Võredel põhinev krüptograafia ja miks see oluline paistab?

Kalev Pihl

Vastus

- Uued krüptoalgoritmid on hädavajalikud, et tagada andmete kaitsmise võime ka tähenduslike kvantarvutite tekkumise järgselt
- Võre probleemide omadused on osutunud viimase 30 aasta jooksul “kullasooneks”, et täiendada krüptograafiat.
- Täishomomorfne krüpteerimine:
  - võimaldab säilitada andmete konfidentsiaalsust “pikemalt” kui teistsugused krüpteerimised
  - see võimaldab keerulisi arvutusi usaldada “odavamatesse” ja “võiekamatesse” keskkondadesse
  - on täna “maru aeglane”

Plaan

- Mis on head probleemid asümmetrilises krüptograafias?
- Mis on võred?
- Mis on Learning With Errors (LWE), ehk Vigadega Õppimine (VÕ)?
- Kus LWE kasulik on?

Miks see teema?

- RSA Conference 2024 Annual Awards for Lifetime Achievement and Excellence in the Field of Mathematics:
  - Oded Regev – “Learning with Errors” võredel põhineva krüptograafia väljatöötamise eest 2005. aastal
  - Craig Gentry – Esimese toimiva “Fully Homomorphic Encryption” lahenduse väljatöötamise eest 2009. aastal

Mis on head probleemid asümmetriliseks krüptograafiaks?

Probleem on midagi, mille lahendamise algoritmid on “kallid” ajas ja tehete hulgas

Head probleemid on funktsioonina:

- Ühesuunalised
- Tagauksega
- Suure entroopiaga

Faktoriseerimise näide koolimatemaatikast

Võre

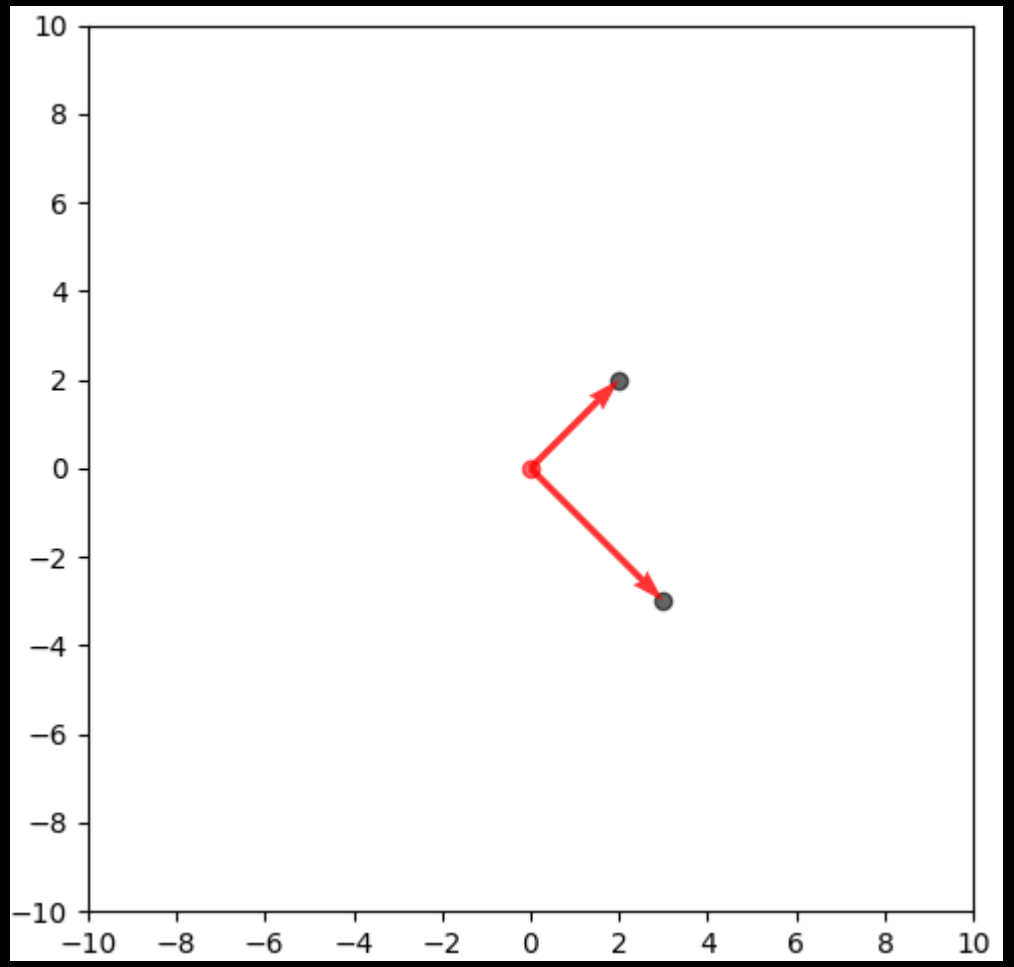
- Punktvõre (Point Lattice) – korrapäraste vahedega punktihulk
- Võre defineerib baas, mis koosneb n-lineaarselt sõltumatust vektorist

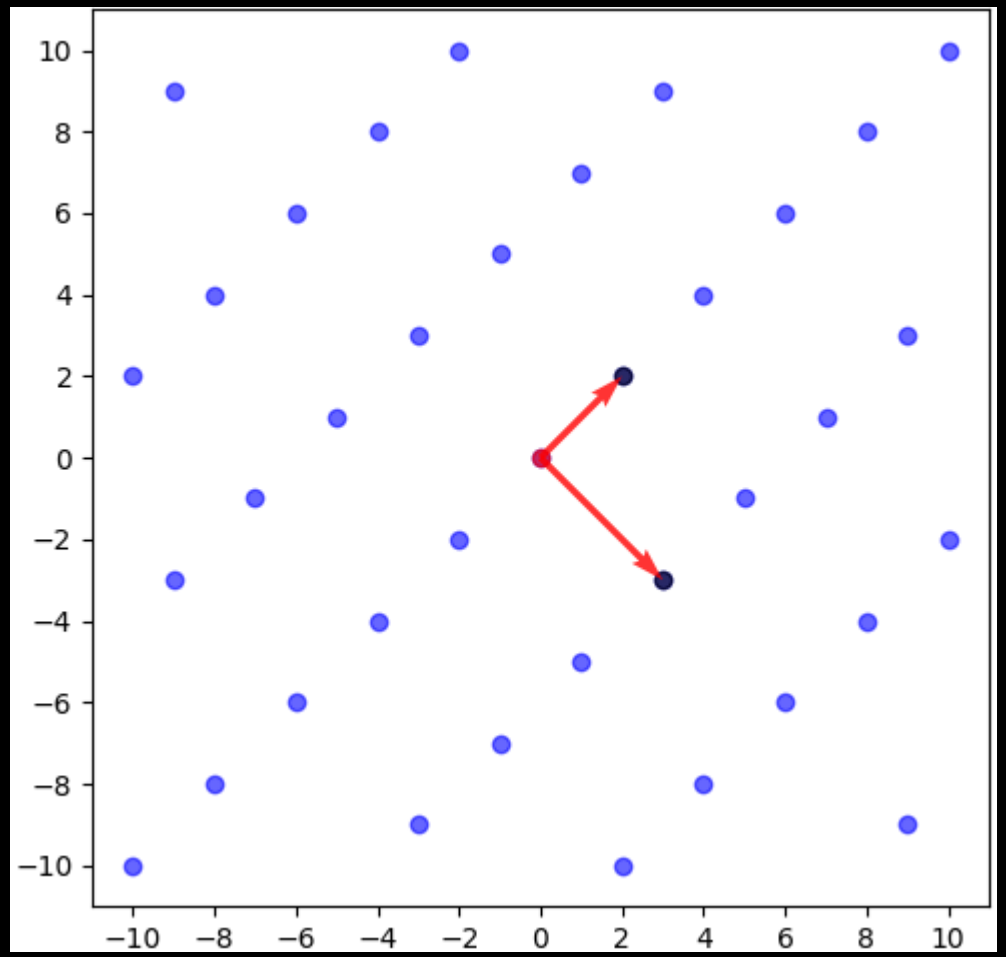
$$\mathrm{B} = \{b_1; b_2; \dots; b_n\} \subset R^n$$

