

Duality in Lattice Cryptography

Daniele Micciancio

Department of Computer Science and Engineering
University of California, San Diego

May 28, 2010 (PKC'10, Paris)

Lattice Cryptography

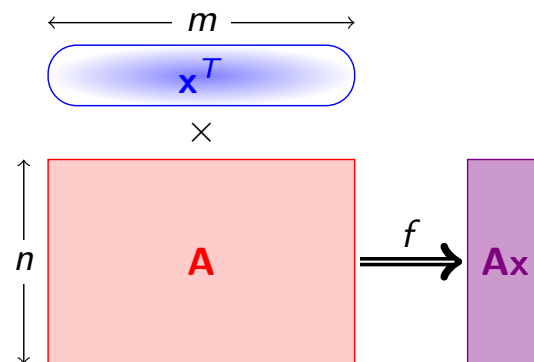
- (Merkle,Hellman'78) Knapsack/subset-sum cryptosystems
 - Subject to lattice reduction attacks
- (Ajtai'96) One-way function based on *worst-case* hardness of lattice problems
 - Applications: hashing, commitment schemes, digital signatures, identification protocols
- (Regev'05) Hardness of “Learning with Errors” based on worst-case **quantum** hardness of lattice problems
 - Applications: (efficient) CPA secure encryption, CCA security, IBE, HIBE, . . . , fully homomorphic encryption?
- Public key encryption can also be based on random subset-sum (Impagliazzo,Naor'96, Lyubashevsky,Palacio,Segev'10) or certain worst-case lattice problems under classical reductions (Ajtai,Dwork'97, Peikert'09, Lyubashevsky,Micciancio'09).

Outline

- 1 Lattice Cryptography
 - Hard on average problems (Ajtai and LWE)
 - Public Key Cryptosystems (Regev and GPV)
- 2 Introduction to Point Lattices
 - Computational Problems
 - The dual lattice
- 3 Duality in Lattice Cryptography
 - Random Lattices and duality
 - Relating Regev and GPV cryptosystems

Ajtai's one-way function

- Parameters: $m, n, q \in \mathbb{Z}$
- Key: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$
- Input: $\mathbf{x} \in \{0, 1\}^m$
- Output: $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{Ax} \bmod q$



Theorem (Ajtai 96)

For $m > n \lg q$, if lattice problems (SIVP) are hard to approximate in the worst-case, then $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{Ax} \bmod q$ is a one-way function.

Properties and Applications of Ajtai's function

Remark

Since $m > n \lg q$, we have $|\mathbf{x}| > |\mathbf{Ax} \bmod q| = |f_{\mathbf{A}}(\mathbf{x})|$ and $f_{\mathbf{A}}$ is a compression function.

Applications:

- Universal hashing [HILL'99]: $f_{\mathbf{A}}(\{0, 1\}^m) \approx \mathbf{Z}_q^n$.
- Collision resistant **hashing** [GGH'97]: $\text{Hash}(\mathbf{m}) = f_{\mathbf{A}}(\mathbf{m})$.
- Statistically hiding **commitments** [KTX'08]:
 $\text{Commit}(\mathbf{m}; \mathbf{r}) = f_{\mathbf{A}}([\mathbf{m} | \mathbf{r}])$
- **Identification** protocols [MV'03, L'08, KTX'08]
- **Digital signatures** [LM'08, GPV'08, L'09, CHKP'10, R'10, B'10]

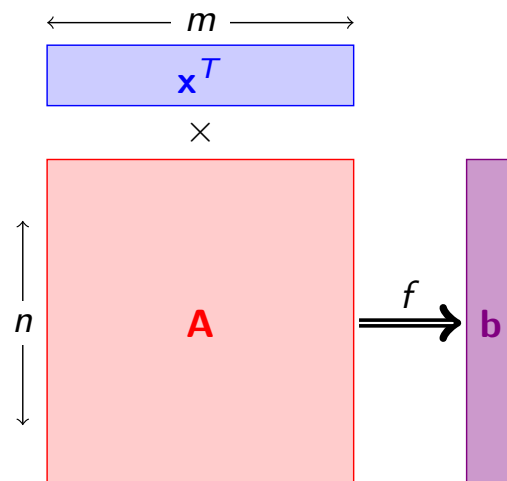
Security Considerations

Inverting $f_{\mathbf{A}}$

Input: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{b} = \mathbf{Ax} \bmod q \in \mathbb{Z}_q^n$

Output: $\mathbf{x} \in \{0, 1\}^m$ such that $\mathbf{Ax} = \mathbf{b} \bmod q$

- Easy to find $\mathbf{x} \in \mathbb{Z}_q^m$ such that $\mathbf{Ax} = \mathbf{b}$
- If $n \geq m$, then $f_{\mathbf{A}}$ is not one-way
 - Find $\mathbf{x}' \in \mathbb{Z}_q^m$ such that $\mathbf{Ax}' = \mathbf{b}$
 - With high probability, solution is unique and $\mathbf{x}' = \mathbf{x} \in \{0, 1\}^m$.

