Introduction to Lattice Based Cryptography

Eduardo Morais
advisor: Ricardo Dahab

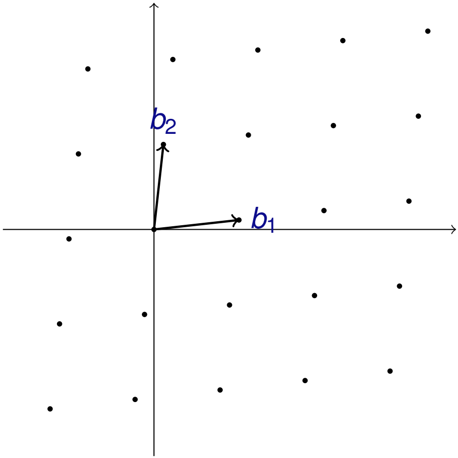
Unicamp

ASCrypto 2013
October 18, 2013

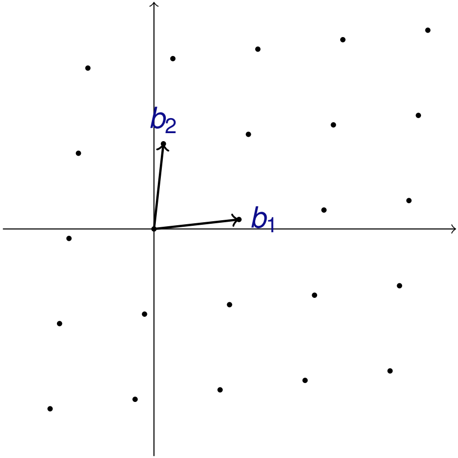
Agenda

- Introduction
  - Definitions
  - Dual Lattices
  - q-ary Lattices
  - Hard Problems
- Schemes
  - Goldreich, Goldwasser and Halevi (GGH)
  - Ajtai's construction
  - Learning With Errors (LWE), Ring LWE, NTRU-like
  - Functional Encryption, Identity Based Encryption, Attribute Based Encryption, Fully Homomorphic Encryption

Lattices



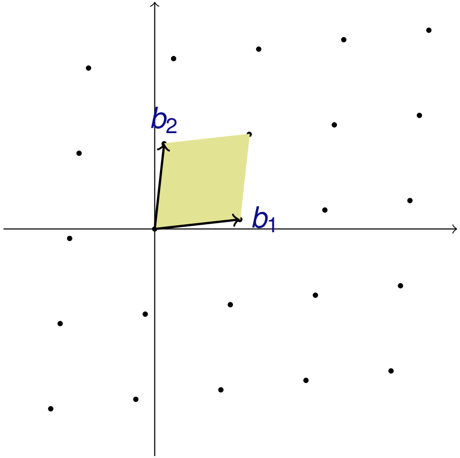
Lattices



$$\mathcal{L}(b_1, b_2) =$$

$$\{\sum x_i b_i : x_i \in \mathbb{Z}\}$$

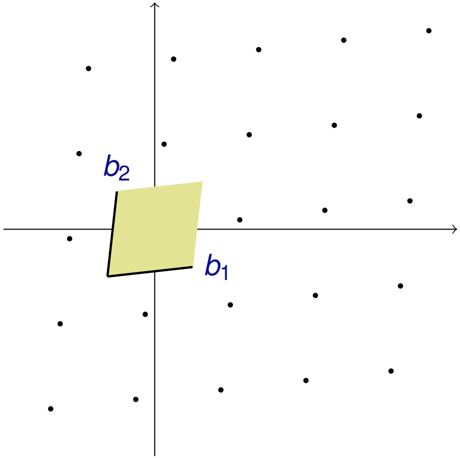
Lattices



Fundamental Domain

$$\{\sum t_i b_i, 0 \leq t_i < 1\}$$

Lattices

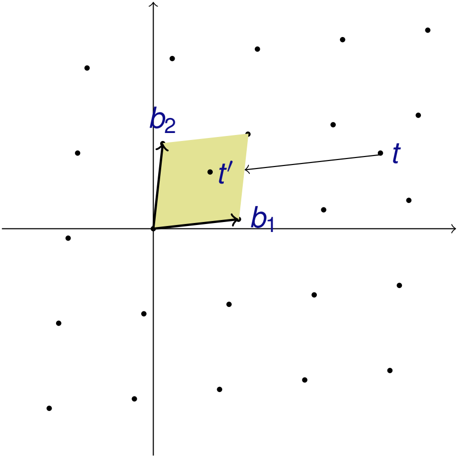


Centered

Fundamental Domain

$$\{\sum t_i b_i, \frac{-1}{2} \le t_i < \frac{1}{2}\}$$

Lattices

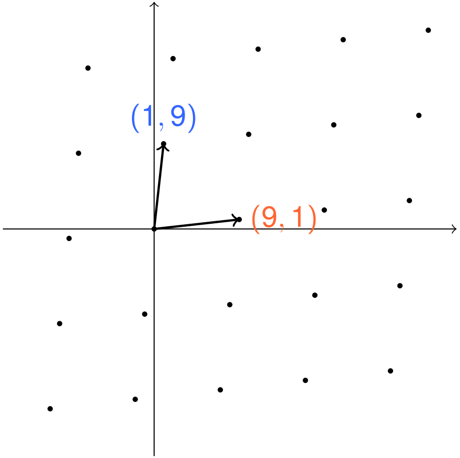


Reduction:

$$t' \equiv t \pmod{\mathcal{L}_B}$$

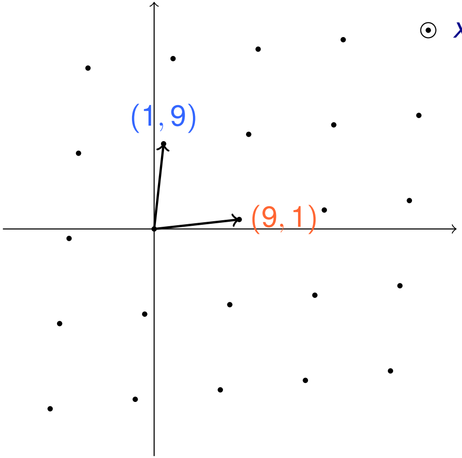
Lattices

$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$



Lattices

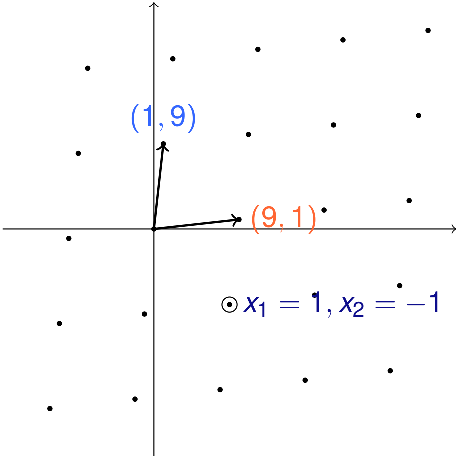
$$\mathcal{L}: \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$



- $x_1 = 3, x_2 = 2$

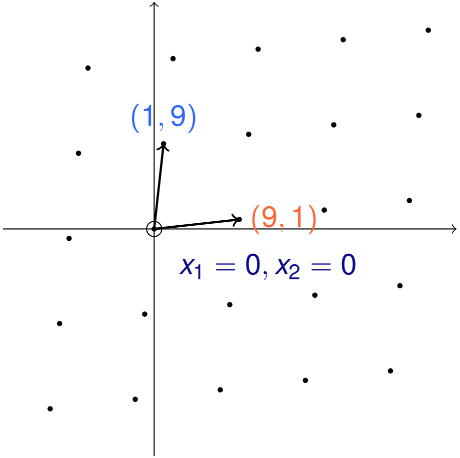
Lattices

$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$



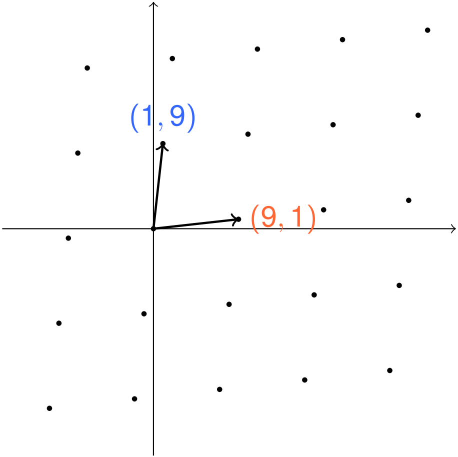
Lattices

$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$



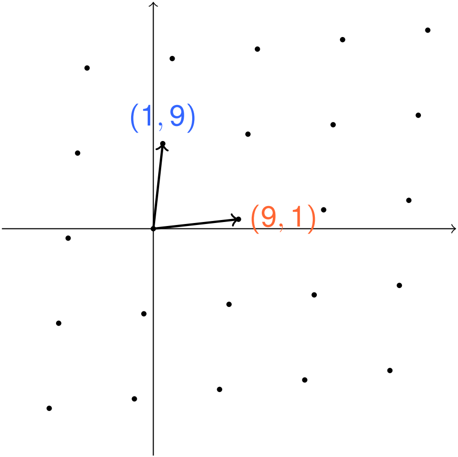
Lattices

$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$



$$\begin{bmatrix} b_{1,1} & \dots & b_{n,1} \\ \vdots & \ddots & \vdots \\ b_{1,n} & \dots & b_{n,n} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Lattices

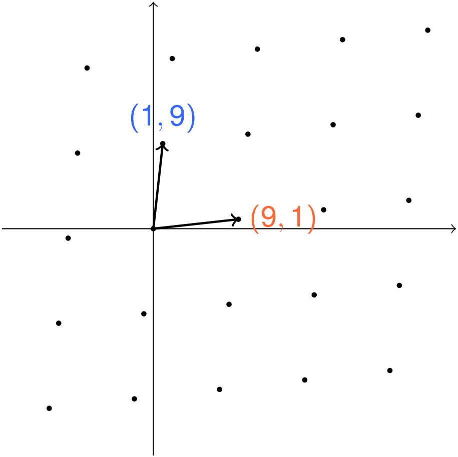


$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$Bx$$

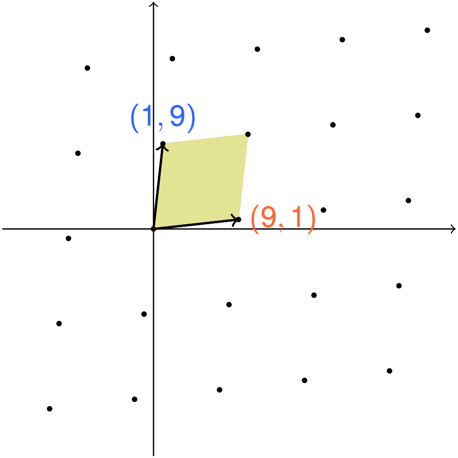
Lattices

$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$



Volume of the Domain?

