FFI Forsvarets forskningsinstitutt

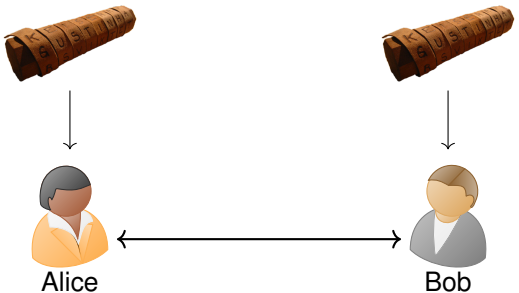
(Kvantesikker) kryptografi

Martin Strand

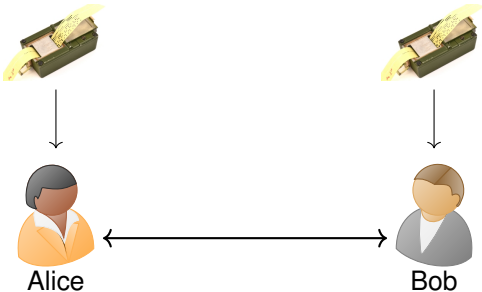
3. august 2023

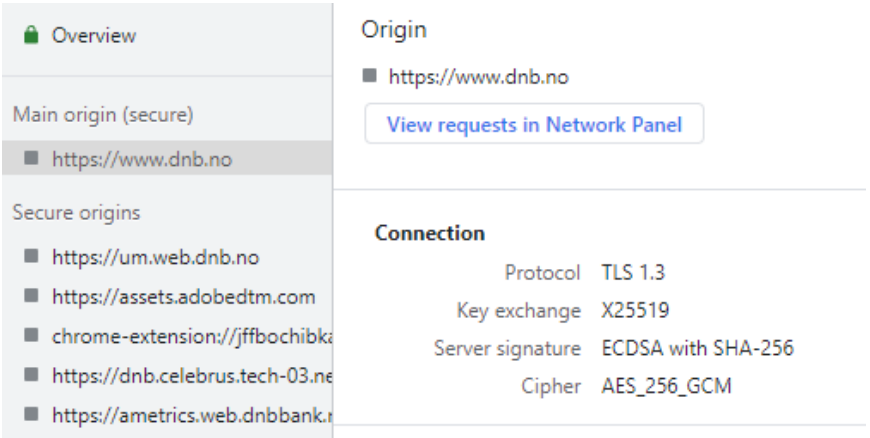
Foto: AdobeStock

Krypto er enkelt (Hellas, år 700 fvt.)



Krypto er enkelt (Hellas, år 700 fvt.)




Overview
Main origin (secure)
https://www.dnb.no
Secure origins
https://um.web.dnb.no
https://assets.adobedtm.com
chrome-extension://jffbochibk
https://dnb.celebrus.tech-03.ne
https://ametrics.web.dnbbank.
Origin
https://www.dnb.no
View requests in Network Panel
Connection
Protocol TLS 1.3
Key exchange X25519
Server signature ECDSA with SHA-256
Cipher AES_256_GCM

Hvem her kan klokka?

- Klokka er 11. Hva er den om 26 timer?

Hvem her kan klokka?

- Klokka er 11. Hva er den om 26 timer?

Eksempel

$$11 + 26 = 37 \equiv 1 \pmod{12}$$

fordi $37 - 1 = 3 \cdot 12$

Eksempel

La $n = 17$.

- $10 + 12 \equiv \pmod{17}$
- $4 \cdot 5 \equiv \pmod{17}$
- $3^3 = 27 \equiv \pmod{17}$

(Denne typen regning fungerer veldig godt når n er et primtall.)

Eksempel

La $n = 17$.

- $10 + 12 \equiv 5 \pmod{17}$
- $4 \cdot 5 \equiv \pmod{17}$
- $3^3 = 27 \equiv \pmod{17}$

(Denne typen regning fungerer veldig godt når n er et primtall.)

Eksempel

La $n = 17$.

- $10 + 12 \equiv 5 \pmod{17}$
- $4 \cdot 5 \equiv 3 \pmod{17}$
- $3^3 = 27 \equiv \pmod{17}$

(Denne typen regning fungerer veldig godt når n er et primtall.)

Eksempel

La $n = 17$.