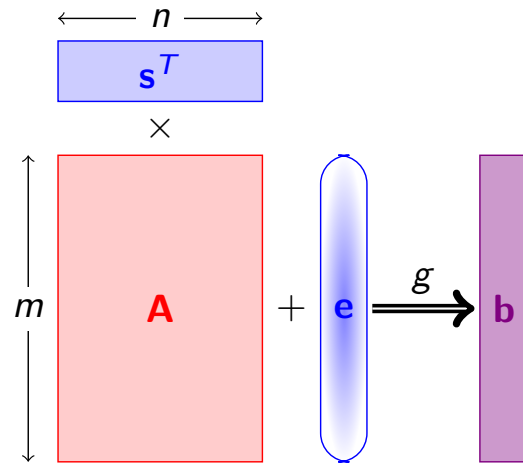


Learning with errors (LWE)

- $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, $\mathbf{s} \in \mathbb{Z}_q^n$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s}; \mathbf{e}) = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
- Learning with Errors: Given \mathbf{A} and $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$, recover \mathbf{s} .

Theorem (Regev'05)

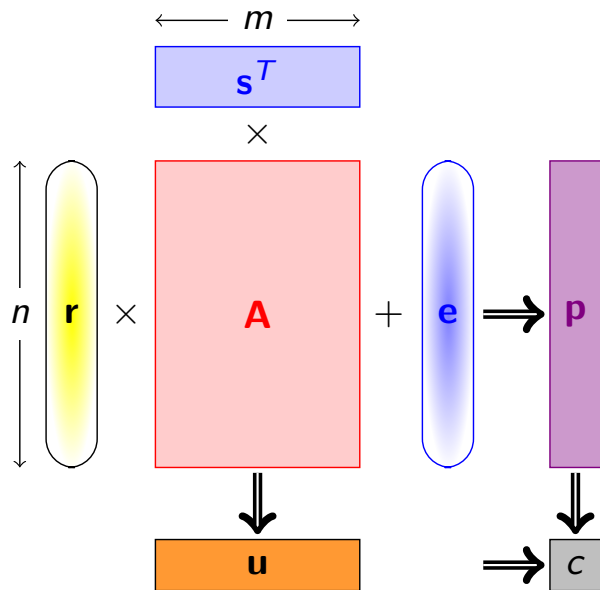
The function $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$ is hard to invert on the average, assuming SIVP is hard to approximate in the worst-case even for **quantum** computers.



Properties and Applications of LWE

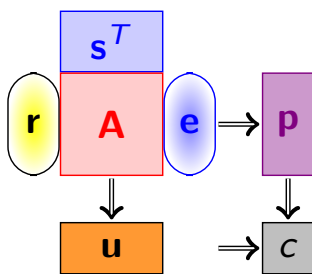
- If $m \gg n$, then $g_{\mathbf{A}}$ expands the input \mathbf{x}, \mathbf{e}
- (Regev'05) If $g_{\mathbf{A}}$ is hard to invert for any $n = m^{O(1)}$, then $g_{\mathbf{A}}(\mathbf{x}; \mathbf{e}) \approx_c \mathbb{Z}_q^m$ is pseudorandom for any $n = m^{O(1)}$.
- Applications:
 - Pseudorandom generators, Stream ciphers, Symmetric encryption, computationally binding commitments.
 - Public key encryption [R'05, GPV'08, PVW'08]
 - CCA secure encryption [PW'08, P'09]
 - (Hierarchical) identity based encryption [GPV'08,CHKP'10,ABB'10,ABB'10]
 - Oblivious Transfer [PVW'08]
 - Threshold Cryptosystems [BD'10]
 - Homomorphic encryption [GHV'10, SV'10, vDGHV'10, AGH'10]
 - Leakage resilient cryptography [DGKP'10, GKPV'10]

Regev (LWE) cryptosystem



- Parameters:
 $m, n, q \in \mathbb{Z}, \mathbf{A} \in \mathbb{Z}_q^{m \times n}$
- Secret key: $\mathbf{s} \in \mathbb{Z}_q^n, \mathbf{e} \in \mathcal{E}^m$
- Public key:
 $\mathbf{p} = \mathbf{A}\mathbf{s} + \mathbf{e} \approx_c \mathbb{Z}_q^m$
- $\text{Encrypt}_{\mathbf{p}}(m; (\mathbf{r}))$:
$$\mathbf{u} = \mathbf{r}^T \mathbf{A}$$
$$\mathbf{c} = \mathbf{r}^T \mathbf{p} + m - r_0$$
- $\text{Decrypt}_{\mathbf{s}}(\mathbf{u}, \mathbf{c}) =$
$$\mathbf{c} - \mathbf{u} \cdot \mathbf{s} \approx m.$$