- Võre

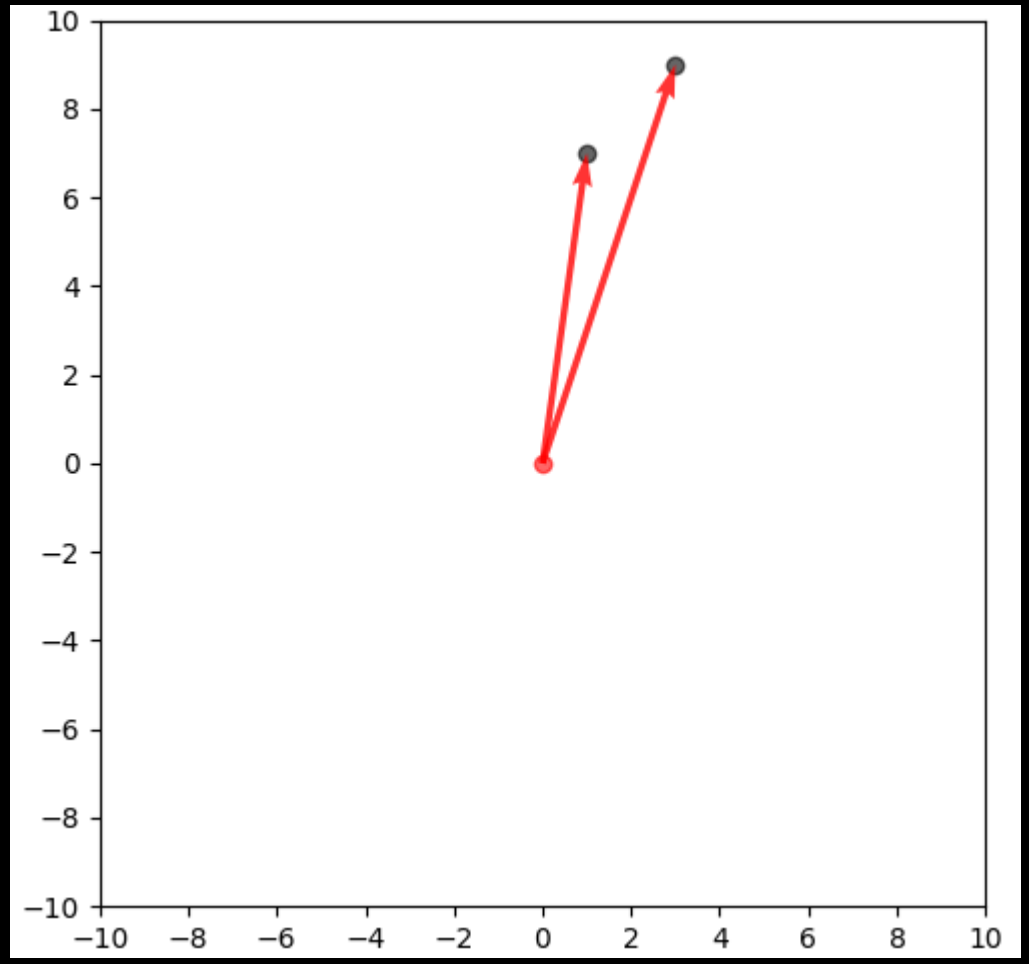
$$\mathcal{L}(B) = \sum_{i=1}^{n} b_i \cdot \mathbb{Z}$$