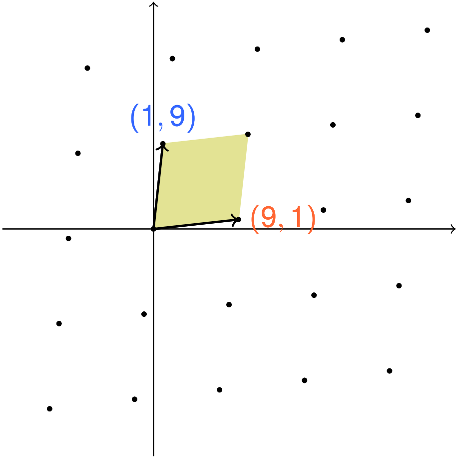
Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge:

Lattices

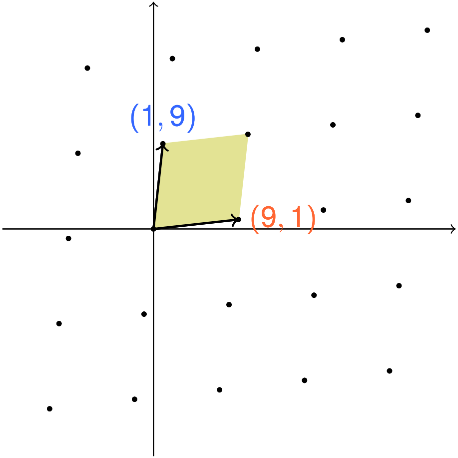


$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

$$\mathcal{A} = D.d/2$$

Lattices



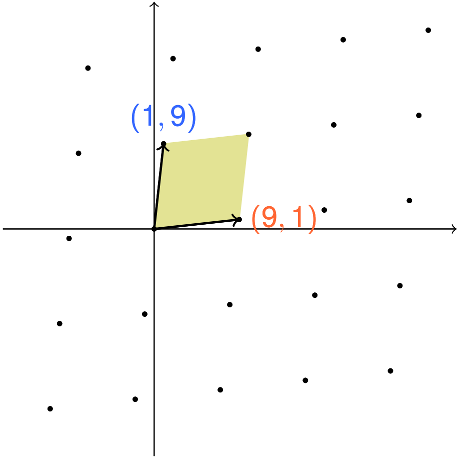
$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

$$\mathcal{A} = D.d/2$$

$$d = |(9,1) - (1,9)|$$

Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

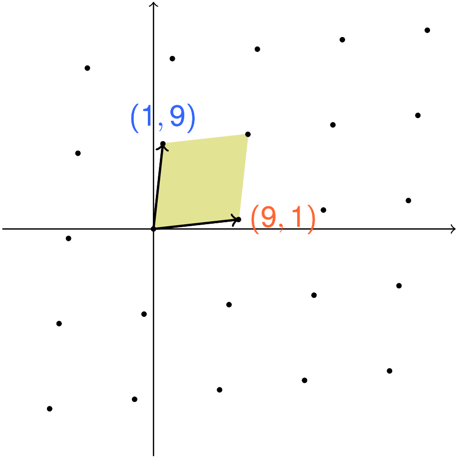
Area of lozenge

$$\mathcal{A} = D.d/2$$

$$d = |(9,1) - (1,9)|$$

$$d = \sqrt{8^2 + (-8)^2}$$

Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

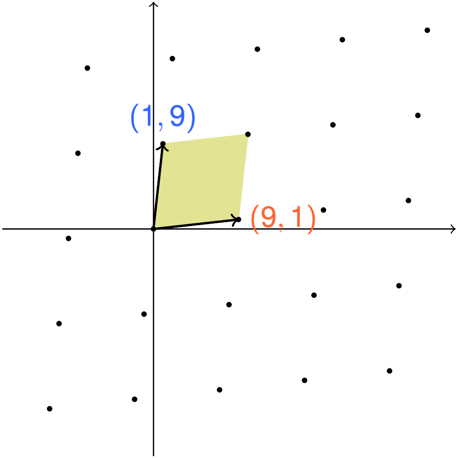
$$\mathcal{A} = D.d/2$$

$$d = |(9,1) - (1,9)|$$

$$d = \sqrt{8^2 + (-8)^2}$$

$$\boxed{d = 8\sqrt{2}}$$

Lattices



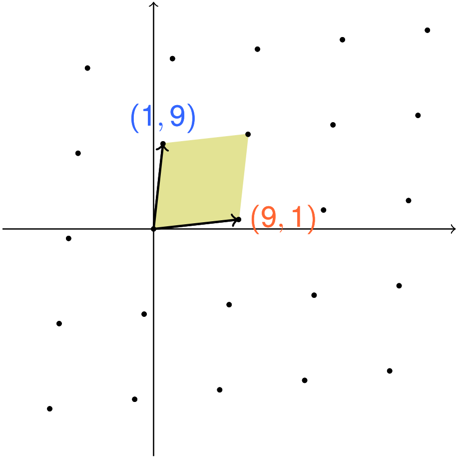
$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

$$\mathcal{A} = D.d/2$$

$$D = |(9,1) + (1,9)|$$

Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

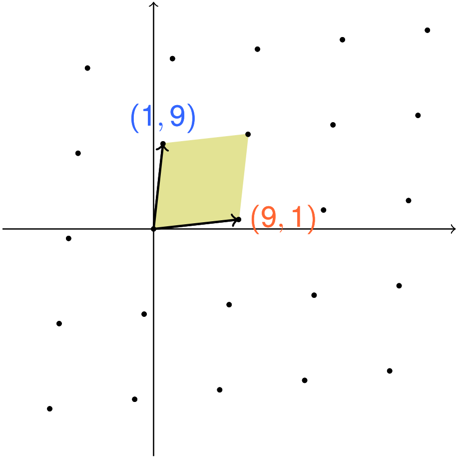
Area of lozenge

$$\mathcal{A} = D.d/2$$

$$D = |(9,1) + (1,9)|$$

$$D = \sqrt{10^2 + (-10)^2}$$

Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

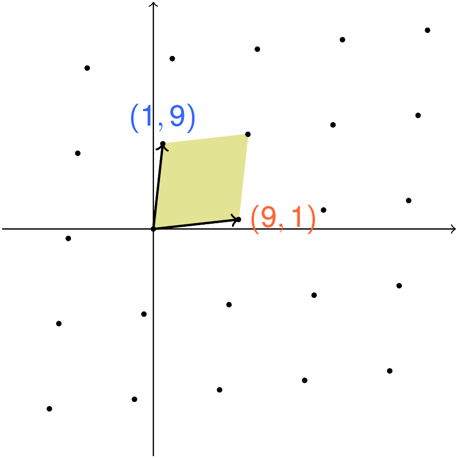
$$\mathcal{A} = D.d/2$$

$$D = |(9,1) + (1,9)|$$

$$D = \sqrt{10^2 + (-10)^2}$$

$$D = 10\sqrt{2}$$

Lattices



$$\mathcal{L}: \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

$$\mathcal{A} = D.d/2$$

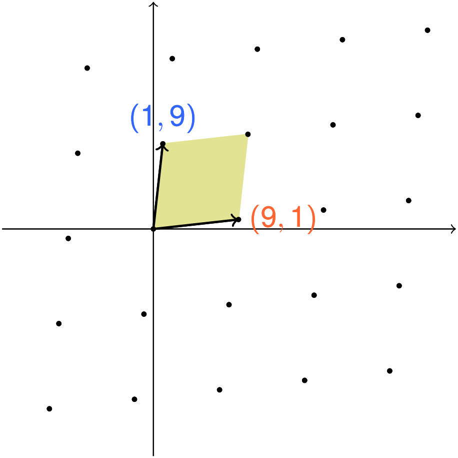
$$D = |(9,1) + (1,9)|$$

$$D = \sqrt{10^2 + (-10)^2}$$

$$D = 10\sqrt{2}$$

$$\mathcal{A} = (10\sqrt{2})(8\sqrt{2})/2$$

Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Area of lozenge

$$\mathcal{A} = D.d/2$$

$$D = |(9,1) + (1,9)|$$

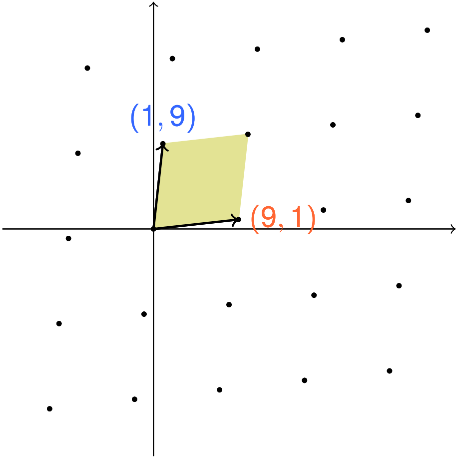
$$D = \sqrt{10^2 + (-10)^2}$$

$$D = 10\sqrt{2}$$

$$\mathcal{A} = (10\sqrt{2})(8\sqrt{2})/2$$

$$\boxed{\mathcal{A} = 10.8 = 80}$$

Lattices



$$\mathcal{L} : \begin{bmatrix} 9 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$\det B = 9.9 - 1.1$$

$$\det B = 81 - 1$$

$$\det B = 80$$

$$\boxed{\text{Volume: } \det B}$$

Orthogonality

$||b_i|| \approx 9.05$

$\mathcal{A} = 80$

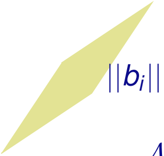
$\mathcal{A}/||b_i||^2 = 0.97$

$||b_i|| \approx 9.05$

$\mathcal{A} = 81.9$

$\mathcal{A}/||b_i||^2 = 1$

Orthogonality



$||b_i|| \approx 21.47$

$\mathcal{A} = 80$

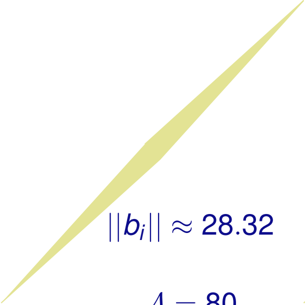
$\mathcal{A}/||b_i||^2 = 0.17$

$||b_i|| \approx 9.05$

$\mathcal{A} = 20.46$

$\mathcal{A}/||b_i||^2 = 0.125$

Orthogonality



$$||b_i|| \approx 28.32$$

$$\mathcal{A} = 80$$

$$\mathcal{A}/||b_i||^2 = 0.10$$

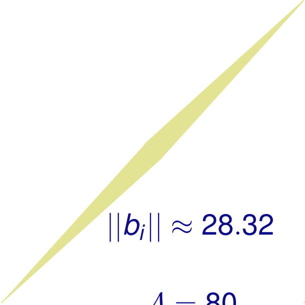
$$||b_i|| \approx 9.05$$

$$\mathcal{A} = 11.52$$

$$\mathcal{A}/||b_i||^2 = 0.14$$

Orthogonality

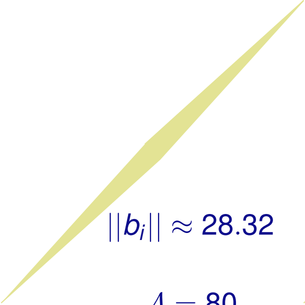
$$\boxed{\frac{\det \mathcal{L}}{\prod_{1 \le i \le n} ||b_i||}}$$