- $10 + 12 \equiv 5 \pmod{17}$
- $4 \cdot 5 \equiv 3 \pmod{17}$
- $3^3 = 27 \equiv 10 \pmod{17}$

(Denne typen regning fungerer veldig godt når n er et primtall.)

Hele tabellen

$3^0 \equiv 1$
$3^1 \equiv 3$
$3^2 \equiv 9$
$3^3 \equiv 10$
$3^4 \equiv 13$
$3^5 \equiv 5$
$3^6 \equiv 15$
$3^7 \equiv 11$
$3^8 \equiv 16$
$3^9 \equiv 14$
$3^{10} \equiv 8$
$3^{11} \equiv 7$
$3^{12} \equiv 4$
$3^{13} \equiv 12$
$3^{14} \equiv 2$
$3^{15} \equiv 6$
$3^{16} \equiv 1$
$3^{17} \equiv 3$

Hvordan bli enige om en hemmelighet

Martin		du
Tilfeldig $0 < a < 17$		
Sett $A \equiv 3^a \pmod{17}$	$A \longrightarrow$	Tilfeldig $0 < b < 17$
	$\longleftarrow B$	Sett $B \equiv 3^b \pmod{17}$
Sett $C_1 \equiv B^a \pmod{17}$		Sett $C_2 \equiv A^b \pmod{17}$

Hvordan bli enige om en hemmelighet

Martin		du
Tilfeldig $0 < a < 17$		
Sett $A \equiv 3^a \pmod{17}$	$A \longrightarrow$	
	$\longleftarrow B$	Tilfeldig $0 < b < 17$
		Sett $B \equiv 3^b \pmod{17}$
Sett $C_1 \equiv B^a \pmod{17}$		Sett $C_2 \equiv A^b \pmod{17}$

Påstand

Vi har $C_1 = C_2$ og ingen andre vet C med mindre de er latterlig gode til å regne.

Hvorfor virker det?

$$
\begin{aligned}
C_1 &= B^a = \left(3^b\right)^a \\
&= 3^{ba} = 3^{ab} \\
&= \left(3^a\right)^b = A^b \\
&= C_2
\end{aligned}
$$

La oss prøve!

http://dh.strandet.no

La oss prøve!

Martin		du
Tilfeldig $0 < a < 17$		
Sett $A \equiv 3^a \pmod{17}$	$A \rightarrow$	
	$\leftarrow B$	Tilfeldig $0 < b < 17$
		Sett $B \equiv 3^b \pmod{17}$
Sett $C_1 \equiv B^a \pmod{17}$		Sett $C_2 \equiv A^b \pmod{17}$

$3^0 \equiv 1$
$3^1 \equiv 3$
$3^2 \equiv 9$
$3^3 \equiv 10$
$3^4 \equiv 13$
$3^5 \equiv 5$

$3^6 \equiv 15$
$3^7 \equiv 11$
$3^8 \equiv 16$
$3^9 \equiv 14$
$3^{10} \equiv 8$
$3^{11} \equiv 7$

$3^{12} \equiv 4$
$3^{13} \equiv 12$
$3^{14} \equiv 2$
$3^{15} \equiv 6$
$3^{16} \equiv 1$
$3^{17} \equiv 3$

Hvor stor må p være?

Noen forutsetninger

Problemet

$h = g^a \pmod{p}$, finn a.

Antagelser

- 2^{40} operasjoner i sekundet (Intel Core i9-13900KS: 2^{37})
- Omtrent en slik per menneske, si 10 000 000 000 stk
- 31 536 000 sekunder i et år
- Totalt, 2^{98} operasjoner i året

Noen forutsetninger

Problemet

$h = g^a \pmod{p}$, finn a.

Antagelser

- 2^{40} operasjoner i sekundet (Intel Core i9-13900KS: 2^{37})
- Omtrent en slik per menneske, si 10 000 000 000 stk
- 31 536 000 sekunder i et år
- Totalt, 2^{98} operasjoner i året
- (Bitcoin: 2^{92} operasjoner i året, $1/64$-del av dette)

Angrep: Brute force

Sett $p \approx 2^{128}$.