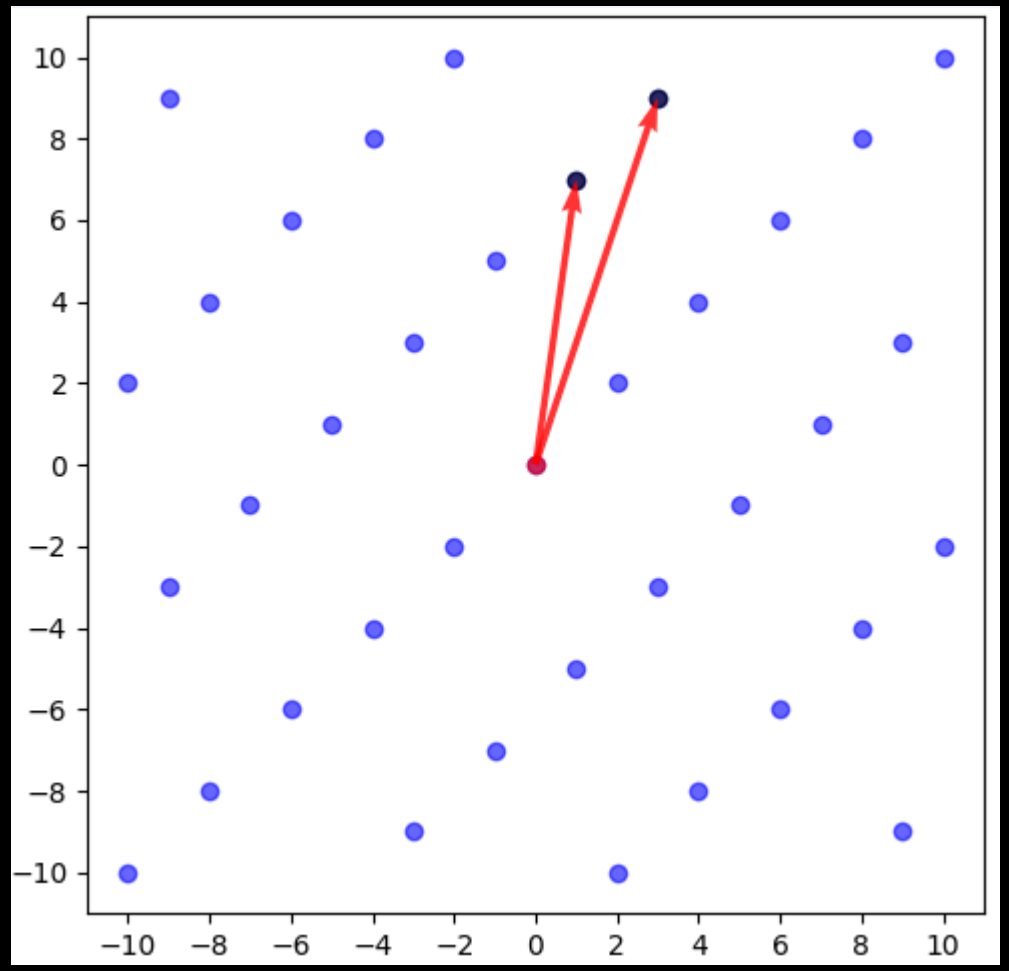
Näide 1


10
8
6
4
2
0
−2
−4
−6
−8
−10
−10 −8 −6 −4 −2 0 2 4 6 8 10

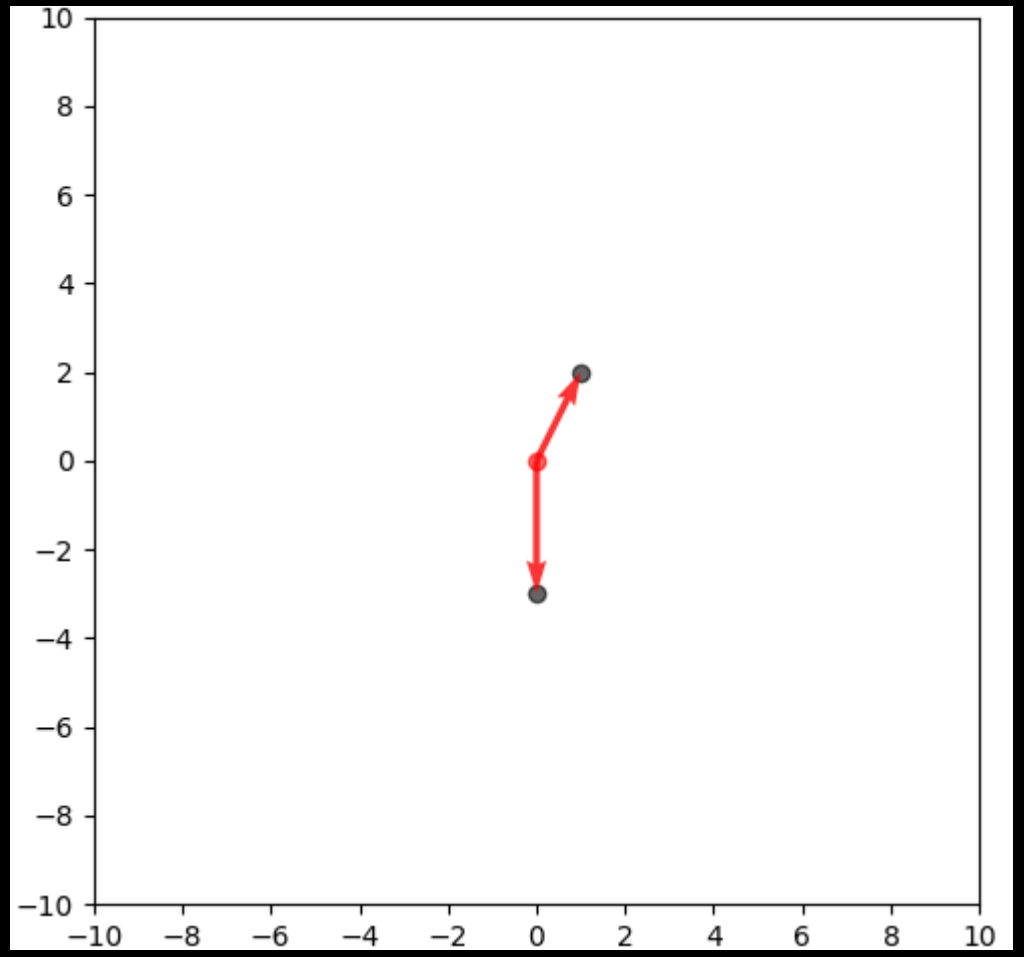

10
8
6
4
2
0
−2
−4
−6
−8
−10
−10 −8 −6 −4 −2 0 2 4 6 8 10

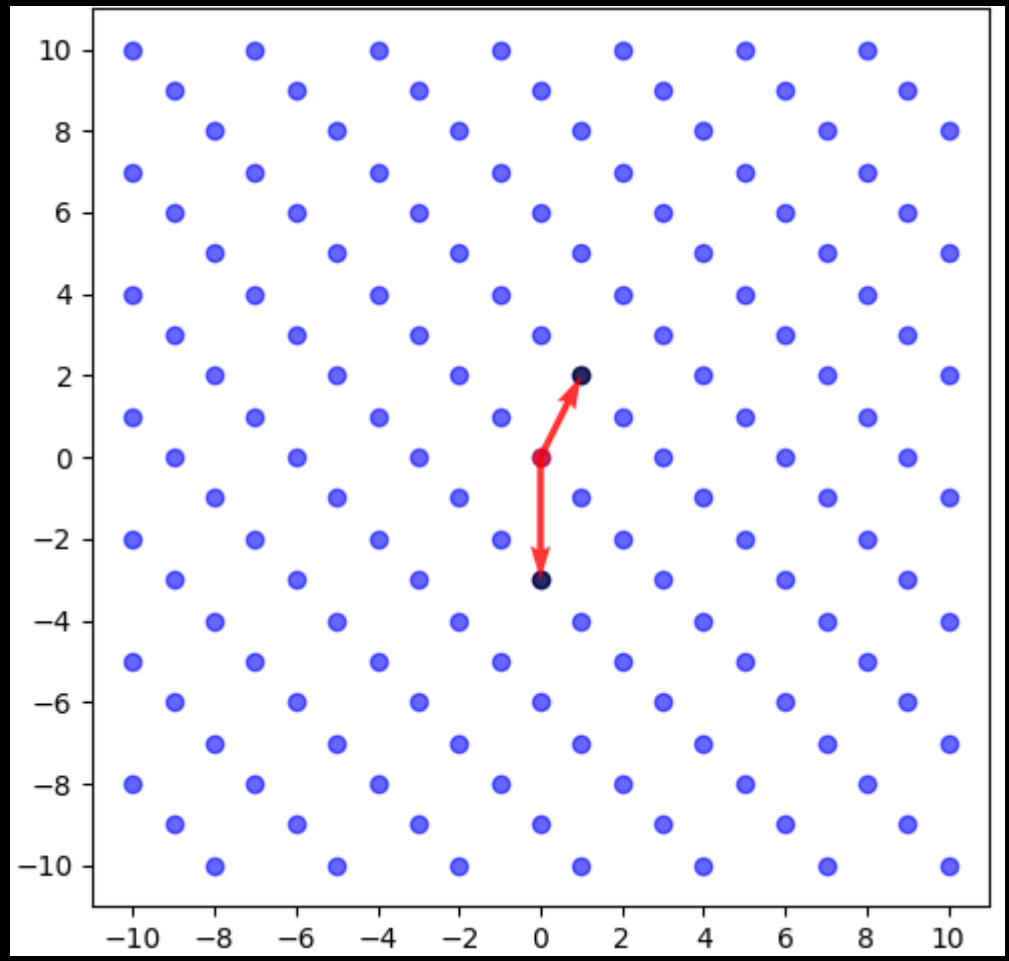
Näide 2


10
8
6
4
2
0
−2
−4
−6
−8
−10
−10 −8 −6 −4 −2 0 2 4 6 8 10


10
8
6
4
2
0
−2
−4
−6
−8
−10
−10 −8 −6 −4 −2 0 2 4 6 8 10

Näide 3


10
8
6
4
2
0
−2
−4
−6
−8
−10
−10 −8 −6 −4 −2 0 2 4 6 8 10


10
8
6
4
2
0
−2
−4
−6
−8
−10
−10 −8 −6 −4 −2 0 2 4 6 8 10

Võre funktsioonid

- Võre determinant on baasi vektorite moodustatud kujundi “ruumala”. Eri baasid samale võrele annavad sama determinandi. Samas kõik sama determinandiga võred ei kattu.

- n-mõõtmelises ruumis on võre punkti ümber võimalik leida kuni n lineaarselt sõltumatut võre punkti, ehk lähimat võre punkti. Samas suunas on sama kaugel alati 2 punkti. Saab tekitada minimaalsete kauguse vahelise seose:

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$$

- Võre kauguse funktsioon:

$$\mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \|t - x\|$$

- Võre katvuse raadius:

$$\mu(\mathcal{L}) = \max_{t \in span(\mathcal{L})} \mu(t, \mathcal{L})$$

Võre probleemid

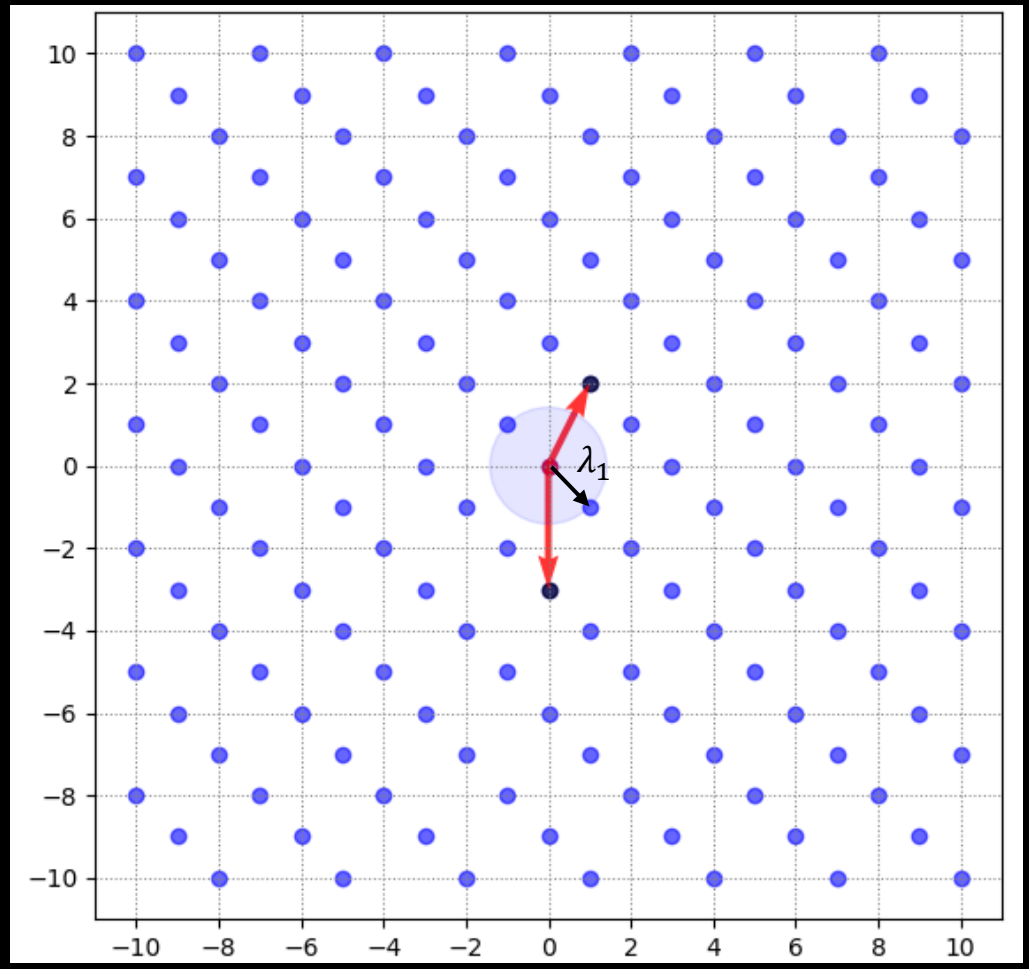
- Osutub, et võrega seondub suur hulk “keerulisi probleeme”
- Determinanti oskame arvutada , aga lühimaid vektoreid λ_i mitte. Proovitakse siis eri teadlaste poolt leida mingeid piire ülemisi ja alumisi neile näiteks:

$$\lambda_1 \leq \sqrt{n}\,\det(\mathcal{L})^{1/n}$$

Lühima vektori problem
SVP - Shortest Vector Problem

- Definitsioon:

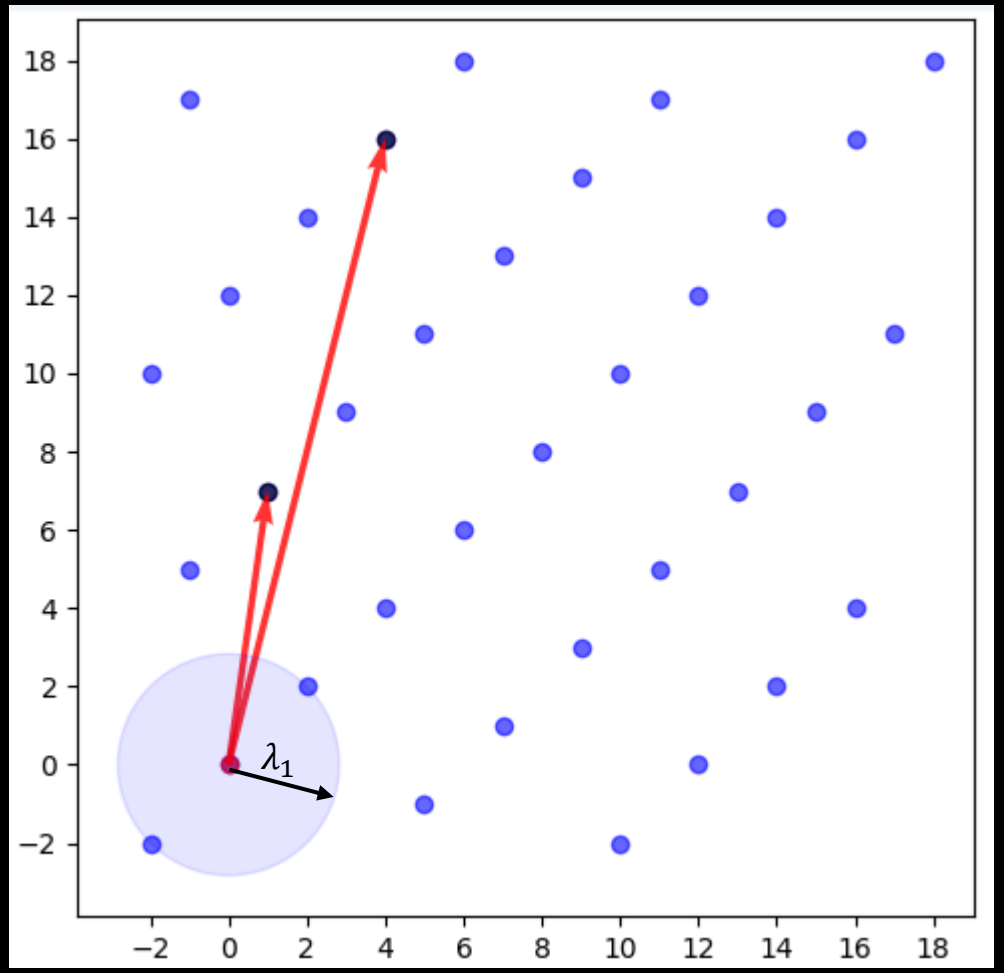
Leia võre $\mathcal{L}(B)$ nullist erinev vektor Bx $(x \in \mathbb{Z}^k)$ nii, et $\|Bx\| \leq \lambda_1$



Lühima vektori problem
SVP - Shortest Vector Problem

- Definitsioon:

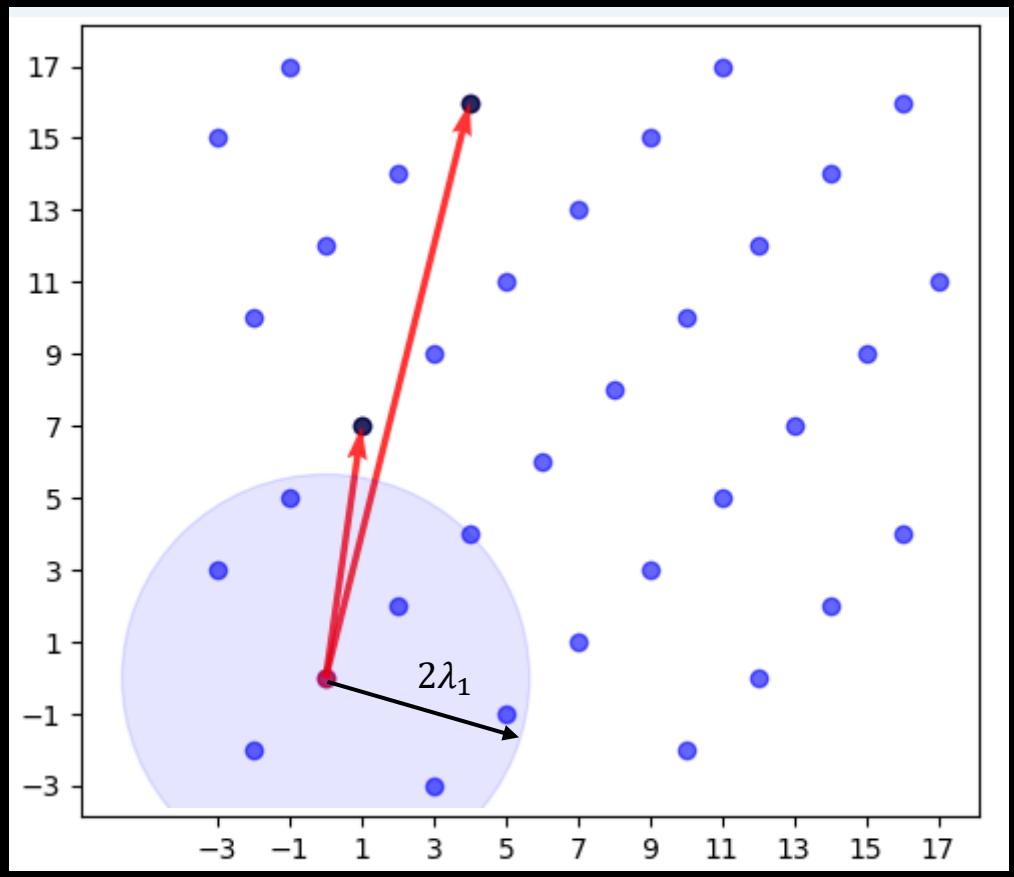
Leia võre $\mathcal{L}(B)$ nullist erinev vektor Bx $(x \in \mathbb{Z}^k)$ nii, et $\|Bx\| \leq \lambda_1$