$\|\|b_i\|\| \approx 28.32$	$\|\|b_i\|\| \approx 9.05$
$\mathcal{A} = 80$	$\mathcal{A} = 11.52$
$\mathcal{A}/\|\|b_i\|\|^2 = 0.10$	$\mathcal{A}/\|\|b_i\|\|^2 = 0.14$

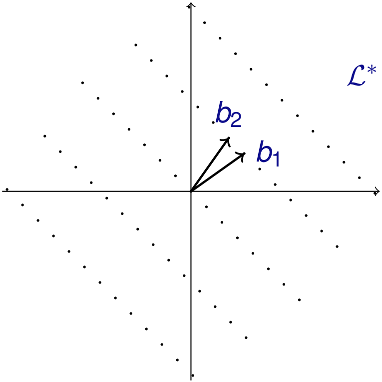
Orthogonality

$$\boxed{\left(\frac{\det \mathcal{L}}{\prod_{1\le i\le n} ||b_i||}\right)^{1/n}}$$ Hadamard Ratio



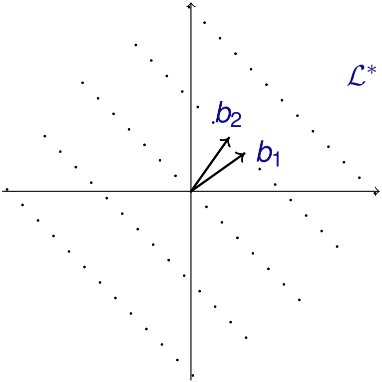
$\|\|b_i\|\| \approx 28.32$	$\|\|b_i\|\| \approx 9.05$
$\mathcal{A} = 80$	$\mathcal{A} = 11.52$
$\mathcal{A}/\|\|b_i\|\|^2 = 0.10$	$\mathcal{A}/\|\|b_i\|\|^2 = 0.14$

Dual Lattices



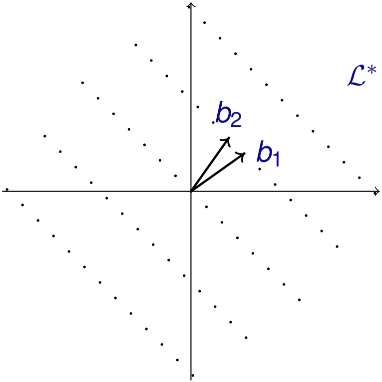
$$\mathcal{L}^* = \{y \mid \langle x, y \rangle \in \mathbb{Z}, \forall x \in \mathcal{L}\}$$

Dual Lattices



$$\mathcal{L}^* = \{y \mid \langle x, y\rangle \in \mathbb{Z}, \forall x \in \mathcal{L}\}$$
$$\langle b_1^*, b_1\rangle = 0$$
$$\langle b_1^*, b_2\rangle = 1$$

Dual Lattices



$$\mathcal{L}^* = \{y \mid \langle x, y\rangle \in \mathbb{Z}, \forall x \in \mathcal{L}\}$$

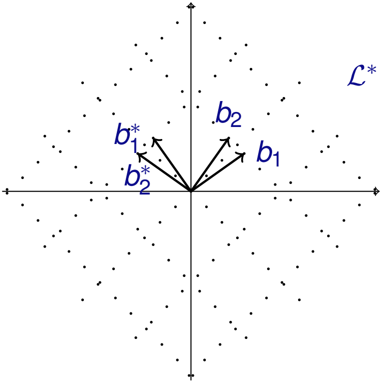
$$\langle b_1^*, b_1\rangle = 0$$

$$\langle b_1^*, b_2\rangle = 1$$

$$\langle b_2^*, b_2\rangle = 0$$

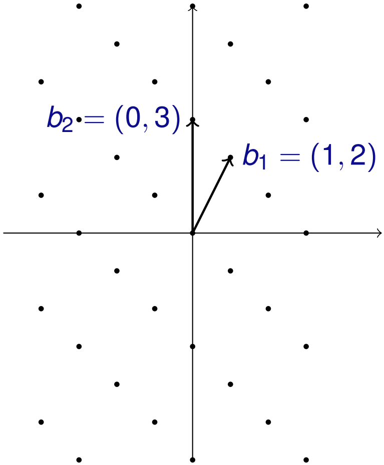
$$\langle b_2^*, b_1\rangle = 1$$

Dual Lattices

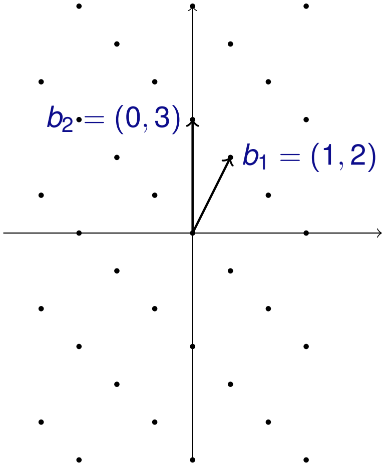


$$\mathcal{L}^* = \{y \mid \langle x, y\rangle \in \mathbb{Z}, \forall x \in \mathcal{L}\}$$
$$\langle b_1^*, b_1\rangle = 0$$
$$\langle b_1^*, b_2\rangle = 1$$
$$\langle b_2^*, b_2\rangle = 0$$
$$\langle b_2^*, b_1\rangle = 1$$

Dual Lattices



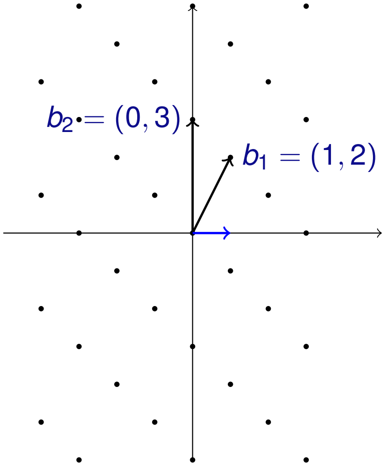
Dual Lattices



$$\langle (x_1, y_1), (0,3) \rangle = 0$$

$$\langle (x_1, y_1), (1,2) \rangle = 1$$

Dual Lattices

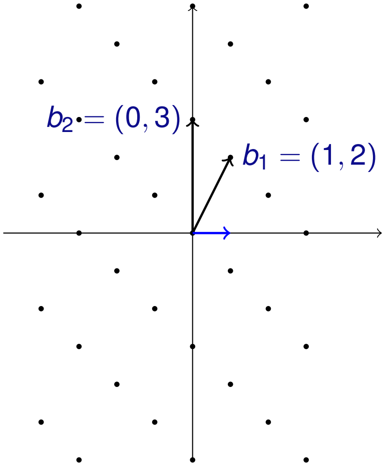


$$\langle (x_1, y_1), (0,3) \rangle = 0$$

$$\langle (x_1, y_1), (1,2) \rangle = 1$$

$$\boxed{(x_1 = 1, y_1 = 0)}$$

Dual Lattices



$$\langle (x_1, y_1), (0,3) \rangle = 0$$

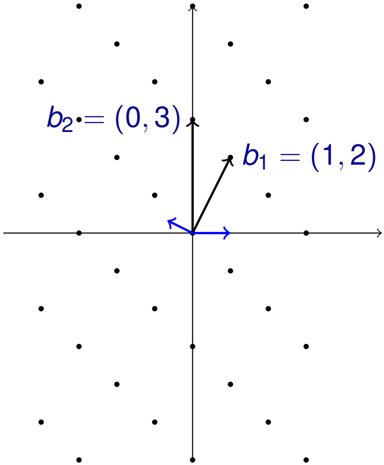
$$\langle (x_1, y_1), (1,2) \rangle = 1$$

$$\boxed{(x_1 = 1, y_1 = 0)}$$

$$\langle (x_2, y_2), (1,2) \rangle = 0$$

$$\langle (x_2, y_2), (0,3) \rangle = 1$$

Dual Lattices



$$\langle (x_1, y_1), (0,3) \rangle = 0$$

$$\langle (x_1, y_1), (1,2) \rangle = 1$$

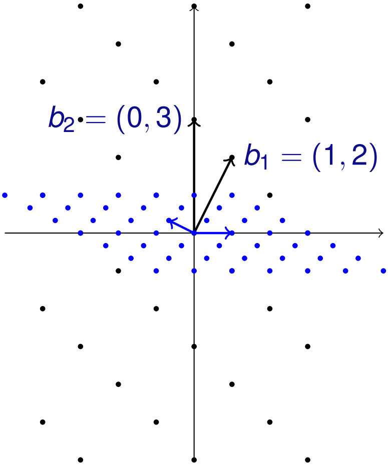
$$\boxed{(x_1 = 1, y_1 = 0)}$$

$$\langle (x_2, y_2), (1,2) \rangle = 0$$

$$\langle (x_2, y_2), (0,3) \rangle = 1$$

$$\boxed{(x_2 = -2/3, y_2 = 1/3)}$$

Dual Lattices



$$\langle (x_1, y_1), (0, 3) \rangle = 0$$

$$\langle (x_1, y_1), (1, 2) \rangle = 1$$

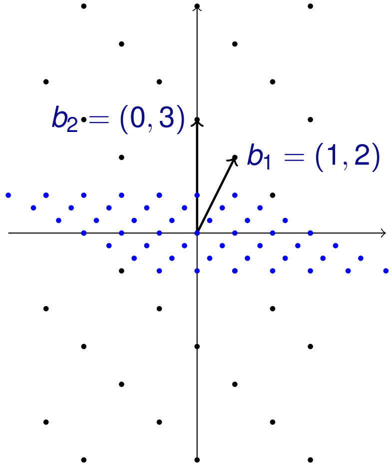
$$\boxed{(x_1 = 1, y_1 = 0)}$$

$$\langle (x_2, y_2), (1, 2) \rangle = 0$$

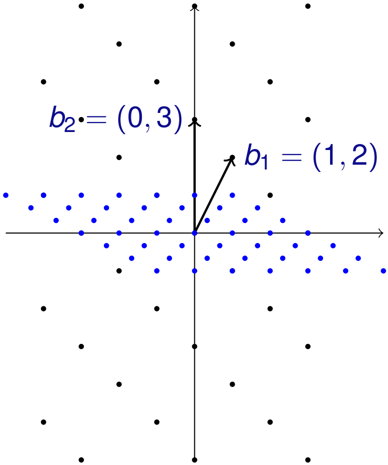
$$\langle (x_2, y_2), (0, 3) \rangle = 1$$