Remarks on LWE cryptosystem

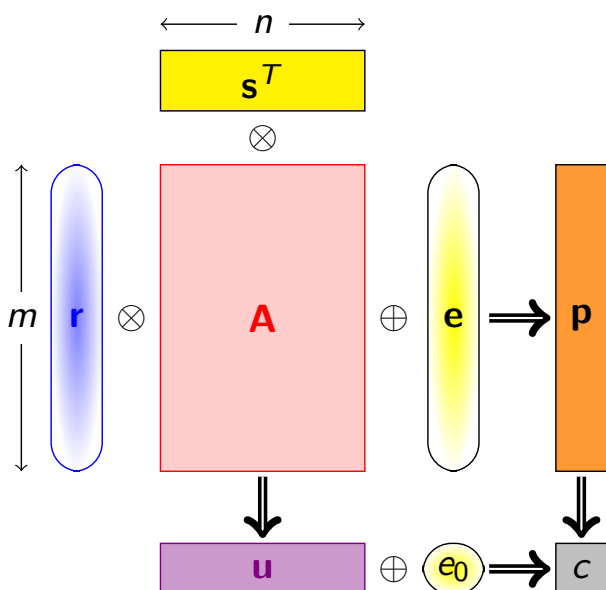


- Public key $\mathbf{p} = \mathbf{A}\mathbf{s} + \mathbf{e} \approx_c \mathbb{Z}_q^m$
- Ciphertexts
 $[\mathbf{u}, \mathbf{c}] = \mathbf{r}^T [\mathbf{A}, \mathbf{p}] + [\mathbf{0}, m + r_0]$
- Set of valid public keys is sparse, but pseudorandom
- When public key is pseudo-random, ciphertexts are sparse too, and can be decrypted using the secret key
- If public key is random, ciphertexts are close to uniform, and decryption is impossible.

GPV (dual LWE) cryptosystem: Motivation and Idea

- Goal: Identity based encryption in the Random Oracle model
- Main technical problems:
 - The public key derivation function (\mathbf{A}) should be generated together with an “inversion trapdoor” [GPV’08: “Trapdoor for hard lattices”]
 - Need an encryption scheme with dense public key space: any string (output by a “random oracle”) can be interpreted as a public key.
- Solution: Variant of Regev (LWE) cryptosystem with dense public key space

GPV (dual LWE) cryptosystem



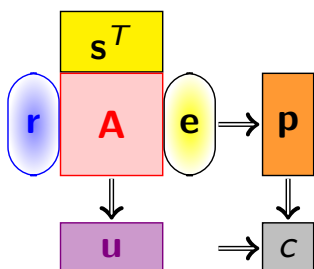
- Parameters:
 $m, n, q \in \mathbb{Z}, \mathbf{A} \in \mathbb{Z}_q^{m \times n}$
- Secret key: $\mathbf{r} \in \mathcal{E}^m$
- Public key: $\mathbf{u} = \mathbf{r}^T \mathbf{A} \approx_s \mathbb{Z}_q^m$
- Encrypt $_{\mathbf{u}}(m; \mathbf{e})$:

$$\mathbf{p} = \mathbf{A}\mathbf{s} + \mathbf{e}$$

$$c = \mathbf{u} \cdot \mathbf{s} + \mathbf{e}_0 + m$$

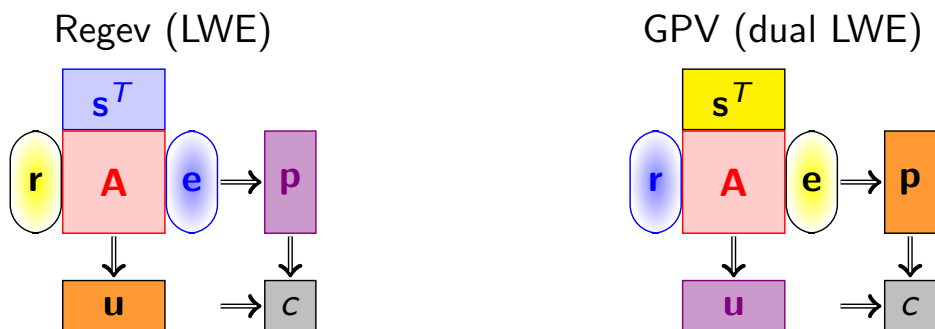
- Decrypt $_{\mathbf{r}}(\mathbf{p}, c) =$
 $c - \mathbf{r}^T \mathbf{p} \approx m$.

Remarks on GPV cryptosystem



- Set of valid public keys $\mathbf{u} = \mathbf{r}^T \mathbf{A}$ equals \mathbb{Z}_q^m
- Useful in Identity Based Encryption (IBE)
- Ciphertexts $[\mathbf{u}, c] = (\mathbf{A}, \mathbf{u})\mathbf{s} + (\mathbf{e}, x) + (\mathbf{0}, m)$ are pseudorandom under LWE assumption

Comparing Regev and GPV encryption



Regev and GPV cryptosystems use the same mathematical objects

$\mathbf{A}, \mathbf{s}, \mathbf{r}, \mathbf{e}, \mathbf{p}, \mathbf{u}, c$, but operate on them in different roles:

Public key generation	\iff	Encryption
Secret key	\iff	Encryption randomness
Public key	\iff	Ciphertext

Naive interpretation

- The schemes are **syntactically similar**: Regev and GPV cryptosystems operate on the same mathematical objects **A, s, r, e, p, u, c**.
- The scheme are **semantically different**:

Common parameters	A	\iff	A	Common parameters
secret key	s, e	\iff	s, e	encryption randomness
encryption randomness	r	\iff	r	secret key
public key	p	\iff	p	ciphertext
ciphertext	u	\iff	u	public key

The true answer: Lattices and Duality

- The schemes are **syntactically different**: The symbols **A, s, r, e, p, u, c** in Regev and GPV cryptosystems represent different mathematical objects
- The two schemes are **semantically equivalent**:

Common parameters	A	\iff	A'	Common parameters
secret key	s, e	\iff	r'	secret key
encryption randomness	r	\iff	s', e'	encryption randomness
public key	p	\iff	u'	public key
ciphertext	u	\iff	p'	ciphertext

