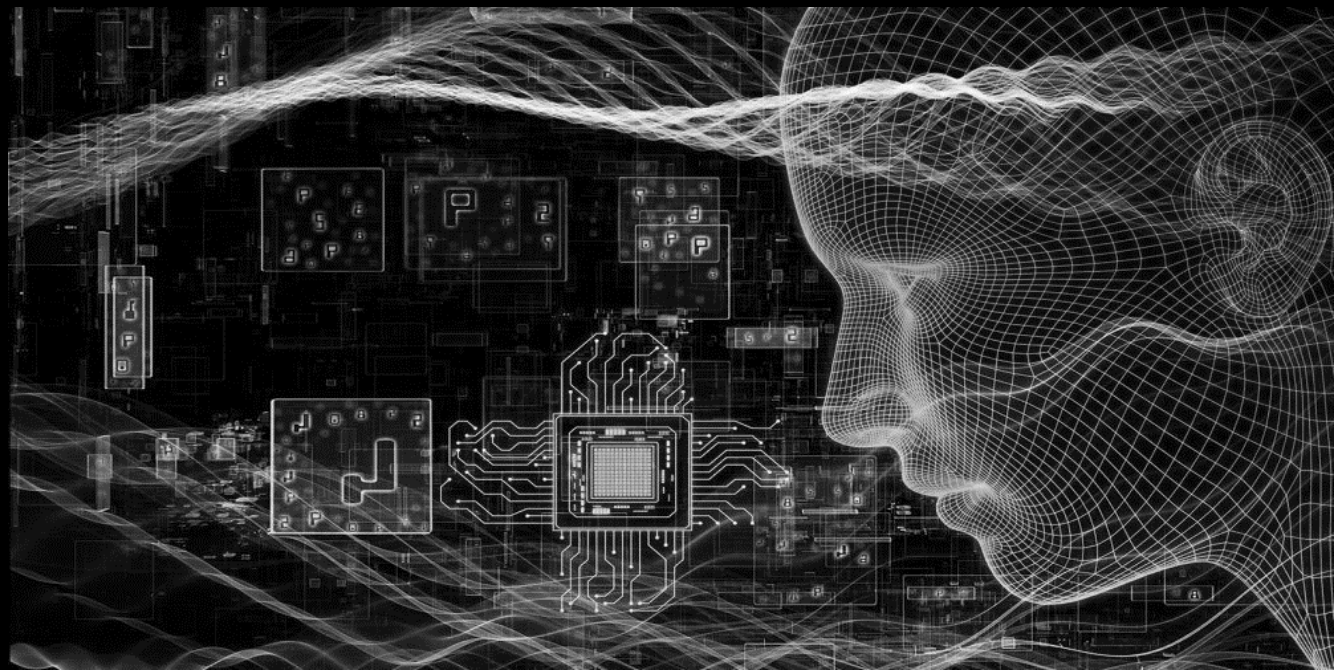
ECDSA
Allkirjastamine

Usaldusteenus

- Kuidas saab üldse usaldada

Praktilised probleemid

- Juhuslikkus
- Algoritmid
- Implementatsioonid
- Riistvara
- Kaitsemeetmed
- Inimene



Tänan!