$$\boxed{(x_2 = -2/3, y_2 = 1/3)}$$

Dual Lattices



Dual Lattices

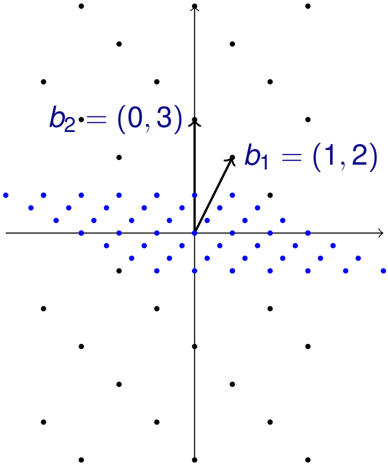


Volume:

$$\left|\begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix}\right| = -3$$

$$\left|\begin{bmatrix} 1 & -2/3 \\ 0 & 1/3 \end{bmatrix}\right| = 1/3$$

Dual Lattices



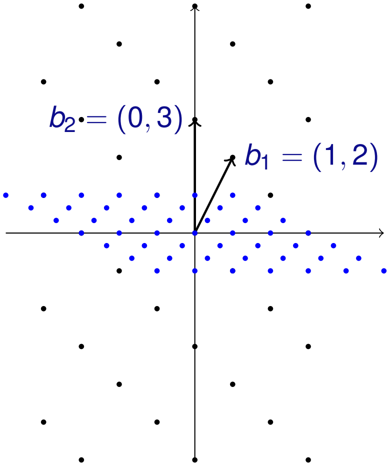
Volume:

$$\left| \begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix} \right| = -3$$

$$\left| \begin{bmatrix} 1 & -2/3 \\ 0 & 1/3 \end{bmatrix} \right| = 1/3$$

$$\mathcal{L}(B)^* = \mathcal{L}((B^{-1})^T)$$

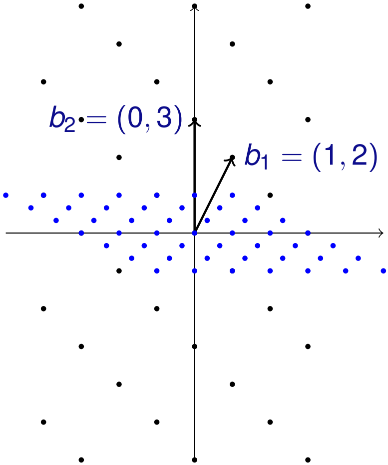
Dual Lattices



$$B^{-1} = 1/3 \begin{bmatrix} 2 & -1 \\ -3 & 0 \end{bmatrix}$$

$$(B^{-1})^T = \begin{bmatrix} -2/3 & 1 \\ 1/3 & 0 \end{bmatrix}$$

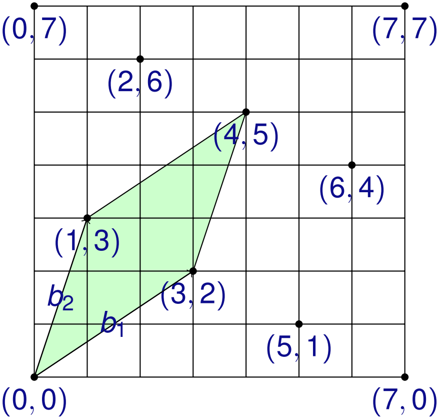
Dual Lattices



$$B^{-1} = 1/3 \begin{bmatrix} 2 & -1 \\ -3 & 0 \end{bmatrix}$$

$$(B^{-1})^T = \begin{bmatrix} 1 & -2/3 \\ 0 & 1/3 \end{bmatrix}$$

q-ary Lattices



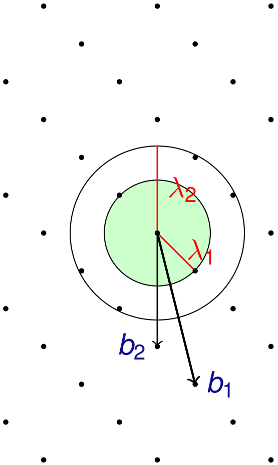
$$\Lambda_q(A) = \{y = As \pmod{q}\}$$

$$\Lambda_q^{\perp}(A) = \{y \mid Ay = 0 \pmod{q}\}$$

$$\Lambda_q^{\perp}(A) = q\Lambda_q(A)^*$$

$$\Lambda_q(A) = q\Lambda_q^{\perp}(A)^*$$

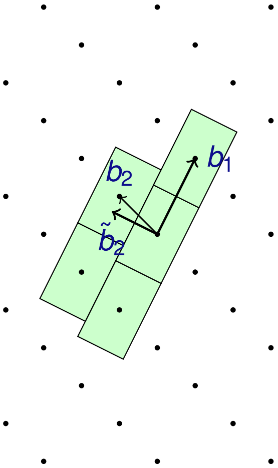
Successive Minima



λ_i: min r s.t.

$\mathcal{B}_r$ has i lin. ind. vectors

Gram-Schmidt Orthogonalization Process



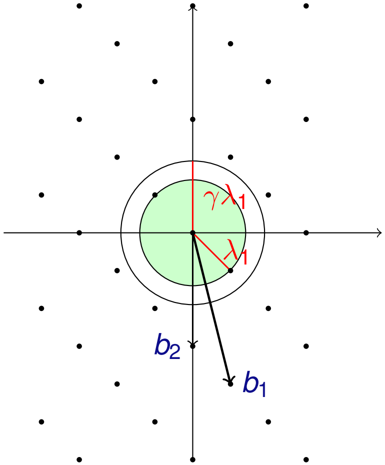
$$\tilde{B} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ \mu_{2,1} & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \mu_{n,1} & \dots & \mu_{n,n-1} & 1 \end{bmatrix} .B$$

$$\mu_{i,j} = \frac{\langle b_i, \tilde{b}_j \rangle}{||\tilde{b}_j||^2}$$

Minkowski's Theorem

- Pigeonhole principle for lattices
- A symmetric and convex region with volume $2^n \det(B)^{1/n}$ has at least 2 non-zero vectors
- Hermite upper bound: $\lambda_1 \leq \sqrt{n} \det(B)^{1/n}$
- Gaussian heuristics: $\lambda_1 \leq \sqrt{\frac{2n}{\pi e}} \det(B)^{1/n}$
- Lower bound: $\lambda_1 \geq \min_i ||\tilde{b}_i||$

Shortest Vector Problem (and Gap-SVP)



Search:($v \neq 0$)

$$||v|| \leq \gamma\lambda_1$$

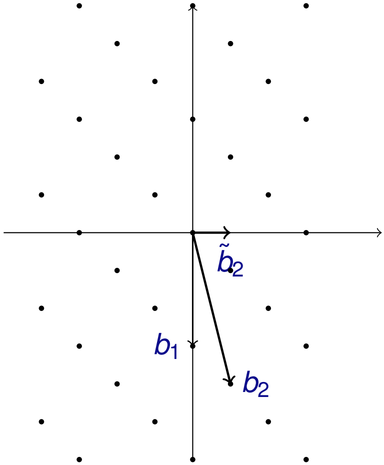
Decision: given d

$$\lambda_1 \leq \gamma d?$$

GapSVP Complexity

γ :	$2^{(\log n)^{1-\epsilon}}$	$\sqrt{n}$	n	2^n
	NP hard	NP $\cap$ coNP	crypto	P (LLL)

LLL



$$||\tilde{b}_{i+1}||^2 \geq 1/2||\tilde{b}_i||^2$$

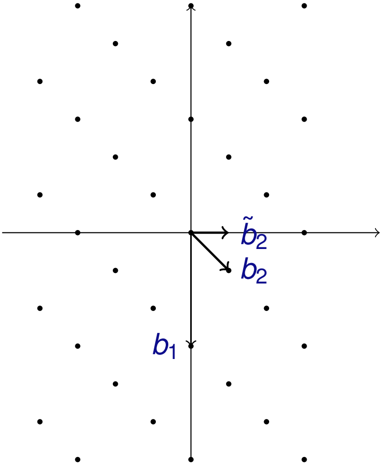
$$||b_1|| \leq 2^{(n-1)/2}\lambda_1(\mathcal{L})$$

$$b_2 = b_2 - c.b_1$$

if $||b_2||^2 < 3/4||b_1||^2$,

swap and loop

LLL



$$||\tilde{b}_{i+1}||^2 \geq 1/2||\tilde{b}_i||^2$$

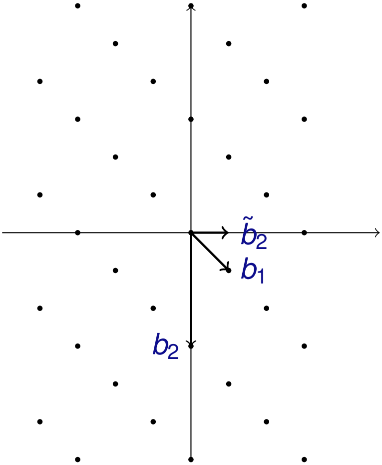
$$||b_1|| \leq 2^{(n-1)/2}\lambda_1(\mathcal{L})$$

$$b_2 = b_2 - c.b_1$$

if $||b_2||^2 < 3/4||b_1||^2$,

swap and loop

LLL



$$||\tilde{b}_{i+1}||^2 \geq 1/2||\tilde{b}_i||^2$$

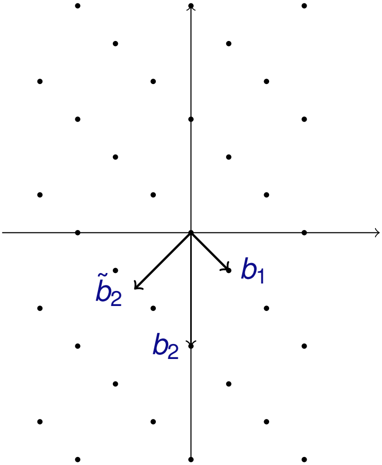
$$||b_1|| \leq 2^{(n-1)/2}\lambda_1(\mathcal{L})$$