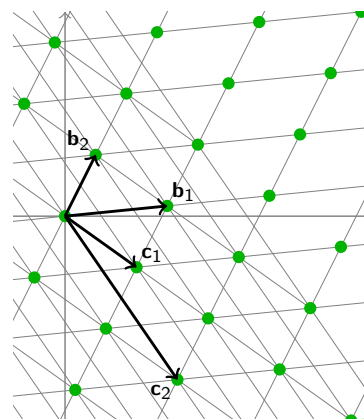
Point Lattices

A lattice is the set of all **integer** linear combinations of (linearly independent) **basis** vectors $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

$$\mathcal{L} = \sum_{i=1}^n \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{B}\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$$

The same lattice has many bases

$$\mathcal{L} = \sum_{i=1}^n \mathbf{c}_i \cdot \mathbb{Z}$$



Definition (Lattice)

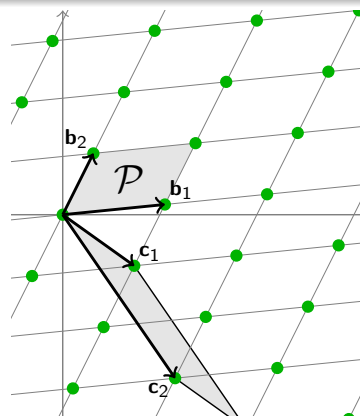
A discrete additive subgroup of \mathbb{R}^n

Quantities associated to a lattice

Definition (Determinant)

$\det(\mathcal{L}) = \text{volume of the fundamental region } \mathcal{P} = \sum_i \mathbf{b}_i \cdot [0, 1)$

- Different bases define different fundamental regions
- All fundamental regions have the same volume
- The determinant of a lattice can be efficiently computed from any basis.



Minimum Distance and Successive Minima

- Minimum distance

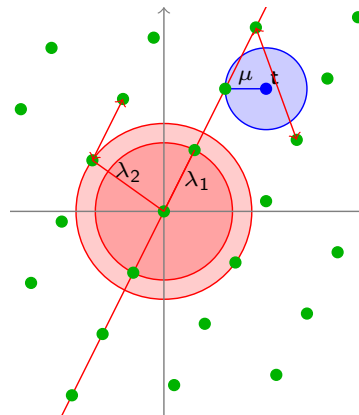
$$\begin{aligned}\lambda_1 &= \min_{\mathbf{x}, \mathbf{y} \in \mathcal{L}, \mathbf{x} \neq \mathbf{y}} \|\mathbf{x} - \mathbf{y}\| \\ &= \min_{\mathbf{x} \in \mathcal{L}, \mathbf{x} \neq \mathbf{0}} \|\mathbf{x}\|\end{aligned}$$

- Successive minima ($i = 1, \dots, n$)

$$\lambda_i = \min\{r : \dim \text{span}(\mathcal{B}(r) \cap \mathcal{L}) \geq i\}$$

- Distance function

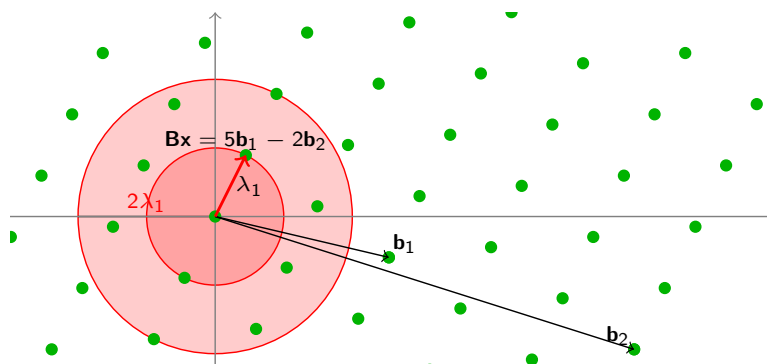
$$\mu(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{t} - \mathbf{x}\|$$



Shortest Vector Problem

Definition (Shortest Vector Problem, SVP_γ)

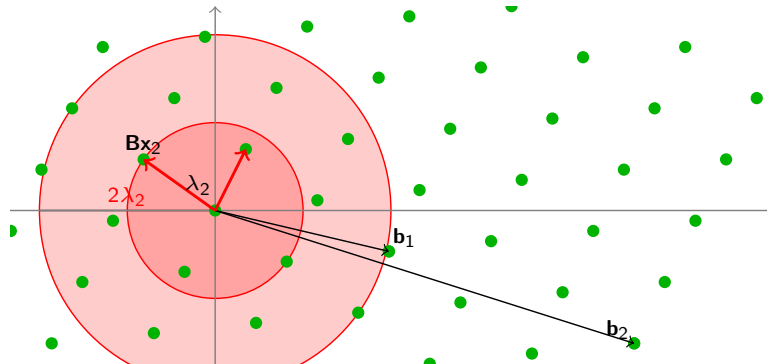
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector \mathbf{Bx} (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \gamma \lambda_1$



Shortest Independent Vectors Problem

Definition (Shortest Independent Vectors Problem, $SIVP_\gamma$)

