The LWE problem from lattices to cryptography

Damien Stehlé

ENS de Lyon

Šibenik, June 2015

ENS DE LYON

What is a good problem, for a cryptographer?

- Almost all of its instances must be hard to solve.

  Attacks must be too expensive.

- Its instances must be easy to sample.

  The algorithms run by honest users should be efficient.

- The problem must be (algebraically) rich/expressive.

  So that interesting models of attacks can be handled, even for advanced cryptographic functionalities.

What is a good problem, for a cryptographer?

- Almost all of its instances must be hard to solve.

  Attacks must be too expensive.

- Its instances must be easy to sample.

  The algorithms run by honest users should be efficient.

- The problem must be (algebraically) rich/expressive.

  So that interesting models of attacks can be handled,
  even for advanced cryptographic functionalities.

What is a good problem, for a cryptographer?

- Almost all of its instances must be hard to solve.

  Attacks must be too expensive.

- Its instances must be easy to sample.

  The algorithms run by honest users should be efficient.

- The problem must be (algebraically) rich/expressive.

  So that interesting models of attacks can be handled,
  even for advanced cryptographic functionalities.

What is a good problem, for a cryptographer?

- Almost all of its instances must be hard to solve.

  Attacks must be too expensive.

- Its instances must be easy to sample.

  The algorithms run by honest users should be efficient.

- The problem must be (algebraically) rich/expressive.

  So that interesting models of attacks can be handled,
  even for advanced cryptographic functionalities.

The Learning With Errors problem

Informal definition

Solve a random system of m noisy linear equations and n unknowns modulo an integer q, with $m \gg n$.

- The best known algorithms are exponential in $n \log q$.
- Sampling an instance costs $\mathcal{O}(mn \log q)$.
  Very often, $m = \mathcal{O}(n \log q)$, so this is $\mathcal{O}((n \log q)^2)$.
- Very rich/expressive:
  encryption [Re05], ID-based encr. [GePeVa08], fully homomorphic encr. [BrVa11], attribute-based encr. [GoVaWe13], etc.

The Learning With Errors problem

Informal definition

Solve a random system of m noisy linear equations and n unknowns modulo an integer q, with $m \gg n$.

- The best known algorithms are exponential in $n \log q$.
- Sampling an instance costs $\mathcal{O}(mn \log q)$.
  Very often, $m = \mathcal{O}(n \log q)$, so this is $\mathcal{O}((n \log q)^2)$.
- Very rich/expressive:
  encryption [Re05], ID-based encr. [GePeVa08], fully homomorphic encr. [BrVa11], attribute-based encr. [GoVaWe13], etc.

The Learning With Errors problem

Informal definition

Solve a random system of m noisy linear equations and n unknowns modulo an integer q, with $m \gg n$.

- The best known algorithms are exponential in $n \log q$.
- Sampling an instance costs $\mathcal{O}(mn \log q)$.
  Very often, $m = \mathcal{O}(n \log q)$, so this is $\mathcal{O}((n \log q)^2)$.
- Very rich/expressive:
  encryption [Re05], ID-based encr. [GePeVa08], fully homomorphic encr. [BrVa11], attribute-based encr. [GoVaWe13], etc.

Goals of this talk

- Introduce LWE.
- Show the relationship between LWE and lattices.
- Use LWE to design a public-key encryption scheme.
- Give some open problems.

Road-map

- Definition of the LWE problem
- Regev's encryption scheme
- Lattice problems
- Hardness of LWE
- Equivalent problems

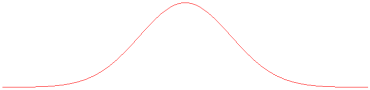
Road-map

- **Definition of the LWE problem**
- Regev's encryption scheme
- Lattice problems
- Hardness of LWE
- Equivalent problems

Gaussian distributions

Continuous Gaussian of parameter s:

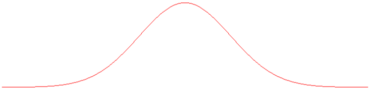
$D_s(x) \sim \frac{1}{s} \exp\left(-\pi \frac{x^2}{s^2}\right)$
$\forall x \in \mathbb{R}$