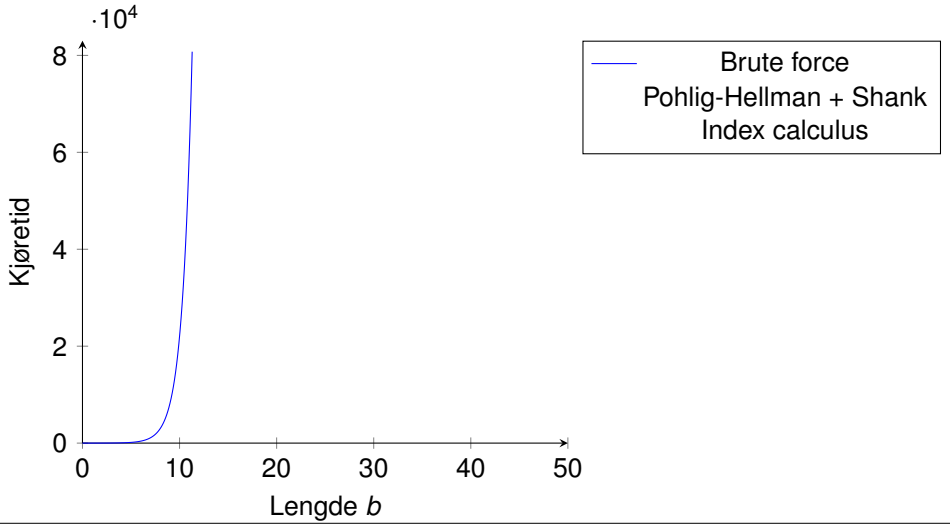
Angrep: Brute force

Sett $p \approx 2^{128}$. Da tar det $2^{128}/2^{98} \approx 1\,000\,000\,000$ år å finne a.

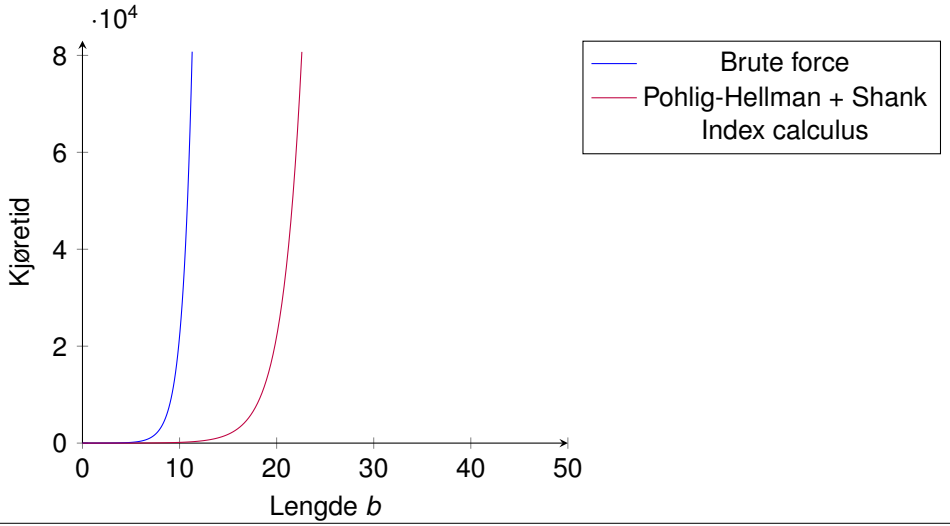
Formell kjøretid

$\mathcal{O}(p)$

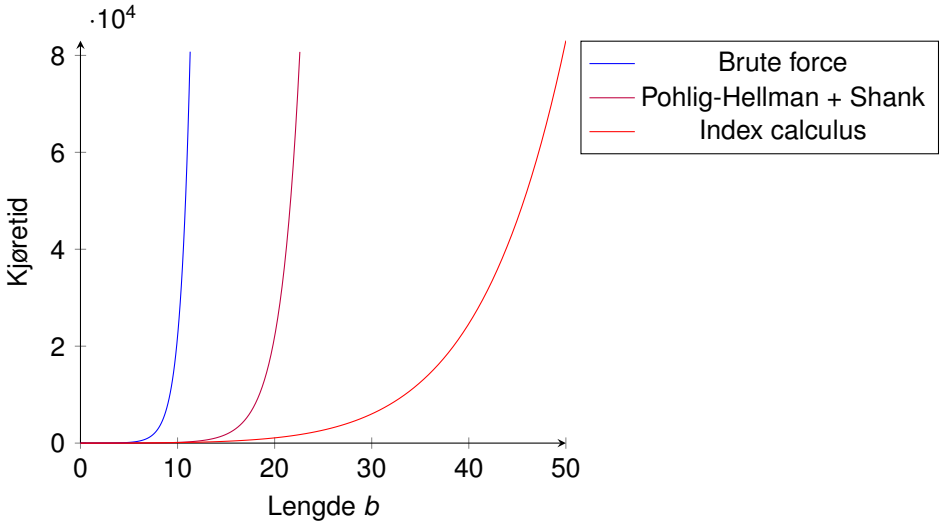
Litt lurere algoritmer



Litt lurere algoritmer



Litt lurere algoritmer



Antall atomer i universet

100 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000 000

Antall unike sjakkspill

```
1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
  000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
  000 000 000 000 000 000 000 000
```