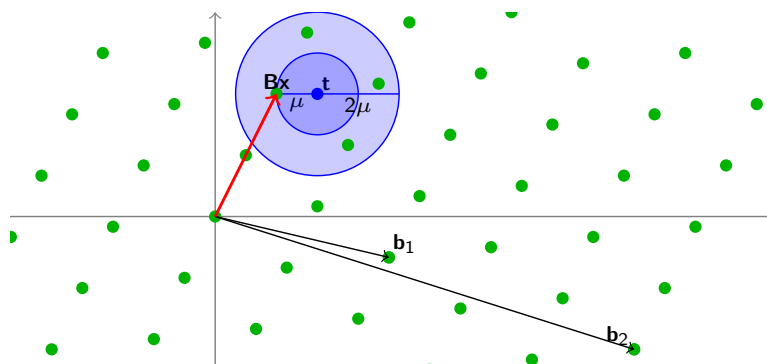
Given a lattice $\mathcal{L}(\mathbf{B})$, find n linearly independent lattice vectors $\mathbf{Bx}_1, \dots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \gamma \lambda_n$



Closest Vector Problem

Definition (Closest Vector Problem, CVP_γ)

Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point \mathbf{t} , find a lattice vector \mathbf{Bx} within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma \mu$ from the target



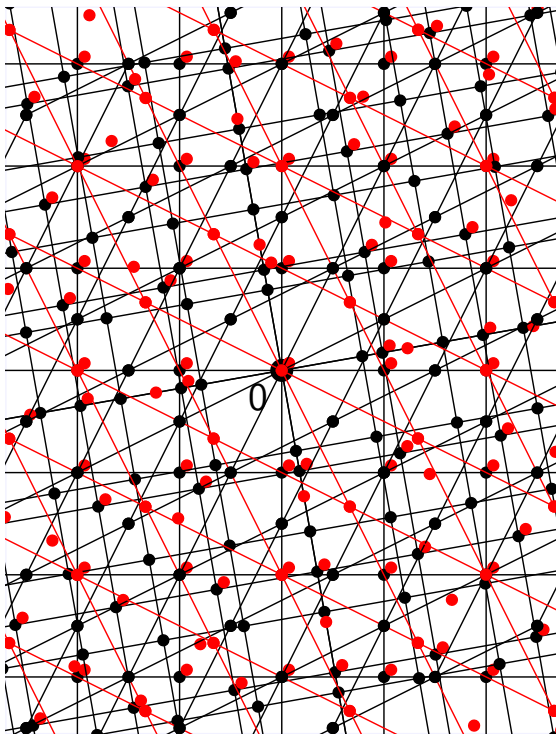
The Dual

- A vector space over \mathbb{R} is a set of vectors V with
 - a vector addition operation $\mathbf{x} + \mathbf{y} \in V$
 - a scalar multiplication $a \cdot \mathbf{x} \in V$
- The dual of a vector space V is the set $V^* = \text{Hom}(V, \mathbb{R})$ of linear functions $\phi : V \rightarrow \mathbb{R}$, typically represented as vectors $\mathbf{x} \in V$, where $\phi_{\mathbf{x}}(\mathbf{y}) = \langle \mathbf{x}, \mathbf{y} \rangle$
- The dual of a lattice Λ is defined similarly as the set of linear functions $\phi_{\mathbf{x}} : \Lambda \rightarrow \mathbb{Z}$ represented as vectors $\mathbf{x} \in \text{span}(\Lambda)$.

Definition (Dual lattice)

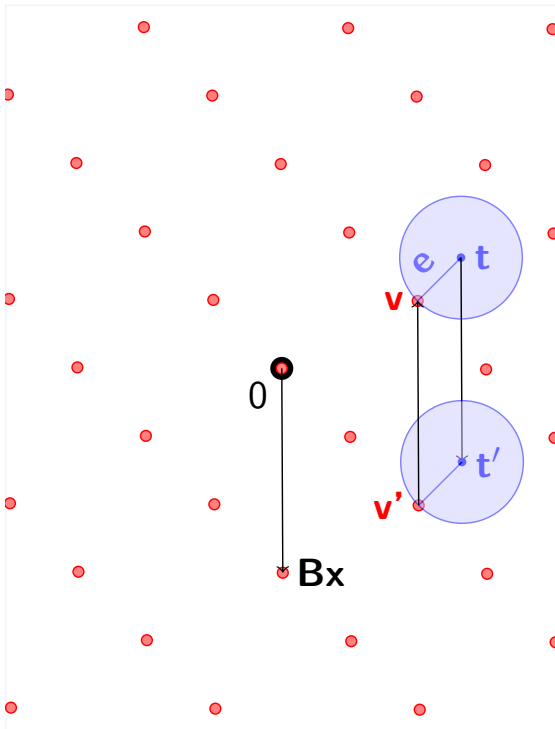
The dual of a lattice Λ is the set of all vectors $\mathbf{x} \in \text{span}(\Lambda)$ such that $\langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}$ for all $\mathbf{v} \in \Lambda$