Peaaegu lühima vektori probleem
ASVP – Approximate Shortest Vector Problem

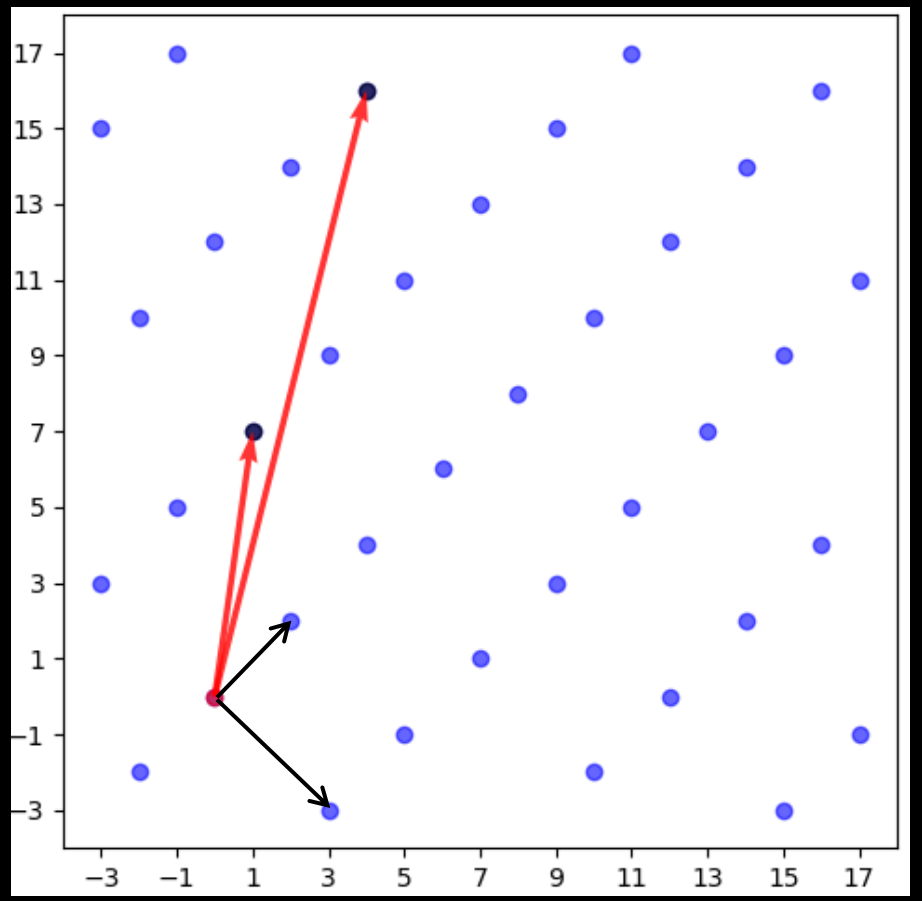
- Definitsioon:

Leia võre $\mathcal{L}(B)$ nullist erinev vektor Bx $(x \in \mathbb{Z}^k)$ nii, et $\|Bx\| \leq \gamma\lambda_1$



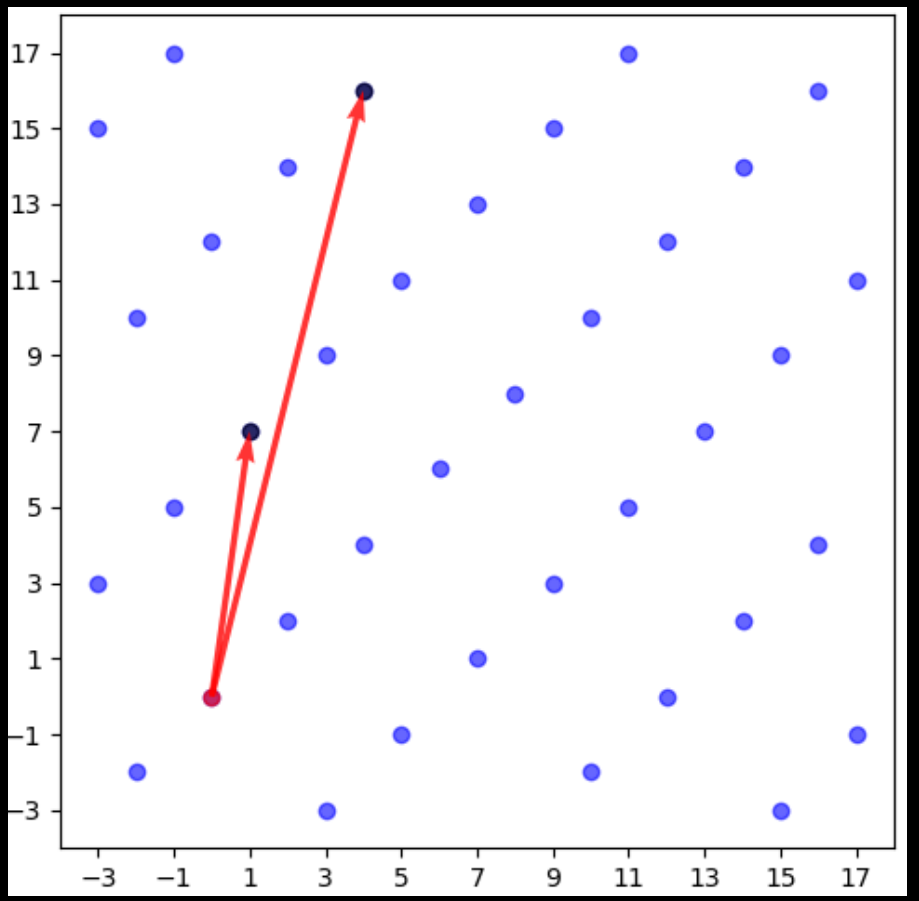
Lühimate sõltumatute vektorite probleem
SIVP – shortest independent vector problem

- Leia võre $\mathcal{L}(B)$ n lineaarselt sõltumatut vektorit $Bx_1, \dots, Bx_n$ pikkusega $\max_i \|Bx_i\| \leq \lambda_n$



Lühikeste sõltumatute vektorite probleem Approximate SIVP

- Leia võre $\mathcal{L}(B)$ n lineaarselt sõltumatut vektorit $Bx_1, \ldots, Bx_n$ pikkusega $\max_i \|Bx_i\| \leq \gamma\lambda_n$