$$b_2 = b_2 - c.b_1$$

if $||b_2||^2 < 3/4||b_1||^2$,

swap and loop

LLL



$$||\tilde{b}_{i+1}||^2 \geq 1/2||\tilde{b}_i||^2$$

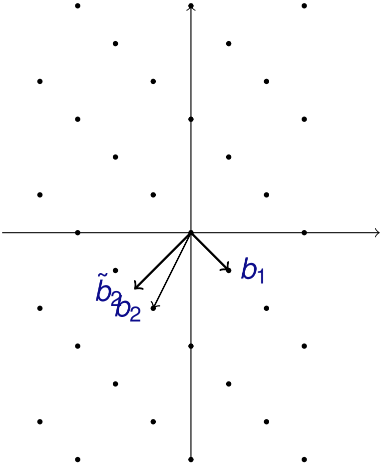
$$||b_1|| \leq 2^{(n-1)/2}\lambda_1(\mathcal{L})$$

$$b_2 = b_2 - c.b_1$$

if $||b_2||^2 < 3/4||b_1||^2$,

swap and loop

LLL



$$||\tilde{b}_{i+1}||^2 \geq 1/2||\tilde{b}_i||^2$$

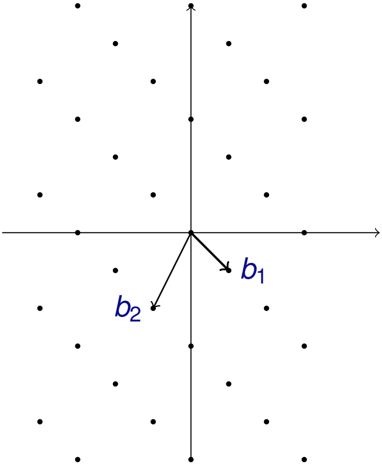
$$||b_1|| \leq 2^{(n-1)/2}\lambda_1(\mathcal{L})$$

$$b_2 = b_2 - c.b_1$$

if $||b_2||^2 < 3/4||b_1||^2$,

swap and loop

LLL



$$||\tilde{b}_{i+1}||^2 \geq 1/2||\tilde{b}_i||^2$$

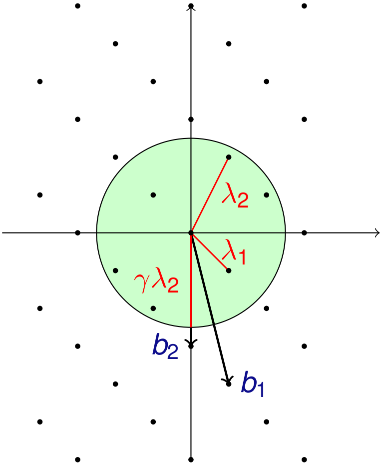
$$||b_1|| \leq 2^{(n-1)/2}\lambda_1(\mathcal{L})$$

$$b_2 = b_2 - c.b_1$$

if $||b_2||^2 < 3/4||b_1||^2$,

swap and loop

Shortest Independent Vectors Problem



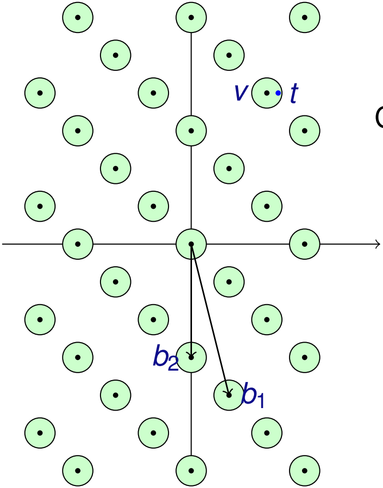
Search:

(v_1, v_2)

lin. ind.

$||v_2|| \leq \gamma\lambda_2$

Bounded Distance Decode



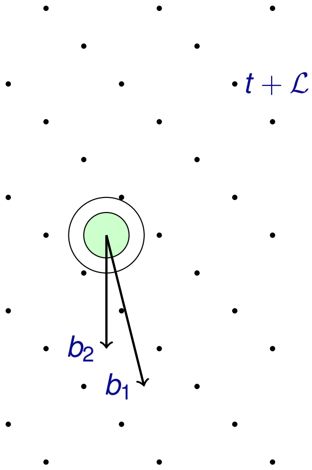
Similar to the
Closest Vector Problem (CVP)

Search: given $d < \lambda_1/2$

given $t \in \mathcal{B}_d(\mathcal{L})$

find v

Bounded Distance Decode



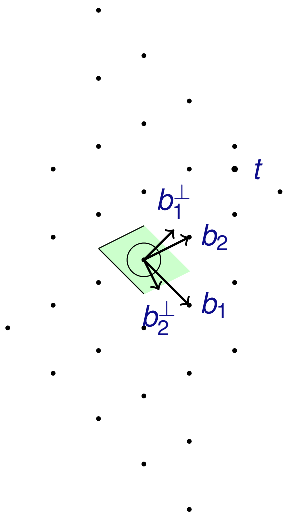
Decision: given d

given coset $t + \mathcal{L}$

decide if there is v s. t.

$||t - v|| \leq \gamma d$

Babai's Roundoff Algorithm



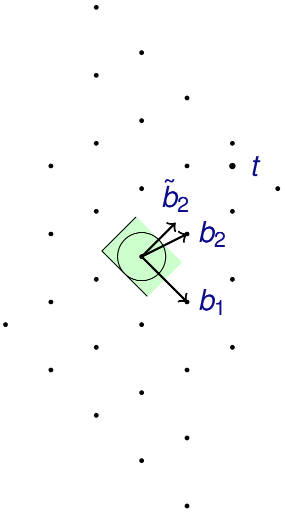
Compute $x \equiv t \pmod{B}$

$\mathcal{B}_d \subset \mathcal{P}_B$

$d = \min_i(b_i^\perp)$

(linear system)

Babai's Nearest Plane Algorithm



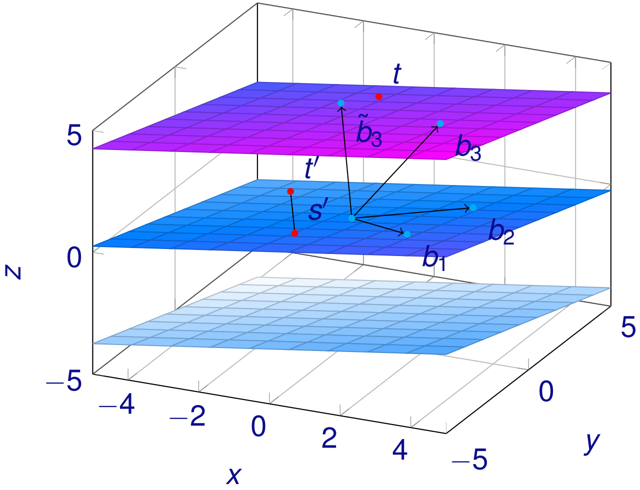
Compute $x \equiv t \pmod{\tilde{B}}$

(iteratively)

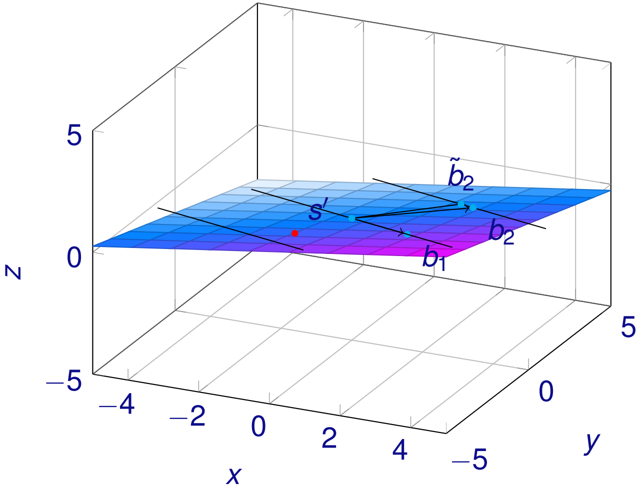
$\mathcal{B}_d \subset \mathcal{P}_{\tilde{B}}$

$d = \min_i(\tilde{b}_i)$

Babai's Nearest Plane Algorithm

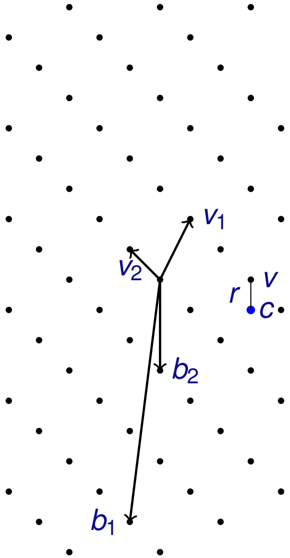


Babai's Nearest Plane Algorithm



Part II - Crypto

Goldreich, Goldwasser and Halevi (GGH)



No security proof

Trapdoor: orthogonality

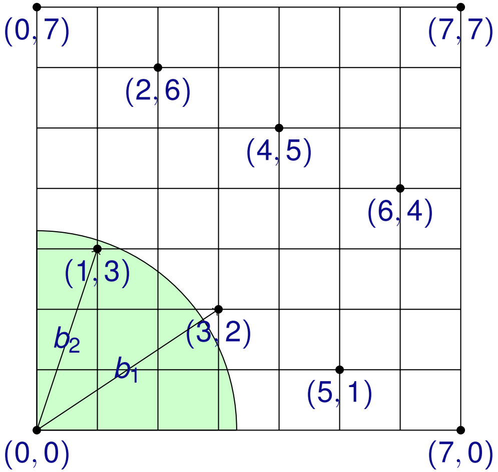
Good base: $V = (v_1, v_2)$

Bad base: $B = (b_1, b_2)$

Encrypt r: $c = v + r \pmod{B}$

Decrypt: $r = c - v$

Ajtai's Construction



$f_A(x) = Ax$

surjective

small x

(SIS problem)

collision: x, x'

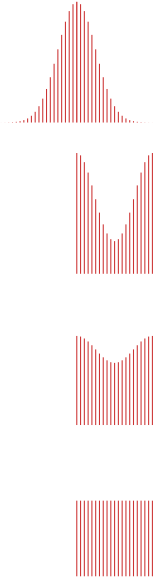
short vector: $(x - x')$

in $\Lambda_q^\perp$

worst to average

quantum reduction

Learning With Errors



Search problem:

Given $b_i = \langle a_i, s \rangle + e_i$

Find s

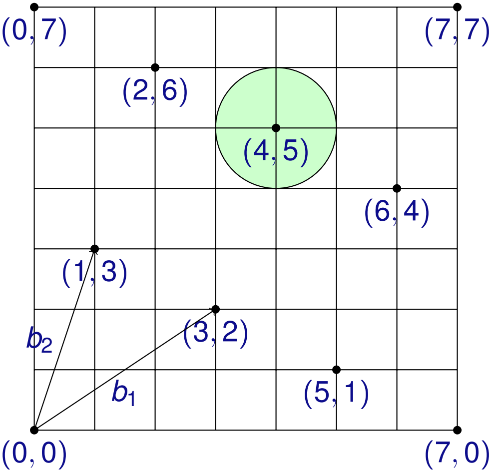
Decision problem:

Distinguish (a_i, b_i)

from uniform

Search to decision reduction

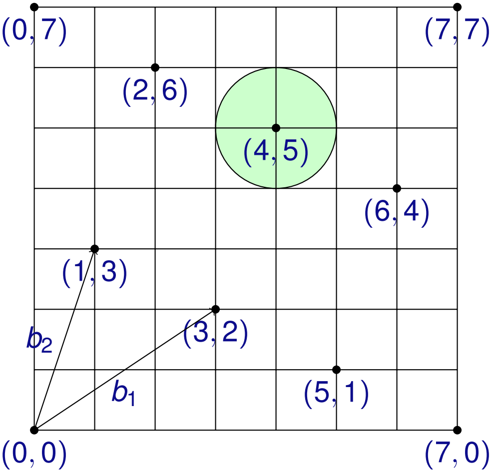
Learning With Errors



$$g_A(x) = Ax + e$$

injective

Learning With Errors



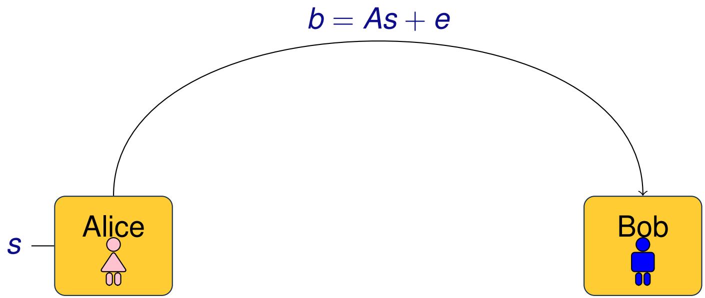
$$g_A(x) = Ax + e$$

injective

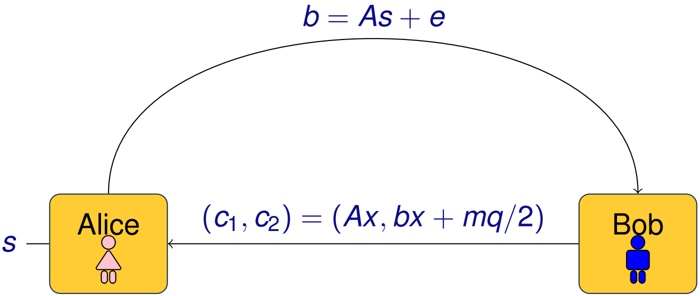
worst to average

quantum reduction

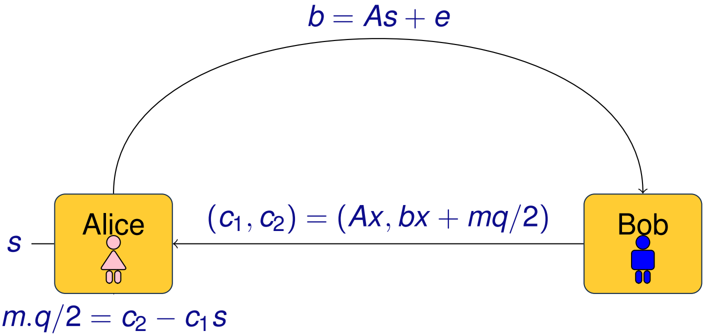
LWE Based Cryptosystem



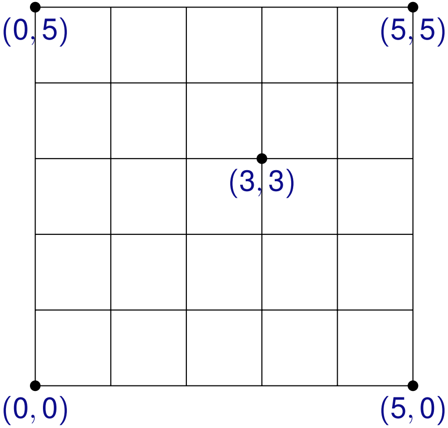
LWE Based Cryptosystem



LWE Based Cryptosystem



Cyclotomic Rings



$$\Phi_{2^n}(x) = (x^{2^{n-1}} + 1)$$

if $\zeta_{2^n} \in \mathbb{Z}_q$ then

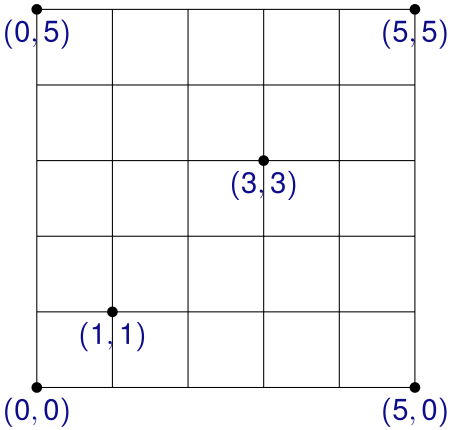
$$\Phi_{2^n} \equiv \prod_{i \in \mathbb{Z}_{2^n}^*} (x - \zeta_{2^n}^i)$$

Ring: $\mathbb{Z}_5[x]/(x^2 + 1)$

$$x^2 + 1 \equiv (x + 2)(x + 3)$$

$$a(x) = 3x + 3$$

Coefficient Representation

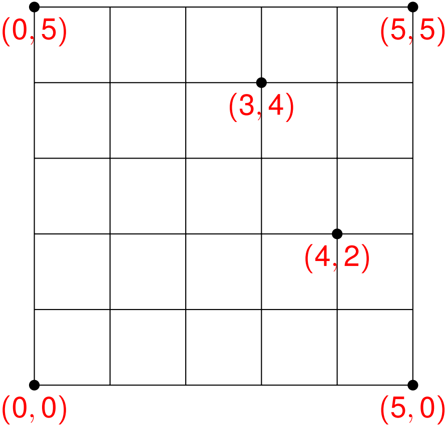


Ring: $\mathbb{Z}_5[x]/(x^2+1)$

$$x^2 + 1 \equiv (x+2)(x+3)$$
$$\equiv (x-3)(x-2)$$

$$a(x) = 3x + 3$$
$$2(3x+3) \equiv x + 1$$
$$\begin{bmatrix} 3 & 3 \end{bmatrix}^T, \begin{bmatrix} 1 & 1 \end{bmatrix}^T$$

Evaluation Representation



Ring: $\mathbb{Z}_5[x]/(x^2+1)$

$$x^2+1 \equiv (x+2)(x+3)$$

$$a(x) = 3x+3$$

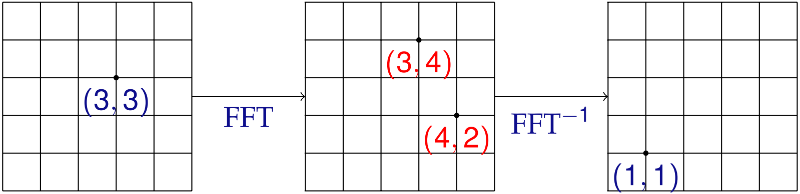
$$2a(x) \equiv x+1$$

$$a(2) \equiv 4, a(3) \equiv 2$$

$$\begin{bmatrix} 4 & 2 \end{bmatrix}^T, \begin{bmatrix} 3 & 4 \end{bmatrix}^T$$

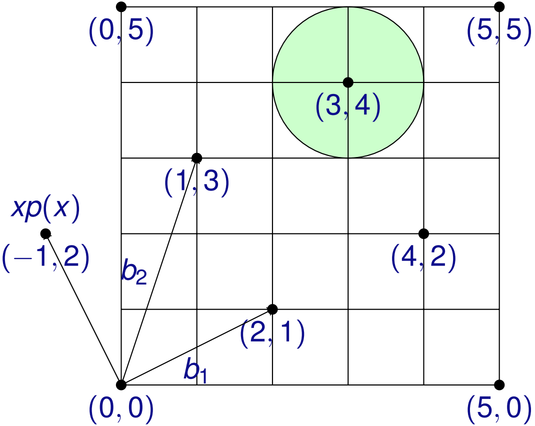
$\boxed{\text{FFT}}$

Cyclotomic Rings



$$\underbrace{\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}}_{\text{Vandermond}} \begin{bmatrix} 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix} \qquad \underbrace{\begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}}_{\text{Vandermond inverse}} \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Ring LWE



$$g_A(x) = Ax + e$$

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}$$

ideal: $p(x) = x + 2$

Ring LWE

- Better reductions, better parameters

Ring LWE

- Better reductions, better parameters
  - Encryption, decryption, keygen: $\tilde{O}(n)$

Ring LWE

- Better reductions, better parameters
  - Encryption, decryption, keygen: $\tilde{O}(n)$
- Preimage sampleable trapdoors

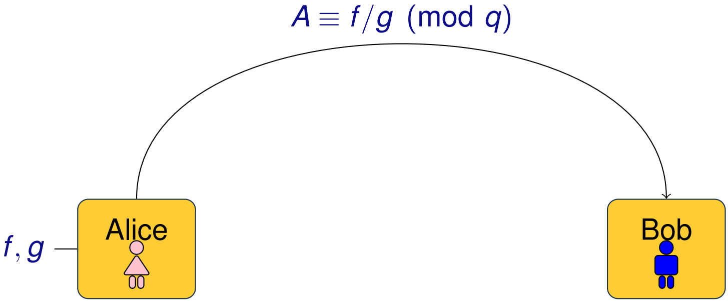
Ring LWE

- Better reductions, better parameters
  - Encryption, decryption, keygen: $\tilde{O}(n)$
- Preimage sampleable trapdoors
  - Digital Signatures