Et egnet primtall for Diffie-Hellman

```
17 371 633 710 861 526 985 402 756 155 605 996 322 196 257 048 455
   675 141 997 211 607 897 588 436 880 112 664 345 732 402 516 434
   975 116 670 023 472 796 825 233 643 612 395 266 186 808 119 984
   996 372 379 602 426 678 900 493 286 192 039 475 551 678 848 776
   585 415 169 949 664 415 820 483 514 690 301 509 982 058 398 659
   940 050 744 425 005 234 342 360 377 140 221 362 953 519 273 046
   483 446 364 930 471 865 451 176 965 825 059 235 201 349 014 188
   384 323 322 347 988 836 585 004 216 878 741 293 400 993 565 478
   114 200 002 489 905 246 623 078 674 988 568 740 682 222 428 856
   692 842 421 774 076 905 917 061 448 967 466 083 362 856 797 534
   215 180 379 822 041 036 186 832 388 654 983 120 685 889 564 412
   266 789 511 781 064 026 694 452 185 724 178 282 543 463 162 021
   793 730 933 403 449 281 865 751 197 897 543 205 563
```

Kan vi bruke et mindre tall?

Kan vi bruke et mindre tall?

ECDHE

Kan vi bruke et mindre tall?

EC DHE
Elliptic curves

Curve25519

```
57 896 044 618 658 097 711 785 492 504 343 953 926 634 992 332 820
   282 019 728 792 003 956 564 819 949
```

$$|\psi\rangle := \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}; \quad |\alpha|^2 + |\beta|^2 = 1$$

Shors algoritme

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Idé

Gitt $N = pq$, finn p, q

1. Velg $1 < a < N$ slik at $\gcd(a, N) = 1$
2. Finn* minste $r > 0$ slik at $a^r \equiv 1 \pmod{N}$
3. Hvis r er et oddetall, start på nytt
4. Hvis $a^{r/2} \equiv -1 \pmod{N}$, start på nytt
5. La $d = \gcd(a^{r/2} - 1, N)$

Kan vise: d en ikke-triviell faktor av N.

Idé

Gitt $N = pq$, finn p, q

1. Velg $1 < a < N$ slik at $\gcd(a, N) = 1$
2. Finn* minste $r > 0$ slik at $a^r \equiv 1 \pmod{N}$
3. Hvis r er et oddetall, start på nytt
4. Hvis $a^{r/2} \equiv -1 \pmod{N}$, start på nytt
5. La $d = \gcd(a^{r/2} - 1, N)$

Kan vise: d en ikke-triviell faktor av N.

Hvorfor?

$a^r - 1 = \ell N$, så $N \mid (a^r - 1)$, og $a^r - 1 = \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right)$.
$a^{r/2} \not\equiv 1, -1 \pmod{N}$ fordi r er minimal og pkt. 4, så $a^{r/2} \pm 1$ deler ikke-triviell faktor med N.

Kvantebidraget

La $Q = 2^q$.

Kvantebidraget

La $Q = 2^q$.

Klassisk Fourier-transformasjon

$$(x_0, x_1, \ldots, x_Q) \mapsto (y_0, y_1, \ldots, y_{Q-1}) \in \mathbb{C}^Q$$

$$y_k = \frac{1}{\sqrt{Q}} \sum_{n=0}^{Q-1} x_n \omega_Q^{-kn}$$

Kompleksitet: $\mathcal{O}(Q \log Q) = \mathcal{O}(2^q \cdot q)$

Kvantebidraget

La $Q = 2^q$.