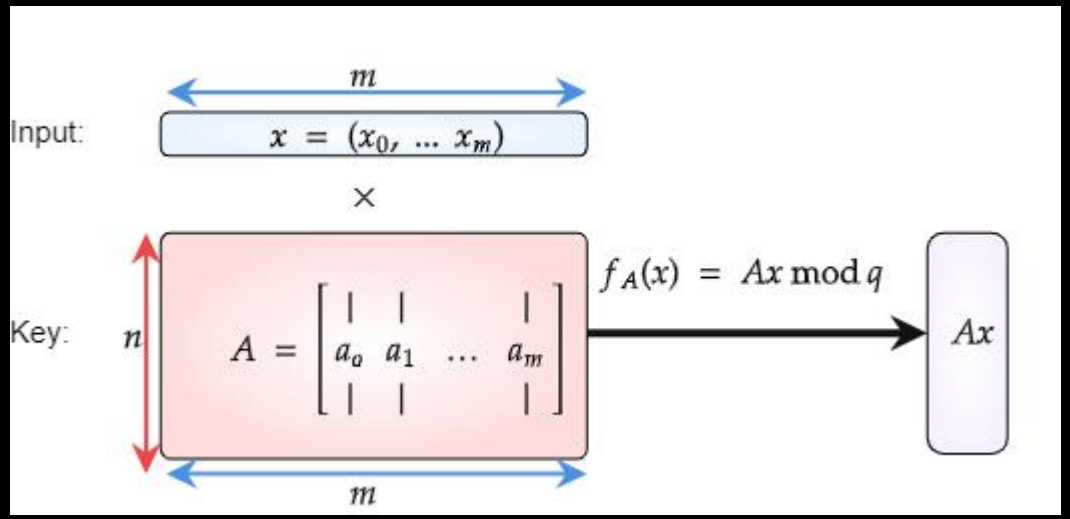
Väikeste täisarvudega lahendus
SIS - Short Integer Solution

- Leia juhuslike vektorite $a_i \in \mathcal{L}(B)$ jaoks lühike mittetriviaalne lahend
  $z_i \in \mathbb{Z}$ nii, et

$$\sum_{i=0}^{m} z_i \cdot a_i = 0$$

Ajtai ühesuunaline funktsioon

- Parameetrid $m, n, q \in \mathbb{Z}$
- Võti: $A \in \mathbb{Z}_q^{n \times m}$
- Sisend: $x \in \{0,1\}^m$
- Väljund: $f_A(x) = Ax \bmod q$



Teoreem:

Kui *SIVP* on keeruline probleem, siis iga $m > n \log q$ korral on $f_A(x) = Ax \bmod q$ ühesuunaline funktsioon

Näide Ajtai funktsioonist

x	1	0	1	1	0	0	1	1	0	mod q=10
A	6	7	4	9	0	3	5	1	9	5 Ax
	7	1	4	2	1	0	7	8	3	8
	5	3	3	1	2	8	7	6	7	2
	7	2	6	6	2	2	4	9	7	2

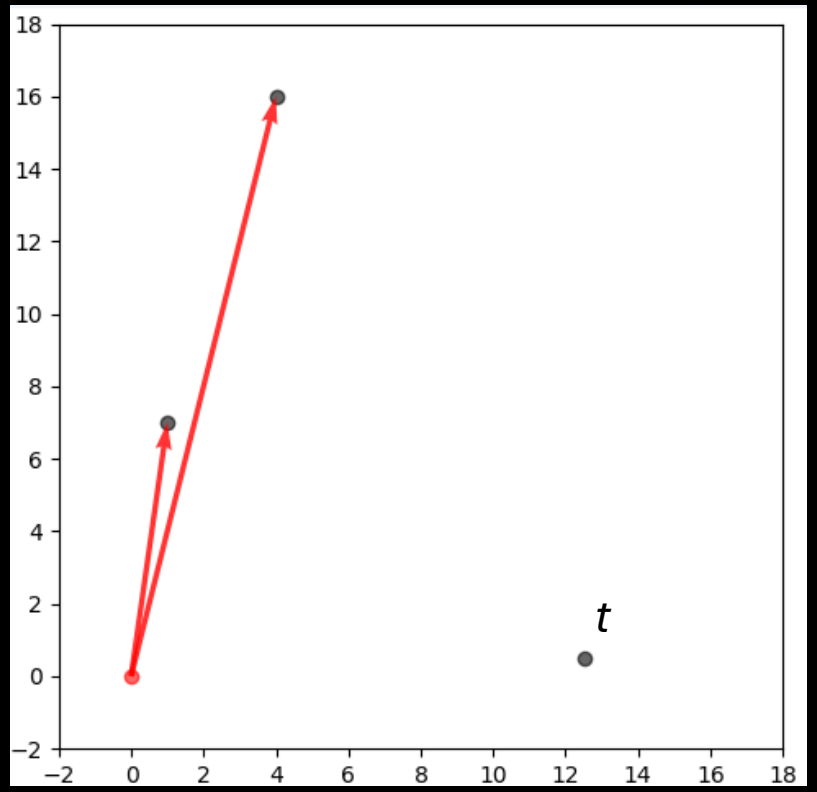
Kuidas Ajtai funktsioon seostub võrega?

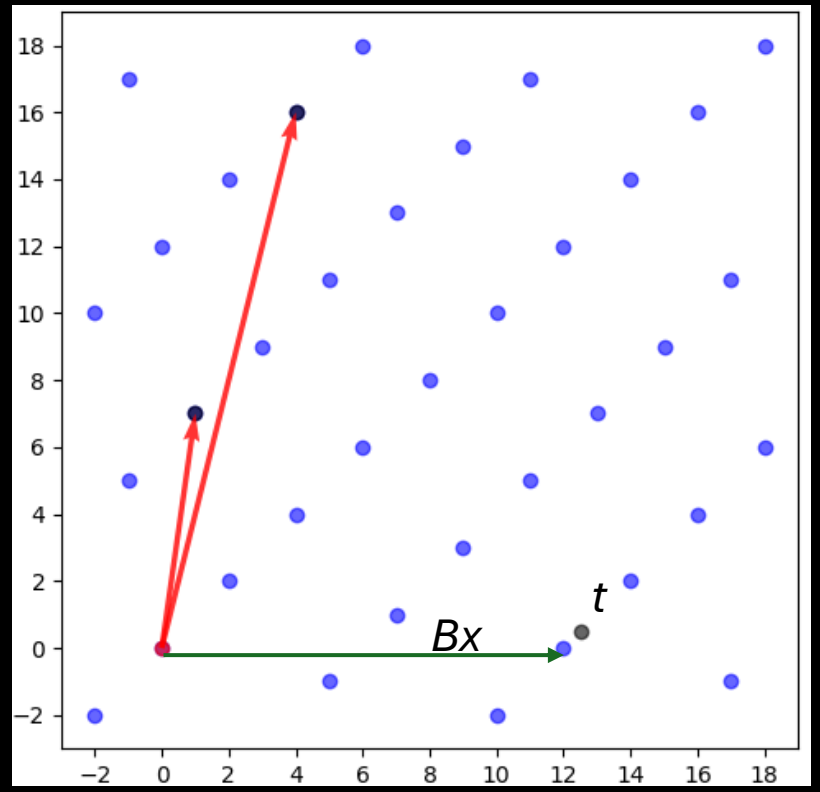
- Antud *A* ja *Ax* abil leia *x*?
- Lihtne on leida “mingi sisend” *t*, mille korral *Az=y(mod q)*

- Kõik lahendid *Ax=y* puhul on kujul *t* + *”maatriks A tuum”*, kus *“maatriks A tuum”* $= \{x \in \mathbb{Z}^m : Ax = 0 \bmod q\}$.
  Maatriksi *A* tuumaks nimetatakse lineaarkujutuse tuuma.
- Võre probleem seega on:
  Leia lühike vektor lineaarkujutuste tuumas, mis oleks *t* lähedal