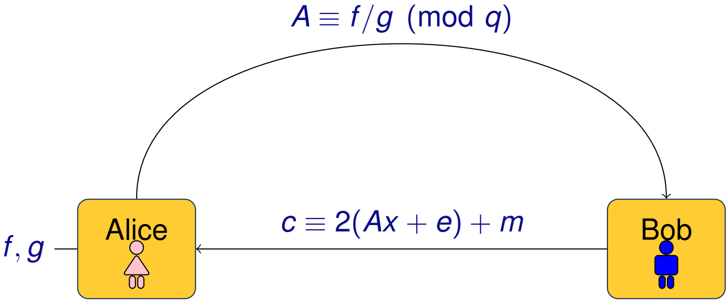
Ring LWE

- Better reductions, better parameters
  - Encryption, decryption, keygen: $\tilde{O}(n)$
- Preimage sampleable trapdoors
  - Digital Signatures
- Cryptomania: IBE, ABE, FE, FHE

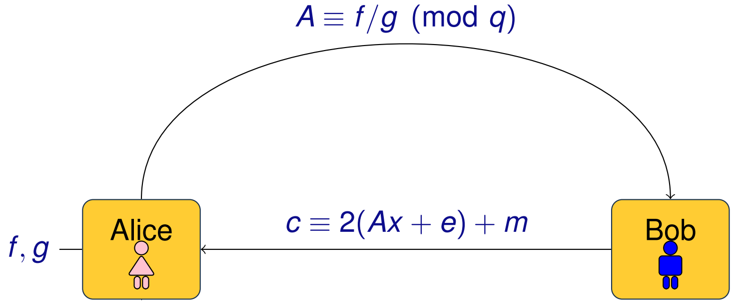
NTRU-like Cryptosystem [13]



NTRU-like Cryptosystem [13]



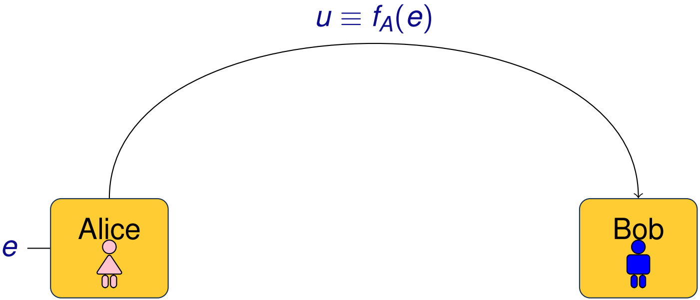
NTRU-like Cryptosystem [13]



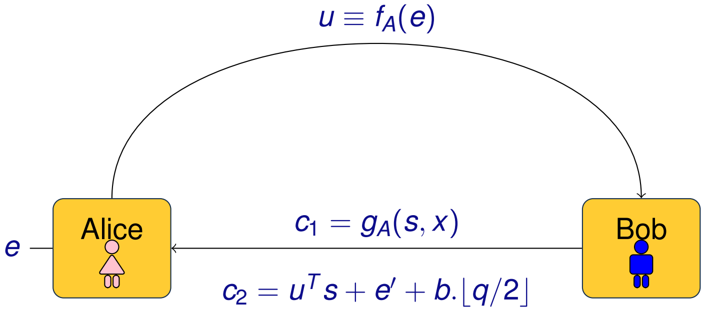
$$cg \equiv 2(fx + eg) + mg$$

$$m \equiv (cg \pmod{2})/g$$

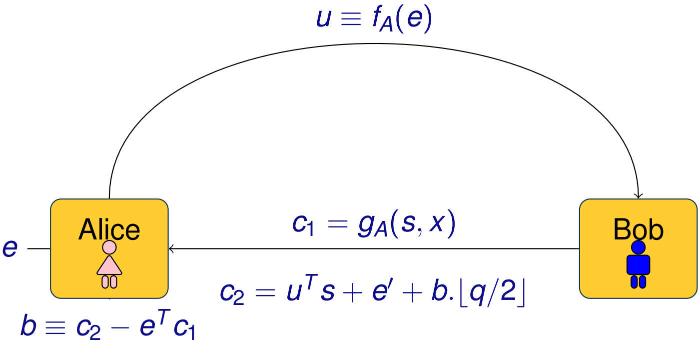
Dual LWE



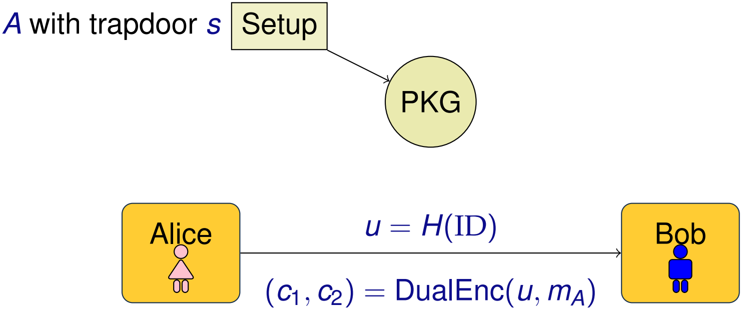
Dual LWE



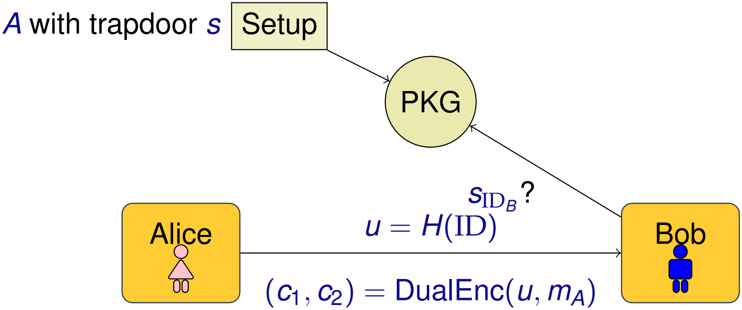
Dual LWE


$u \equiv f_A(e)$
Alice
Bob
e
$c_1 = g_A(s, x)$
$c_2 = u^T s + e' + b.\lfloor q/2 \rfloor$
$b \equiv c_2 - e^T c_1$