Klassisk Fourier-transformasjon

$$(x_0, x_1, \ldots, x_Q) \mapsto (y_0, y_1, \ldots, y_{Q-1}) \in \mathbb{C}^Q$$

$$y_k = \frac{1}{\sqrt{Q}} \sum_{n=0}^{Q-1} x_n \omega_Q^{-kn}$$

Kompleksitet: $\mathcal{O}(Q \log Q) = \mathcal{O}(2^q \cdot q)$

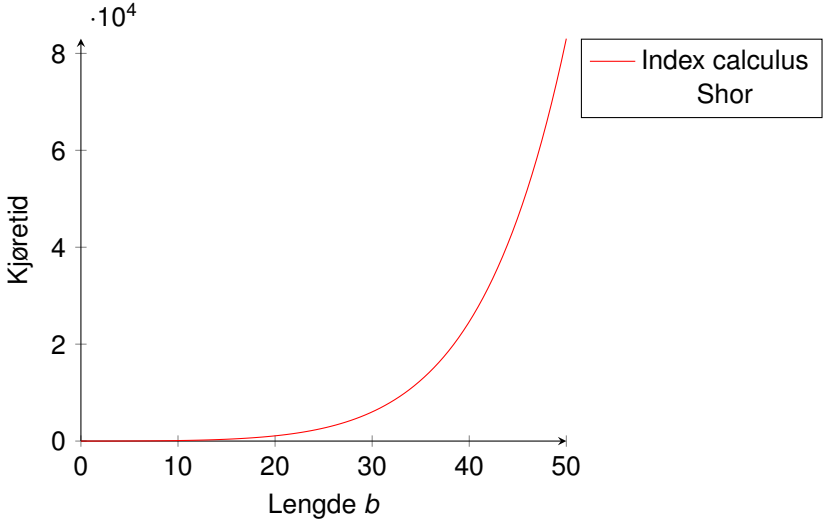
Kvante-Fourier-transformasjon

$$|x\rangle = \sum_{i=0}^{Q-1} x_i |i\rangle \mapsto \sum_{i=0}^{Q-1} y_i |i\rangle$$

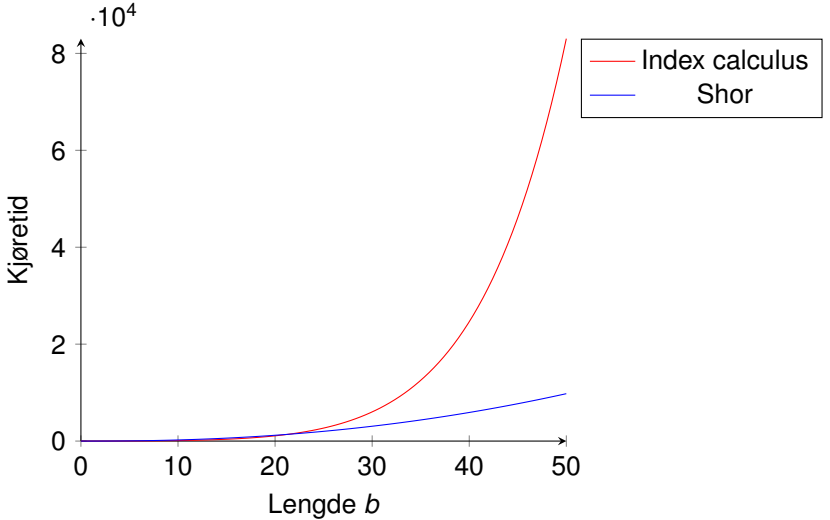
$$y_k = \frac{1}{\sqrt{Q}} \sum_{n=0}^{Q-1} x_n \omega_Q^{nk}$$

Kompleksitet: $\mathcal{O}(q \log q)$

Shors algoritme vs. dlog og faktorisering



Shors algoritme vs. dlog og faktorisering



Konsekvens for kryptosystemer

Transition Algorithms

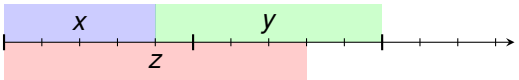
Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

Konsekvens for kryptosystemer

Transition Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
~~Elliptic Curve Diffie-Hellman (ECDH) Key Exchange~~	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
~~Elliptic Curve Digital Signature Algorithm (ECDSA)~~	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
~~Diffie-Hellman (DH) Key Exchange~~	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
~~RSA~~	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
~~RSA~~	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

Kvantedatamaskinene kommer (?)



Theorem (Mosca)

Hvis $x + y > z$, vær bekymret.