Gaussian distributions

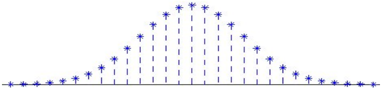
Continuous Gaussian of parameter s:

$$D_s(x) \sim \frac{1}{s}\exp\left(-\pi\frac{x^2}{s^2}\right)$$
$$\forall x \in \mathbb{R}$$



Discrete Gaussian of support $\mathbb{Z}$ and parameter s:

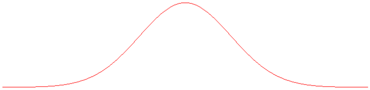
$$D_{\mathbb{Z},s}(x) \sim \frac{1}{s}\exp\left(-\pi\frac{x^2}{s^2}\right)$$
$$\forall x \in \mathbb{Z}$$



Gaussian distributions

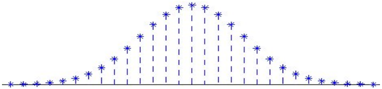
Continuous Gaussian of parameter s:

$$D_s(x) \sim \frac{1}{s}\exp\left(-\pi\frac{x^2}{s^2}\right)$$
$$\forall x \in \mathbb{R}$$



Discrete Gaussian of support $\mathbb{Z}$ and parameter s:

$$D_{\mathbb{Z},s}(x) \sim \frac{1}{s}\exp\left(-\pi\frac{x^2}{s^2}\right)$$
$$\forall x \in \mathbb{Z}$$



- That's not the rounding of a continuous Gaussian.
- One may efficiently sample from it.
- The usual tail bound holds.

The LWE problem [Re05]

Let $n \geq 1, q \geq 2$ and $\alpha \in (0,1)$.
For all $\mathbf{s} \in \mathbb{Z}_q^n$, we define the distribution $D_{n,q,\alpha}(\mathbf{s})$:

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \text{ with } \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \text{ and } e \hookleftarrow D_{\mathbb{Z},\alpha q}.$$

Search LWE

For all $\mathbf{s}$: Given arbitrarily many samples from $D_{n,q,\alpha}(\mathbf{s})$, find $\mathbf{s}$.

(Information-theoretically, $\approx n \frac{\log q}{\log 1/\alpha}$ samples uniquely determine $\mathbf{s}$.)

Decision LWE

With non-negligible probability over $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$:
distinguish between the distributions $D_{n,q,\alpha}(\mathbf{s})$ and $U(\mathbb{Z}_q^{n+1})$.

(Non-negligible: $1/(n \log q)^c$ for some constant $c > 0$.)

The LWE problem [Re05]

Let $n \geq 1$, $q \geq 2$ and $\alpha \in (0,1)$.
For all $\mathbf{s} \in \mathbb{Z}_q^n$, we define the distribution $D_{n,q,\alpha}(\mathbf{s})$:

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \text{ with } \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \text{ and } e \hookleftarrow D_{\mathbb{Z},\alpha q}.$$

Search LWE

For all $\mathbf{s}$: Given arbitrarily many samples from $D_{n,q,\alpha}(\mathbf{s})$, find $\mathbf{s}$.

(Information-theoretically, $\approx n \frac{\log q}{\log 1/\alpha}$ samples uniquely determine $\mathbf{s}$.)

Decision LWE

With non-negligible probability over $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$:
distinguish between the distributions $D_{n,q,\alpha}(\mathbf{s})$ and $U(\mathbb{Z}_q^{n+1})$.

(Non-negligible: $1/(n \log q)^c$ for some constant $c > 0$.)

The LWE problem [Re05]

Let $n \geq 1$, $q \geq 2$ and $\alpha \in (0,1)$.
For all $\mathbf{s} \in \mathbb{Z}_q^n$, we define the distribution $D_{n,q,\alpha}(\mathbf{s})$:

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \text{ with } \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \text{ and } e \hookleftarrow D_{\mathbb{Z},\alpha q}.$$

Search LWE

For all $\mathbf{s}$: Given arbitrarily many samples from $D_{n,q,\alpha}(\mathbf{s})$, find $\mathbf{s}$.