CVP – Closest Vector Problem

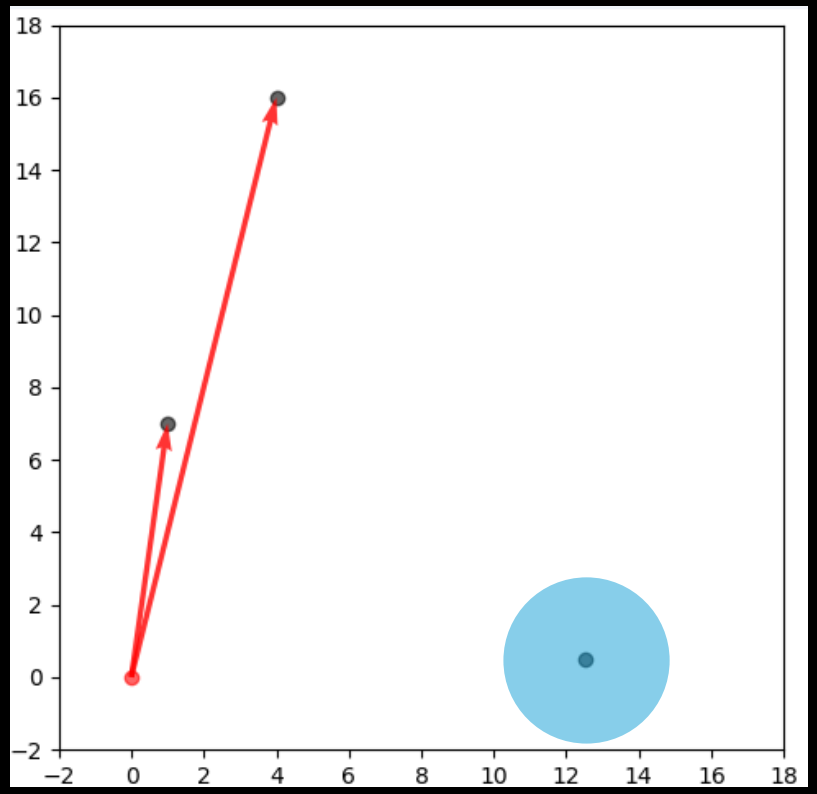
- Leia võres $\mathcal{L}(B)$ vektor Bx, mis on etteantud punktile t lähim, ehk $\|BX - t\| \leq \mu$

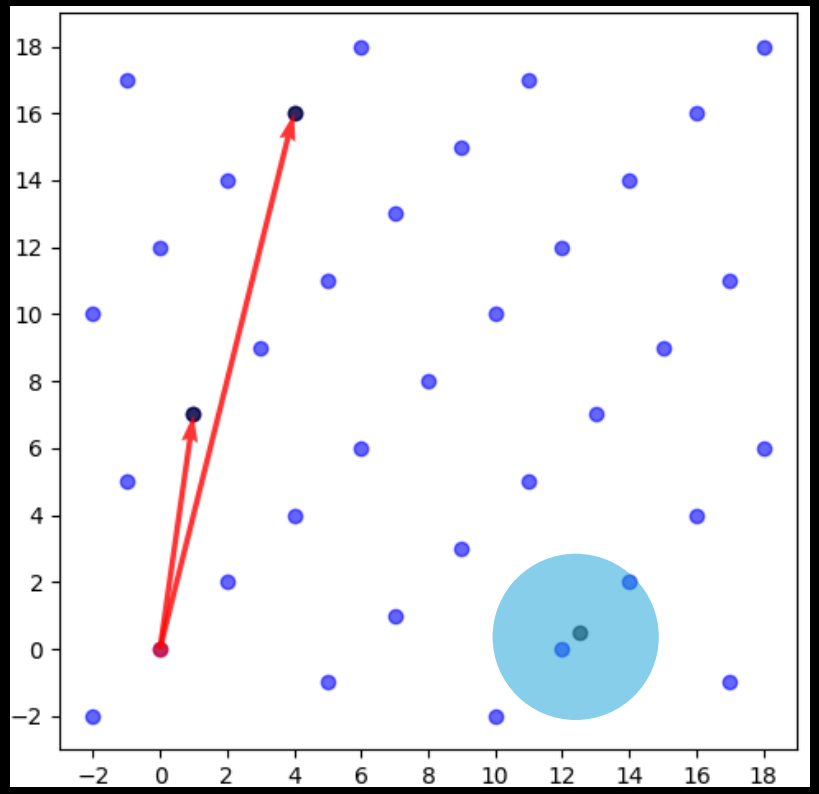




ACVP – Approximate Closest Vector Problem

- Leia võres $\mathcal{L}(B)$ vektor Bx, mis on lähedal etteantud punktile t ehk $\|BX - t\| \leq \gamma\mu$





Vigadega õppimise (VÕ) ehk Learning With Errors (LWE) probleem

- Leidmisprobleem – leia etteantud punktile lähim võre punkt
- Otsustusprobleem
  - Kas see on juhuslik punkt või LWE punkt? Erista võrelähedane punkt juhuslikust punktist.
  - Kui lühim vektor on probleem, siis ka punkti leidmine ja vahe tegemine, mis on lähim punkt on keerukas.

Võredel põhinev krüpteerimine praktikas

- Minu avalik võti on (mod 1000)

  20 404 830 992 341 145 759 507

- Krüpteerimaks bitti valige mistahes arvud minu avalikus võtmes liitke kokku (mod 1000) ja lisage oma salasõnum: “0” või “1”

Mis toimus?

kordajad	62	66	60	72	55	53	49	67
vea jaotus	6	2	10	8	6	4	6	8
avalik võti	6020	6404	5830	6992	5341	5145	4759	6507
moduliga avalik võti	20	404	830	992	341	145	759	507

- Tsükli võti 97
- Moodul 1000
- Dekrüpteerimisel jagatakse krüptogramm 97’ga mod 1000 ning kui jääk on paarisarv siis on krüpteeritud 0 ning kui paaritu, siis krüpteeriti 1

Veidi keerukam näide

- Salajane võti on vektor *n*-mõõtmelises ruumis
- Avalik võti on lineaarkombinatsioonide loend (*m* rida ja *m*>*n*)

$$\sum a_{ij} v_i = m_j + e_j \ (mod\ q)$$

- 0 krüpteerimine lisab 0 ja 1 krüpteerimine lisab *int(q/2)*

Näide

Salajane võti

- x = (4; 27; 55; 13)

Avalik võti on

$$
\begin{array}{rcrcrcrcrcr}
80x & + & 38y & + & 16z & + & 53w & = & 5 & + & 1 \pmod{97} \\
44x & + & 93y & + & 12z & + & 81w & = & 35 & + & 0 \pmod{97} \\
96x & + & 20y & + & 67z & + & 41w & = & 1 & + & -2 \pmod{97} \\
33x & + & 64y & + & 19z & + & 18w & = & 35 & + & -2 \pmod{97} \\
56x & + & 26y & + & 56z & + & 79w & = & 86 & + & -1 \pmod{97} \\
26x & + & 69y & + & 57z & + & 61w & = & 75 & + & 1 \pmod{97} \\
36x & + & 27y & + & 49z & + & 85w & = & 17 & + & 0 \pmod{97} \\
40x & + & 12y & + & 10z & + & 75w & = & 69 & + & -1 \pmod{97} \\
77x & + & 16y & + & 38z & + & 63w & = & 60 & + & 2 \pmod{97}
\end{array}
$$

$$
\begin{array}{rcrcrcrcr}
80x & + & 38y & + & 16z & + & 53w & = & 6 \pmod{97} \\
44x & + & 93y & + & 12z & + & 81w & = & 35 \pmod{97} \\
96x & + & 20y & + & 67z & + & 41w & = & 96 \pmod{97} \\
33x & + & 64y & + & 19z & + & 18w & = & 33 \pmod{97} \\
56x & + & 26y & + & 56z & + & 79w & = & 85 \pmod{97} \\
26x & + & 69y & + & 57z & + & 61w & = & 76 \pmod{97} \\
36x & + & 27y & + & 49z & + & 85w & = & 17 \pmod{97} \\
40x & + & 12y & + & 10z & + & 75w & = & 68 \pmod{97} \\
77x & + & 16y & + & 38z & + & 63w & = & 62 \pmod{97}
\end{array}
$$