Et nytt håp

Gitter

La $\mathbb{R}^n \cong V = \text{span}\left\{\vec{b}_1, \ldots \vec{b}_n\right\}$ være et reelt vektorrom.
Da er

$$L = \left\{ \sum_{i=1}^{n} a_i \vec{b}_i \mid a_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

gitteret generert av $\left\{\vec{b}_1, \ldots \vec{b}_n\right\}$.

Gitter

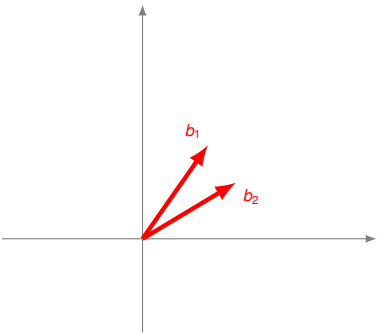
La $\mathbb{R}^n \cong V = \text{span}\left\{\vec{b}_1, \ldots \vec{b}_n\right\}$ være et reelt vektorrom.
Da er

$$L = \left\{ \sum_{i=1}^{n} a_i \vec{b}_i \mid a_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

gitteret generert av $\left\{\vec{b}_1, \ldots \vec{b}_n\right\}$.

Eksempel

Betrakt $\mathbb{R}^2 \cong \text{span}\{(2,3),(3,2)\}$



Gitter

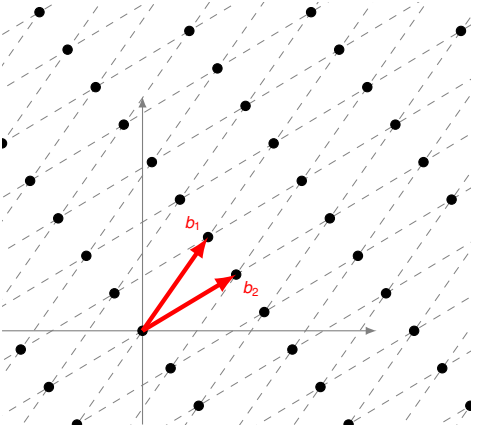
La $\mathbb{R}^n \cong V = \text{span}\left\{\vec{b}_1, \ldots \vec{b}_n\right\}$ være et reelt vektorrom.
Da er

$$L = \left\{ \sum_{i=1}^{n} a_i \vec{b}_i \mid a_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

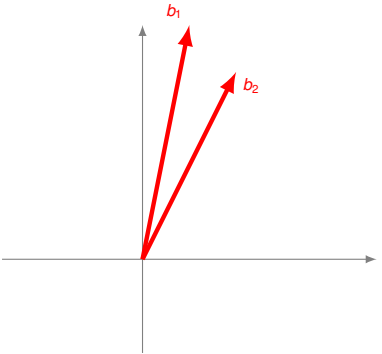
gitteret generert av $\left\{\vec{b}_1, \ldots \vec{b}_n\right\}$.

Eksempel

Betrakt $\mathbb{R}^2 \cong \text{span}\{(2,3),(3,2)\}$



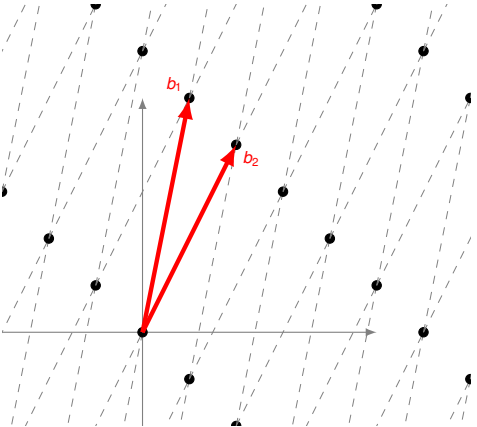
Gitterproblemer



Gitterproblemer

Shortest Vector Problem

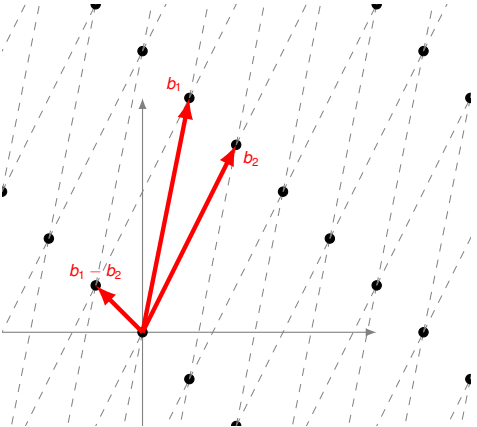
Gitt en basis for L, finn den korteste vektoren i V som også er et punkt i L.