(Information-theoretically, $\approx n\frac{\log q}{\log 1/\alpha}$ samples uniquely determine $\mathbf{s}$.)

Decision LWE

With non-negligible probability over $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$:
distinguish between the distributions $D_{n,q,\alpha}(\mathbf{s})$ and $U(\mathbb{Z}_q^{n+1})$.

(Non-negligible: $1/(n \log q)^c$ for some constant $c > 0$.)

Decision LWE

Let $n \geq 1, q \geq 2$ and $\alpha \in (0,1)$.
For all $\mathbf{s} \in \mathbb{Z}_q^n$, we define the distribution $D_{n,q,\alpha}(\mathbf{s})$:

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e), \text{ with } \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \text{ and } e \hookleftarrow D_{\mathbb{Z},\alpha q}.$$

Decision LWE

With non-negligible probability over $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$:
distinguish between the distributions $D_{n,q,\alpha}(\mathbf{s})$ and $U(\mathbb{Z}_q^{n+1})$.

We are given an oracle $\mathcal{O}$ that produces independent samples from always the same distribution, which is:

- either $D_{n,q,\alpha}(\mathbf{s})$ for a fixed $\mathbf{s}$,
- or $U(\mathbb{Z}_q^{n+1})$.

We have to tell which, with probability $\geq \frac{1}{2} + \frac{1}{(n \log q)^{\Omega(1)}}$.

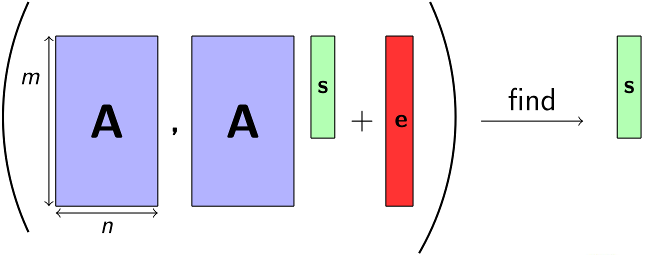
Search LWE $\equiv$ solving noisy linear systems

Find $s_1, s_2, s_3, s_4, s_5 \in \mathbb{Z}_{23}$ such that:

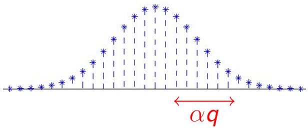
$$\begin{aligned}
s_1 + 22s_2 + 17s_3 + 2s_4 + s_5 &\approx 16 \mod 23 \\
3s_1 + 2s_2 + 11s_3 + 7s_4 + 8s_5 &\approx 17 \mod 23 \\
15s_1 + 13s_2 + 10s_3 + s_4 + 22s_5 &\approx 3 \mod 23 \\
17s_1 + 11s_2 + s_3 + 10s_4 + 3s_5 &\approx 8 \mod 23 \\
2s_1 + s_2 + 13s_3 + 6s_4 + 2s_5 &\approx 9 \mod 23 \\
4s_1 + 4s_2 + s_3 + 5s_4 + s_5 &\approx 18 \mod 23 \\
11s_1 + 12s_2 + 5s_3 + s_4 + 9s_5 &\approx 7 \mod 23
\end{aligned}$$

We can even ask for arbitrarily many noisy equations.

Matrix version of LWE



- $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$,
- $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^{n})$,
- $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.



Discrete Gaussian error

Decision LWE:

Determine whether $(\mathbf{A}, \mathbf{b})$ is of the form above, or uniform.

Some simple remarks

- If $\alpha \approx 0$, LWE is easy to solve.
- If $\alpha \approx 1$, LWE is trivially hard.
- Very often, we are interested in

$$\alpha \approx \frac{1}{n^c}, \ q \approx n^{c'}, \quad \text{for some constants } c' > c > 0.$$

- Why a discrete Gaussian noise?

Why is LWE interesting for crypto?

- LWE is just noisy linear algebra: Easy to use, expressive.
- LWE seems to be a (very) hard problem.