Dual lattice: Examples



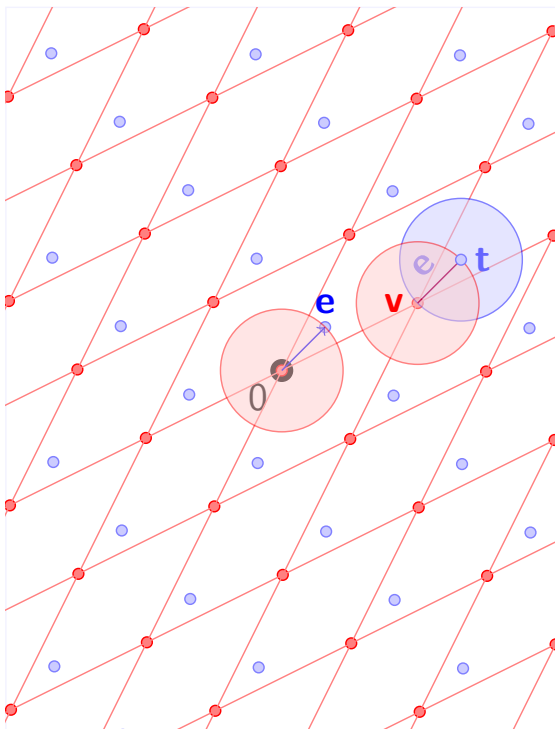
- Integer lattice $(\mathbb{Z}^n)^* = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^* = \mathbf{R}(\Lambda^*)$
- Scaling $(q \cdot \Lambda)^* = \frac{1}{q} \cdot \Lambda^*$
- Properties of dual:
 - $\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^* \supseteq \Lambda_2^*$
 - $(\Lambda^*)^* = \Lambda$
- Operations on $\mathbf{x} \in \Lambda$ and $\mathbf{y} \in \Lambda^*$:
 - $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$
 - but $\mathbf{x} + \mathbf{y}$ has no geometric meaning

Closest Vector Problem



- Lattice Λ , target \mathbf{t}
- CVP: Find \mathbf{v} such that $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is shortest possible
- $\mathbf{t}' = \mathbf{t} + \mathbf{Bx}$
- $\mathbf{v} = \mathbf{v}' - \mathbf{Bx}$

CVP and dual lattice



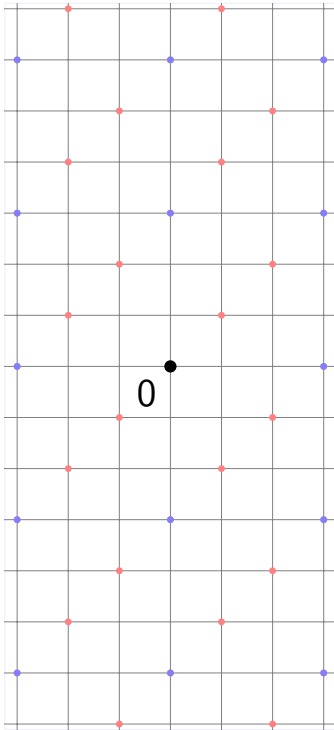
- Lattice Λ , target $\mathbf{t} = \mathbf{v} + \mathbf{e}$
- Dual lattice $\Lambda^* = \mathcal{L}(\mathbf{D})$.
- Syndrome of \mathbf{t} :

$$\begin{aligned} \mathbf{s} &= \langle \mathbf{D}, \mathbf{t} \rangle \bmod 1 \\ &= \langle \mathbf{D}, \mathbf{v} \rangle + \langle \mathbf{D}, \mathbf{e} \rangle \bmod 1 \\ &= \langle \mathbf{D}, \mathbf{e} \rangle \bmod 1. \end{aligned}$$
- \mathbf{e} belongs to coset $\mathbf{t} + \Lambda = \{\mathbf{x} : \langle \mathbf{D}, \mathbf{x} \rangle = \mathbf{s} \bmod 1\}$

Problem (Syndrome Decoding)

Find shortest \mathbf{e} such that $\langle \mathbf{D}, \mathbf{e} \rangle = \mathbf{s} \bmod 1$

Random lattices in Cryptography



- Cryptography typically uses (random) lattices Λ such that
 - $\Lambda \subseteq \mathbb{Z}^d$ is an integer lattice
 - $q\mathbb{Z}^d \subseteq \Lambda$ is periodic modulo a small integer q .
- Cryptographic functions based on q -ary lattices involve only arithmetic modulo q .

Definition (q -ary lattice)

Λ is a q -ary lattice if $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

Examples of q -ary lattices

Examples (for any $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$)

- $\Lambda_q(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A}^T \mathbb{Z}_q^n\} \subseteq \mathbb{Z}^d$
- $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\} \subseteq \mathbb{Z}^d$

Theorem

For any lattice Λ the following conditions are equivalent:

- $q\mathbb{Z}^d \subseteq \Lambda \subseteq \mathbb{Z}^d$
- $\Lambda = \Lambda_q(\mathbf{A})$ for some \mathbf{A}
- $\Lambda = \Lambda_q^\perp(\mathbf{A})$ for some \mathbf{A}

Duality of q -ary lattices

- For any fixed \mathbf{A} , the lattices $\Lambda_q(\mathbf{A})$ and $\Lambda_q^\perp(\mathbf{A})$ are **different**
- For any $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$ there is a $\mathbf{A}' \in \mathbb{Z}_q^{k \times d}$ such that $\Lambda_q(\mathbf{A}) = \Lambda_q^\perp(\mathbf{A}')$.
- For any $\mathbf{A}' \in \mathbb{Z}_q^{k \times d}$ there is a $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$ such that $\Lambda_q(\mathbf{A}) = \Lambda_q^\perp(\mathbf{A}')$.
- The q -ary lattices associated to \mathbf{A} are dual (up to scaling)