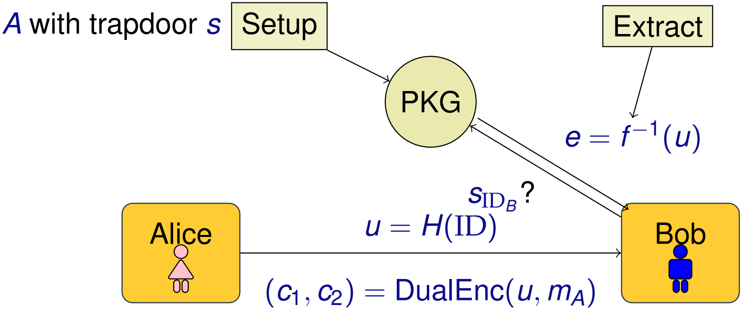
Identity Based Encryption



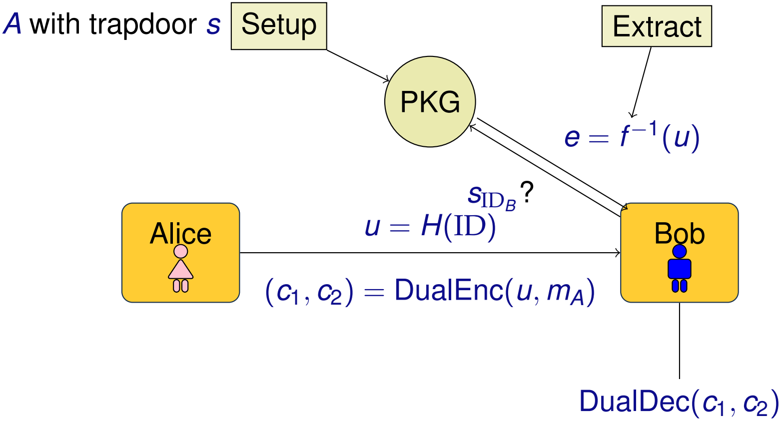
Identity Based Encryption



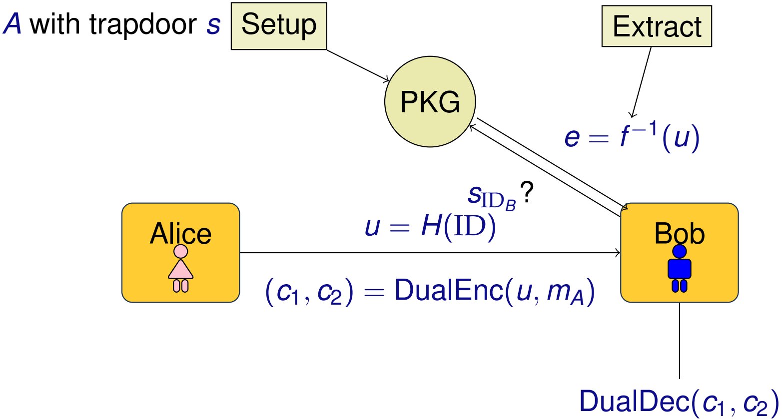
Identity Based Encryption



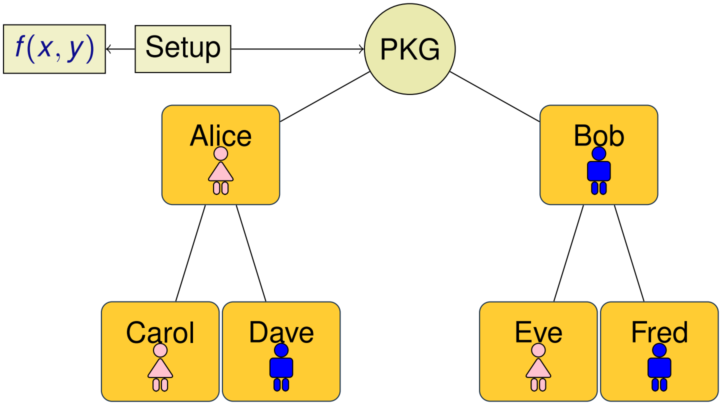
Identity Based Encryption



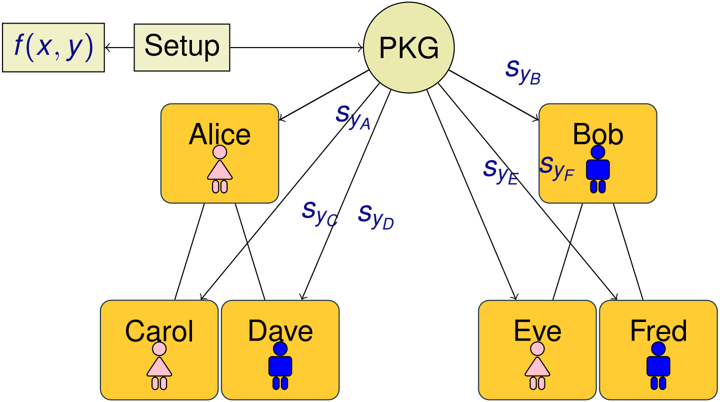
Identity Based Encryption



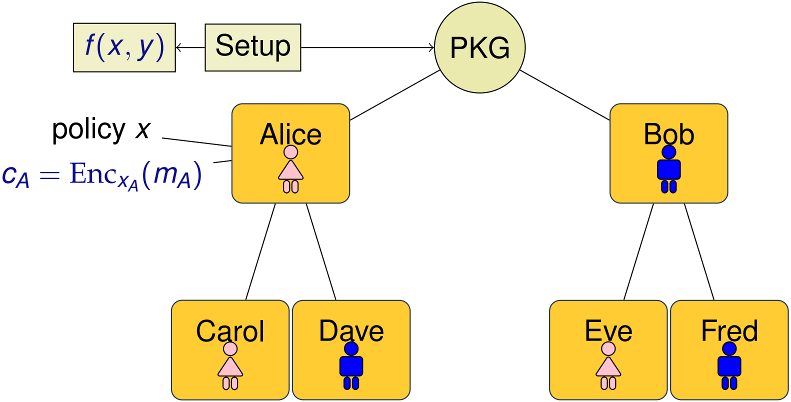
Functional Encryption



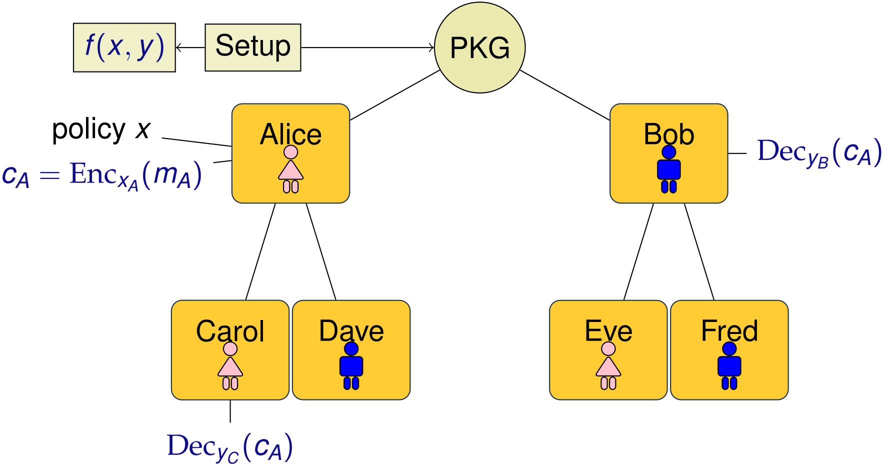
Functional Encryption



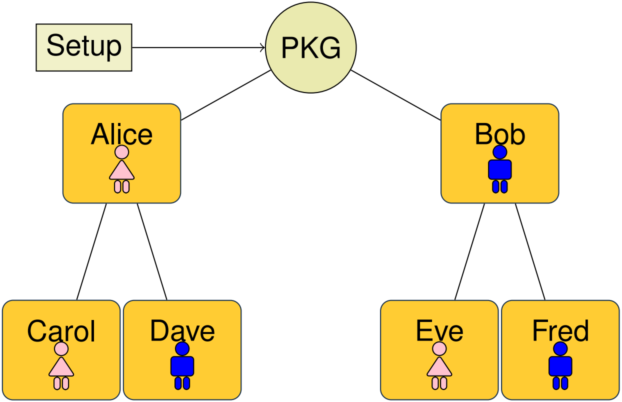
Functional Encryption



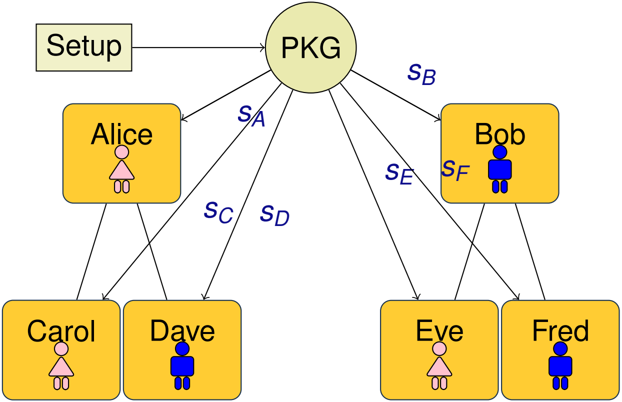
Functional Encryption



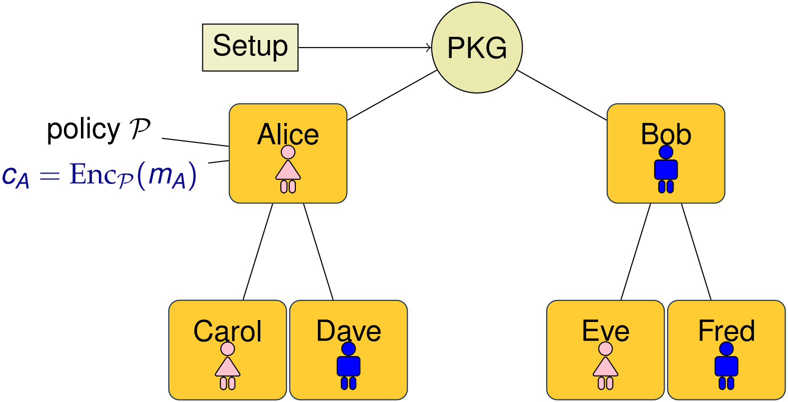
Attribute Based Encryption



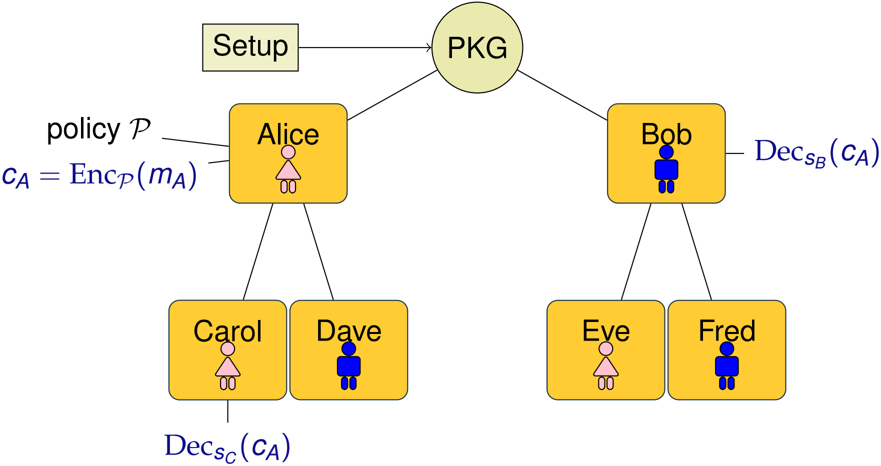
Attribute Based Encryption



Attribute Based Encryption



Attribute Based Encryption



Fully Homomorphic Encryption

- Operations over encrypted messages

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications
- The error allows the computation, but can't decrypt after some point

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications
- The error allows the computation, but can't decrypt after some point
- Bootstrapping

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications
- The error allows the computation, but can't decrypt after some point
- Bootstrapping
- Initially close to GGH cryptosystem

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications
- The error allows the computation, but can't decrypt after some point
- Bootstrapping
- Initially close to GGH cryptosystem
- Now: RLWE and NTRU-like

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications
- The error allows the computation, but can't decrypt after some point
- Bootstrapping
- Initially close to GGH cryptosystem
- Now: RLWE and NTRU-like
- Not practical yet

Fully Homomorphic Encryption

- Operations over encrypted messages
- Evaluate functions with encrypted arguments
- Very interesting applications
- The error allows the computation, but can't decrypt after some point
- Bootstrapping
- Initially close to GGH cryptosystem
- Now: RLWE and NTRU-like
- Not practical yet
- More with Zvika Brakerski

Conclusion

- Worst case reductions

Conclusion

- Worst case reductions
- Efficient (at least asymptotically): $\tilde{O}(n)$

Conclusion

- Worst case reductions
- Efficient (at least asymptotically): $\tilde{O}(n)$
- Cryptomania: IBE, FE, ABE, FHE

Conclusion

- Worst case reductions
- Efficient (at least asymptotically): $\tilde{O}(n)$
- Cryptomania: IBE, FE, ABE, FHE
- Post-quantum cryptography

Conclusion

- Worst case reductions
- Efficient (at least asymptotically): $\tilde{O}(n)$
- Cryptomania: IBE, FE, ABE, FHE
- Post-quantum cryptography
- Lattices are not yet recommended by NSA!

References

M. Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, pages 99–108, New York, NY, USA, 1996. ACM.

L Babai.
On lovász lattice reduction and the nearest lattice point problem.
Combinatorica, (6), 1986.

Sanjam Garg, Craig Gentry, and Shai Halevi.
Candidate multilinear maps from ideal lattices.
In *EUROCRYPT*, pages 1–17, 2013.

Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters.
Candidate indistinguishability obfuscation and functional encryption for all circuits.
IACR Cryptology ePrint Archive, 2013:451, 2013.

Craig Gentry.
A fully homomorphic encryption scheme.
PhD thesis, Stanford University, 2009.
`crypto.stanford.edu/craig`.

Craig Gentry and Shai Halevi.
Hierarchical identity based encryption with polynomially many levels.
In *TCC*, pages 437–456, 2009.

Craig Gentry, Amit Sahai, and Brent Waters.
Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based.
In *CRYPTO (1)*, pages 75–92, 2013.

Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman.
An Introduction to Mathematical Cryptography.
Springer Publishing Company, Incorporated, 1 edition, 2008.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
Ntru: A ring-based public key cryptosystem.
In *Lecture Notes in Computer Science*, pages 267–288. Springer-Verlag, 1998.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
On ideal lattices and learning with errors over rings.
Advances in Cryptology EUROCRYPT 2010, 6110/2010(015848):1?23, 2010.

Daniele Micciancio and Chris Peikert.
Trapdoors for lattices: Simpler, tighter, faster, smaller.
In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer Berlin Heidelberg, 2012.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.

Damien Stehlé and Ron Steinfeld.
Making ntru as secure as worst-case problems over ideal lattices.
In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, EUROCRYPT'11, pages 27–47, Berlin, Heidelberg, 2011. Springer-Verlag.

Thank you

Questions?