Gitterproblemer

Shortest Vector Problem

Gitt en basis for L, finn den korteste vektoren i V som også er et punkt i L.



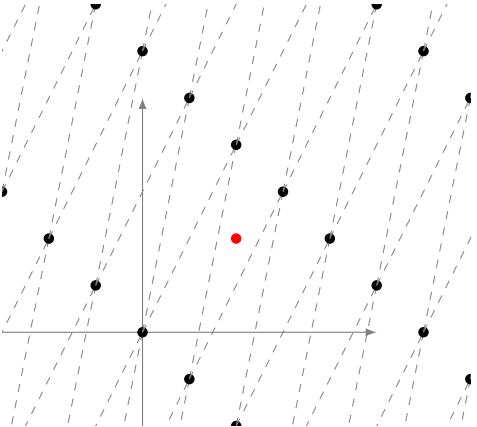
Gitterproblemer

Shortest Vector Problem

Gitt en basis for L, finn den korteste vektoren i V som også er et punkt i L.

Closest Vector Problem

Gitt en basis for L og et punkt v i V, finn nærmeste gitterpunkt til v i L.



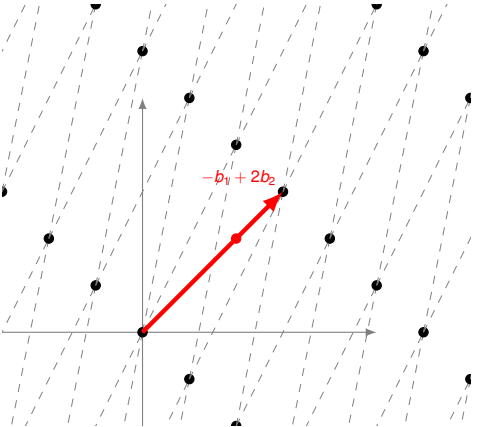
Gitterproblemer

Shortest Vector Problem

Gitt en basis for L, finn den korteste vektoren i V som også er et punkt i L.

Closest Vector Problem

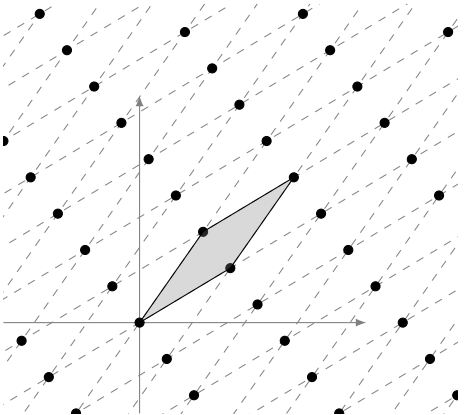
Gitt en basis for L og et punkt v i V, finn nærmeste gitterpunkt til v i L.



Learning with errors

$$
\begin{aligned}
a_{1,1}x_1 + \ldots a_{1,n}x_n + e_1 &= b_1 \\
a_{2,1}x_1 + \ldots a_{2,n}x_n + e_2 &= b_2 \\
a_{3,1}x_1 + \ldots a_{3,n}x_n + e_3 &= b_3 \\
a_{4,1}x_1 + \ldots a_{4,n}x_n + e_4 &= b_4 \\
a_{5,1}x_1 + \ldots a_{5,n}x_n + e_5 &= b_5 \\
&\vdots
\end{aligned}
$$

Gitt A, $\vec{b}$ og at alle e_i er små, hva er $\vec{x}$?



Referanser

Regev (2005); Lyubashevsky, Peikert, Regev (2010)

LWE-kryptering

Oppsett La q være et primtall og n et naturlig tall. Velg en vektor $\vec{s} \in \mathbb{Z}_q^n$ som privat nøkkel. Velg m vektorer $\vec{a}_1, \ldots \vec{a}_m \in \mathbb{Z}_q^n$, og feilvektorer $\vec{e}_1, \ldots, \vec{e}_m$ fra en diskret gaussisk fordeling.
Offentlig nøkkel:

$$(\mathbf{a}_i, b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle / q + e_i)_{i=1}^m$$

Kryptering Gitt meldingsbit x, en delmengde $S \subset \{1, \ldots, m\}$, beregn

$$\left(\sum_{i \in S} \mathbf{a}_i, \frac{x}{2} + \sum_{i \in S} b_i \right)$$

Dekryptering Gitt chiffertekst $(\vec{a}, b)$. Beregn $x' = b - \langle \mathbf{a}, \mathbf{s} \rangle / q$. Dekrypteringen er 0 hvis x' er nærmere 0 enn $\frac{1}{2}$, ellers 1.