$$\Lambda_q(\mathbf{A})^* = \frac{1}{q} \Lambda_q^\perp(\mathbf{A})$$

$$\Lambda_q^\perp(\mathbf{A})^* = \frac{1}{q} \Lambda_q(\mathbf{A})$$

LWE and q -ary lattices

- Learning with errors:
 - Input: $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{As} + \mathbf{e}$, where \mathbf{e} is small and \mathbf{s} is arbitrary
 - Output: \mathbf{s}, \mathbf{e}
- If $\mathbf{e} = \mathbf{0}$, then $\mathbf{As} + \mathbf{e} = \mathbf{As} \in \Lambda(\mathbf{A}^T)$
- Same as CVP in random q -ary lattice $\Lambda(\mathbf{A}^T)$ with random target $\mathbf{t} = \mathbf{As} + \mathbf{e}$
- Usually \mathbf{e} is shorter than $\frac{1}{2} \lambda_1(\Lambda(\mathbf{A}^T))$, and \mathbf{e} is uniquely determined

Ajtai's function and q -ary lattices

- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where \mathbf{x} is short
- The q -ary lattice $\Lambda_q^\perp(\mathbf{A})$ is the kernel of $f_{\mathbf{A}}$
- Finding collisions $f_{\mathbf{A}}(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{y})$ is equivalent to finding short vectors $\mathbf{x} - \mathbf{y} \in \Lambda_q^\perp(\mathbf{A})$
- The output of $f_{\mathbf{A}}(\mathbf{x})$ is the syndrome of \mathbf{x}
- Inverting $f_{\mathbf{A}}(\mathbf{x})$ is the same as CVP in its syndrome decoding formulation with lattice $\Lambda_q^\perp(\mathbf{A})$ and target $\mathbf{t} \in \mathbf{x} + \Lambda_q^\perp(\mathbf{A})$
- For $f_{\mathbf{A}}$ to be a compression function, \mathbf{x} is longer than $\frac{1}{2}\lambda_1(\Lambda_q^\perp(\mathbf{A}))$

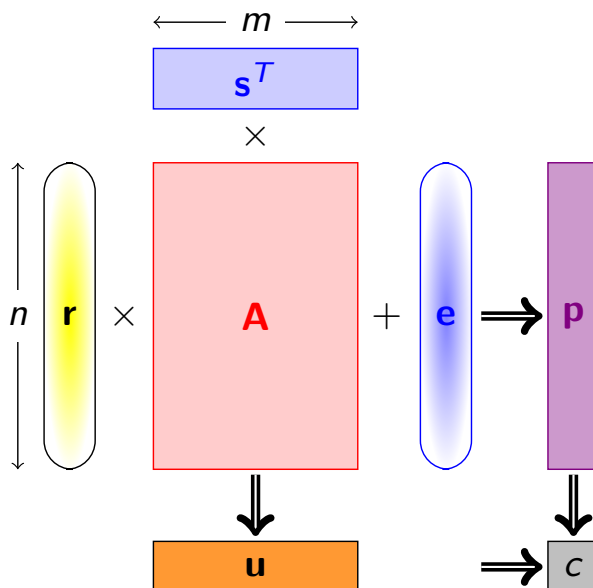
Duality of Ajtai's function and LWE

- Ajtai: $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{A}\mathbf{e} \bmod q$
- LWE: $g_{\mathbf{A}'}(\mathbf{s}, \mathbf{e}) = \mathbf{A}'\mathbf{s} + \mathbf{e} \bmod q$
- If $\Lambda_q^\perp(\mathbf{A}) = \Lambda_q((\mathbf{A}')^T) = \Lambda$
 - Inverting $f_{\mathbf{A}}(\mathbf{e})$ and inverting $g_{\mathbf{A}'}(\mathbf{s}, \mathbf{e})$ both describe the same CVP instance on lattice Λ and target $\mathbf{t} \in \mathbf{e} + \Lambda$
 - Inverting $f_{\mathbf{A}}(\mathbf{e})$ and inverting $g_{\mathbf{A}'}(\mathbf{s}, \mathbf{e})$ are equivalent problems, for appropriate choice of parameters
 - In Ajtai's and Regev's proofs, parameters are chosen differently

Ajtai vs Regev

- In Ajtai's function,
 - $\|\mathbf{e}\| \leq \beta$ is usually longer than covering radius of the lattice
 - A lattice point within distance β always exists
 - There are usually many such points
 - Finding any of them at least as hard as classic worst-case SIVP
 - Applications: Hashing, Signatures and a few more
- In LWE
 - $\|\mathbf{e}\| \leq \beta$ is usually smaller than packing radius of the lattice
 - A lattice point within distance β does not always exist
 - If it exists, it is unique
 - Finding any of them at least as hard as classic worst-case SIVP
 - Applications: PRG, PKE and much more

Regev (LWE) cryptosystem



- Parameters:
 $m, n, q \in \mathbb{Z}, \mathbf{A} \in \mathbb{Z}_q^{m \times n}$
- Secret key: $\mathbf{s} \in \mathbb{Z}_q^n, \mathbf{e} \in \mathcal{E}^m$
- Public key:
 $\mathbf{p} = \mathbf{A}\mathbf{s} + \mathbf{e} \approx_c \mathbb{Z}_q^m$
- $\text{Encrypt}_{\mathbf{p}}(0;(\mathbf{r})):$

$$\begin{aligned} \mathbf{u} &= \mathbf{r}^T \mathbf{A} \\ \mathbf{c} &= \mathbf{r}^T \mathbf{p} - r_0 \end{aligned}$$