Krüpteerimine

- Valime read ja liidame kokku ning lisame kas 0 või 48

80	x	+	38	y	+	16	z	+	53	w	=	6 (mod 97)
44	x	+	93	y	+	12	z	+	81	w	=	35 (mod 97)
96	x	+	20	y	+	67	z	+	41	w	=	96 (mod 97)
33	x	+	64	y	+	19	z	+	18	w	=	33 (mod 97)
56	x	+	26	y	+	56	z	+	79	w	=	85 (mod 97)
26	x	+	69	y	+	57	z	+	61	w	=	76 (mod 97)
36	x	+	27	y	+	49	z	+	85	w	=	17 (mod 97)
40	x	+	12	y	+	10	z	+	75	w	=	68 (mod 97)
77	x	+	16	y	+	38	z	+	63	w	=	62 (mod 97)
29	x	+	23	y	+	69	z	+	74	w	=	15 (mod 97)

Dekrüpteerimine

$$29x + 23y + 69z + 74w = 15 \pmod{97}$$

$$x = (4 ; 27 ; 55 ; 13)$$

$$29 \cdot 4 + 23 \cdot 27 + 69 \cdot 55 + 74 \cdot 13 = 62 \pmod{97}$$

Allkirjastamine

- Avalik võti $(A, T), A \in \mathbb{Z}_q^{K \times L}, T = AS_1 + S_2 \in \mathbb{Z}_q^K$
- Salajane võti $(S_1, S_2), S_1 \in \mathbb{Z}_q^{L \times n}, S_2 \in \mathbb{Z}_q^{K \times n}$
- Kinnitatav väärtus $y \in \mathbb{Z}_q^L$, kinnitus w_{approx}
- Sõnum *M*. See lisatakse vektoriga c $= f\left(M, psrand(w_{approx})\right)$, c $\in \mathbb{Z}_q^n$
- Tingimus: S_1, S_2, y, y_2, c on kõik valitud "väikeste koefitsentidega"
- Allkiri: $w_{approx} = Ay + y_2, y_2 \in \mathbb{Z}_q^K, z = y + S_1 c$
- Kontroll: z on väikeste väärtustega ja $Az - Tc \approx w_{approx}$

$$A(z) - (T)c = A(y + S_1 c) - (AS_1 + S_2)c = Ay + AS_1 c - AS_1 c - S_2 c = Ay - S_2 c$$

NIST: FIPS 204

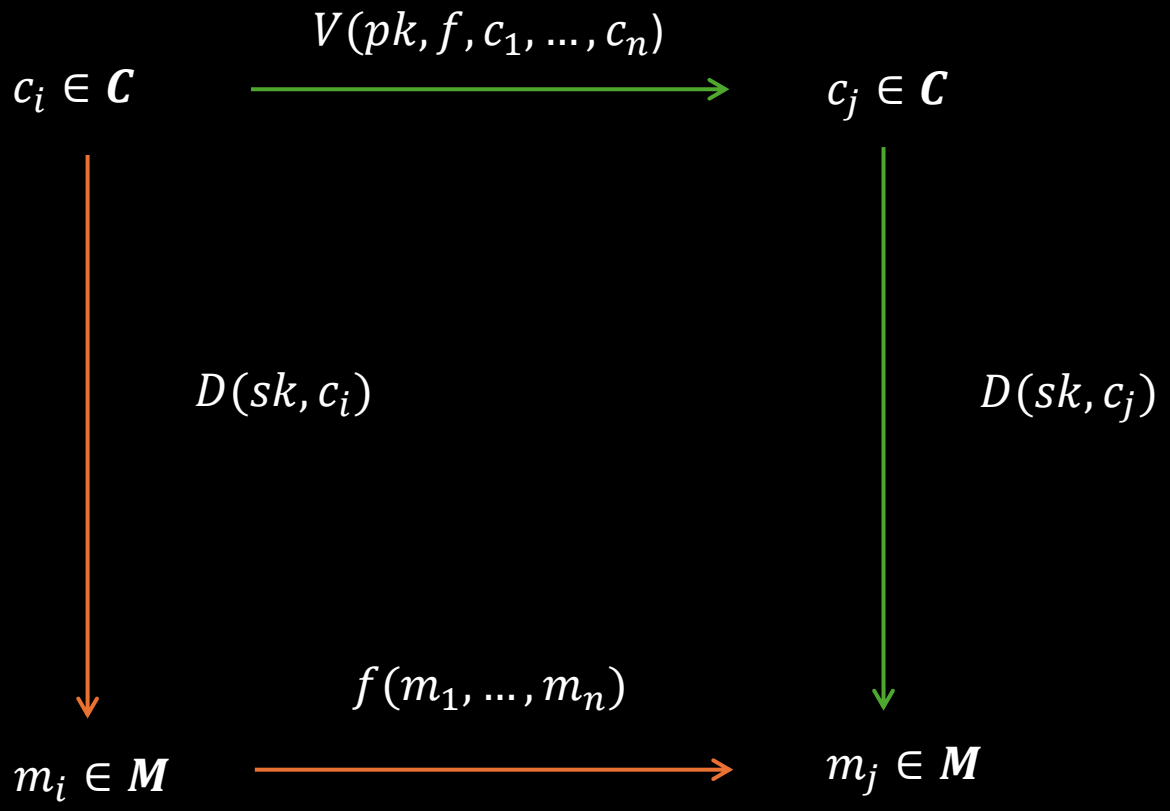
- Defineerib 3 allkirjastamise algoritmi:
  - ML-DSA-44
    - A on 4x4 maatriks
    - Koefitsendi/vigade vahemik [-2,2]
  - ML-DSA-65
    - A on 6x5 maatriks
    - Koefitsendi/vigade vahemik [-4,4]
  - ML-DSA-87
    - A on 8x7 maatriks
    - Koefitsendi/vigade vahemik [-2,2]
- Moodul q =8 380 417

Täishomomorfne krüptograafia
FHE – Fully Homomorphic Encryption

- Meil on privaatsed sõnumid m_1 ja m_2
- Sõnumi privaatsise säilitamiseks me teeme neist krüptogrammid c_1 ja c_2
- Meid huvitab $(m_1 + m_2)$ või (m_1/m_2)
- Selline uudishimu viib klassikalise krüptograafia korral paratamatu m_1 ja m_2 avaldamiseni tehete sooritajatele
- Täishomomorfne krüpteerimine lubab meil aga teostada tehted krüptogrammidega c_1 ja $c_2$ning saadud krüptogramme c_3 ja c_4 dekrüpteerides saada kätte $(m_1 + m_2)$ või (m_1/m_2)

Täishomomorfne krüptograafia
FHE – Fully Homomorphic Encryption

- Võtmed
  (pk, sk)
- Krüpteerimine
  $K(pk, m) = c$
- Dekrüpteerimine
  $D(sk, c) = m$



Kuidas kaks eelmist juttu seotud on?

- Sissejuhatus juba küll reetis, kuid täishomomorfne krüptograafia õnnestus esmalt ja on seni õnnestunud kirjeldada ainult kasutades LWE’d.
- Lihtsustatult:
  - Osutub, et tehes meisterlikult tehteid võrepunktide ümber satuvad tulemused taas võrepunktide ümber

Miks see on huvitav?

- Uued krüptoalgoritmid on hädavajalikud, et tagada andmete kaitsmise võime ka tähendusliku võimekusega kvantarvutite tekkumise järgselt
- Võre probleemide omadused on osutunud viimase 30 aasta jooksul “kullasooneks”
- Täishomomorfne krüpteerimine:
  - võimaldab säilitada andmete konfidentsiaalsust “pikemalt” kui seni
  - see võimaldab keerulisi arvutusi usaldada “odavamatesse” keskkondadesse
  - on täna “maru aeglane”
- Maailm ja Eesti sealhulgas ootavad matemaatikuid, kes nende teemadega soovivad ja oskavad tegeleda!

Vastuseid?

Aitüma!