Men vent, det blir verre ...

Algorithm 5 KYBER.CPAPKE.Enc(pk, m, r): encryption

Input: Public key $pk \in \mathcal{B}^{12 \cdot k \cdot n/8+32}$
Input: Message $m \in \mathcal{B}^{32}$
Input: Random coins $r \in \mathcal{B}^{32}$
Output: Ciphertext $c \in \mathcal{B}^{d_u \cdot k \cdot n/8+d_v \cdot n/8}$

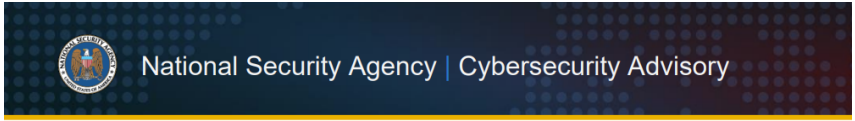
$N := 0$
$\hat{\mathbf{t}} := \mathsf{Decode}_{12}(pk)$
$\rho := pk + 12 \cdot k \cdot n/8$
for i from 0 to $k-1$ **do** ▷ Generate matrix $\hat{\mathbf{A}} \in R_q^{k \times k}$ in NTT domain
  for j from 0 to $k-1$ **do**
    $\hat{\mathbf{A}}^T[i][j] := \mathsf{Parse}(\mathsf{XOF}(\rho, i, j))$
  end for
end for
for i from 0 to $k-1$ **do** ▷ Sample $\mathbf{r} \in R_q^k$ from B_{η_1}
  $\mathbf{r}[i] := \mathsf{CBD}_{\eta_1}(\mathsf{PRF}(r, N))$
  $N := N + 1$
end for
for i from 0 to $k-1$ **do** ▷ Sample $\mathbf{e}_1 \in R_q^k$ from B_{η_2}
  $\mathbf{e}_1[i] := \mathsf{CBD}_{\eta_2}(\mathsf{PRF}(r, N))$
  $N := N + 1$
end for
$e_2 := \mathsf{CBD}_{\eta_2}(\mathsf{PRF}(r, N))$ ▷ Sample $e_2 \in R_q$ from B_{η_2}
$\hat{\mathbf{r}} := \mathsf{NTT}(\mathbf{r})$
$\mathbf{u} := \mathsf{NTT}^{-1}(\hat{\mathbf{A}}^T \circ \hat{\mathbf{r}}) + \mathbf{e}_1$ ▷ $\mathbf{u} := \mathbf{A}^T\mathbf{r} + \mathbf{e}_1$
$v := \mathsf{NTT}^{-1}(\hat{\mathbf{t}}^T \circ \hat{\mathbf{r}}) + e_2 + \mathsf{Decompress}_q(\mathsf{Decode}_1(m), 1)$ ▷ $v := \mathbf{t}^T\mathbf{r} + e_2 + \mathsf{Decompress}_q(m, 1)$
$c_1 := \mathsf{Encode}_{d_u}(\mathsf{Compress}_q(\mathbf{u}, d_u))$
$c_2 := \mathsf{Encode}_{d_v}(\mathsf{Compress}_q(v, d_v))$
return $c = (c_1 \| c_2)$ ▷ $c := (\mathsf{Compress}_q(\mathbf{u}, d_u), \mathsf{Compress}_q(v, d_v))$

Nøkkeltall

	Offentlig nøkkel	Privat nøkkel	Chiffertekst
ECDH	97 B	48 B	
Kyber	1568 B	3168 B	1568 B

	Verifiseringsnøkkel	Signeringsnøkkel	Signatur
ECDSA	48 B	48 B	96 B
Dilithium	2592 B	4864 B	4595 B

CNSA 2.0-annonsering



Announcing the Commercial National Security Algorithm Suite 2.0

Table III: CNSA 2.0 quantum-resistant public-key algorithms

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.