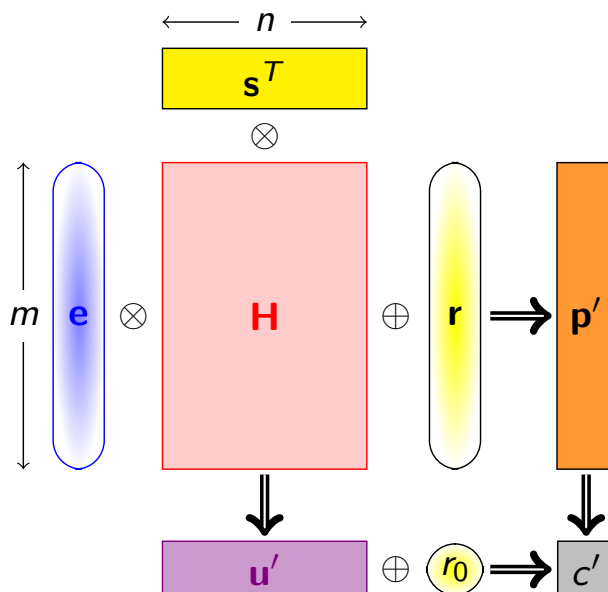
Regev's cryptosystem revisited

- Parameters: $m, n, q \in \mathbb{Z}, \mathbf{A} \in \mathbb{Z}_q^{m \times n}$
 - $\Lambda_q(\mathbf{A}^T) = \Lambda_q^\perp(\mathbf{H}^T)$ where $\mathbf{A}^T \mathbf{H} \equiv_q \mathbf{O}$.
- Public key: $\mathbf{p} = \mathbf{A}\mathbf{s} + \mathbf{e} \approx_c \mathbb{Z}_q^m$
 - $\mathbf{p} \in \Lambda_q(\mathbf{A}^T) + \mathbf{e}$
 - $\mathbf{u}' = (\mathbf{H}^T \mathbf{e})^T = \mathbf{e}^T \mathbf{H}$
- Encrypt $_{\mathbf{p}}(0; \mathbf{r})$: $(\mathbf{u}, c) = (\mathbf{r}^T \mathbf{A}, \mathbf{r}^T \mathbf{p} - r_0)$

$$\begin{bmatrix} \mathbf{u} \\ c \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{A}^T & \mathbf{0} \\ \mathbf{p}^T & -1 \end{bmatrix}}_{\mathbf{X}} \begin{bmatrix} \mathbf{r} \\ r_0 \end{bmatrix} \quad \begin{bmatrix} \mathbf{p}' \\ c' \end{bmatrix} \in \begin{bmatrix} \mathbf{r}^T \\ r_0 \end{bmatrix} + \Lambda_q(\mathbf{Y})$$

- $\Lambda_q^\perp(\mathbf{X}) = \Lambda_q(\mathbf{Y})$ where $\mathbf{Y} = [\mathbf{H}^T \mid (\mathbf{u}')^T]^T$
- $(\mathbf{p}', c') = (\mathbf{H}\mathbf{s} + \mathbf{r}, \mathbf{u}'\mathbf{s} + r_0)$

GPV cryptosystem revisited



- Parameters: $\mathbf{H} \in \mathbb{Z}_q^{m \times n}$
- Secret key: $\mathbf{e} \in \mathcal{E}^m$
- Public key: $\mathbf{u}' = \mathbf{e}^T \mathbf{H}$
- Encrypt $_{\mathbf{u}'}(m; \mathbf{r}, r_0)$:

$$\begin{aligned} \mathbf{p}' &= \mathbf{H}\mathbf{s} + \mathbf{r} \\ c' &= \mathbf{u}' \cdot \mathbf{s} + r_0 + m \end{aligned}$$

Equivalence of Regev's and GPV cryptosystems

Theorem

For appropriate choice of the parameters, Regev's cryptosystem and the GPV cryptosystem are equivalent

- The distribution of the secret key \mathbf{e} should be the same
- The distribution of the encryption randomness \mathbf{r} should be the same
- Message encoding m is also the same
- Common parameters $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{H} \in \mathbb{Z}_q^{k \times m}$ should satisfy $\Lambda_q(\mathbf{A}^T) = \Lambda_q^\perp(\mathbf{H})$

Hard random lattices

- Define the probability distributions over lattices

$$\begin{aligned} \mathcal{L}_q^\perp(n, m) &= \{\Lambda_q^\perp(\mathbf{H}) \mid \mathbf{H} \in \mathbb{Z}_q^{n \times m}\} \\ \mathcal{L}_q(k, m) &= \{\Lambda_q(\mathbf{A}) \mid \mathbf{A} \in \mathbb{Z}_q^{k \times m}\} \end{aligned}$$

Question

Are the distributions $\mathcal{L}_q^\perp(n, m)$ and $\mathcal{L}_q(k, m)$ the same?

- Answer: No.
- ... but the two distributions are the same if one conditions \mathbf{A} and \mathbf{H} to have full rank and sets $n + k = m$

Conclusion

- Cryptographic functions based on lattices can be described in terms of matrices, without reference to lattices at all
- This may look simple and attractive, but can also be misleading
- Lattice duality provides a powerful tool to better understand lattice based cryptographic constructions