Two particularly useful properties:

- Unlimited number of samples.
- Random self-reducibility over **s**.

If q is prime and $\leq n^{\mathcal{O}(1)}$, there are polynomial-time reductions between the Search and Decision versions of LWE [Re05].

(We may remove these assumptions, if we allow some polynomial blow-up on α.)

Why is LWE interesting for crypto?

- LWE is just noisy linear algebra: Easy to use, expressive.
- LWE seems to be a (very) hard problem.

Two particularly useful properties:

- Unlimited number of samples.
- Random self-reducibility over **s**.

If q is prime and $\leq n^{\mathcal{O}(1)}$, there are polynomial-time reductions between the Search and Decision versions of LWE [Re05].

(We may remove these assumptions, if we allow some polynomial blow-up on α.)

Road-map

- Definition of the LWE problem
- **Regev's encryption scheme**
- Lattice problems
- Hardness of LWE
- Equivalent problems

Public-key encryption

A public-key encryption scheme over $\{0,1\} \times \mathcal{C}$ consists in three algorithms:

- $\textsc{KeyGen}$: Security parameter $\mapsto (pk, sk)$.
- $\textsc{Enc}$: $(pk, M) \mapsto C \in \mathcal{C}$.
- $\textsc{Dec}$: $(sk, C) \mapsto M' \in \{0,1\}$.

Correctness

With probability ≈ 1, $\forall M \in \{0,1\}$: $\textsc{Dec}_{sk}(\textsc{Enc}_{pk}(M)) = M$.

Security (IND-CPA)

The distributions of $(pk, \textsc{Enc}_{pk}(0))$ and $(pk, \textsc{Enc}_{pk}(1))$ must be **computationally indistinguishable**.

Public-key encryption

A public-key encryption scheme over $\{0,1\} \times \mathcal{C}$ consists in three algorithms:

- $\textsc{KeyGen}$: Security parameter $\mapsto (pk, sk)$.
- $\textsc{Enc}$: $(pk, M) \mapsto C \in \mathcal{C}$.
- $\textsc{Dec}$: $(sk, C) \mapsto M' \in \{0,1\}$.

Correctness

With probability ≈ 1, $\forall M \in \{0,1\}$: $\textsc{Dec}_{sk}(\textsc{Enc}_{pk}(M)) = M$.

Security (IND-CPA)

The distributions of $(pk, \textsc{Enc}_{pk}(0))$ and $(pk, \textsc{Enc}_{pk}(1))$ must be **computationally indistinguishable**.

Public-key encryption

A public-key encryption scheme over $\{0,1\} \times \mathcal{C}$ consists in three algorithms:

- $\textsc{KeyGen}$: Security parameter $\mapsto (pk, sk)$.
- $\textsc{Enc}$: $(pk, M) \mapsto C \in \mathcal{C}$.
- $\textsc{Dec}$: $(sk, C) \mapsto M' \in \{0,1\}$.

Correctness

With probability ≈ 1, $\forall M \in \{0,1\}$: $\textsc{Dec}_{sk}(\textsc{Enc}_{pk}(M)) = M$.

Security (IND-CPA)

The distributions of $(pk, \textsc{Enc}_{pk}(0))$ and $(pk, \textsc{Enc}_{pk}(1))$ must be **computationally indistinguishable**.

Regev's encryption scheme

- **Parameters**: n, m, q, α.
- **Keys**: $\mathrm{sk} = \mathbf{s}$ and $\mathrm{pk} = (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$
- **ENC**$(M \in \{0,1\})$**:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rfloor \cdot M.$$

- **DEC**$(\mathbf{u}, v)$: Compute $v - \mathbf{u}^T \mathbf{s}$ (modulo q).

$$\mathbf{r}^T \left[\mathbf{A}\mathbf{s} + \mathbf{e} \right] + \lfloor q/2 \rfloor \cdot M - \mathbf{r}^T \mathbf{A}\mathbf{s} = \text{small} + \lfloor q/2 \rfloor \cdot M$$

If it's close to 0, output 0, else output 1.

Regev's encryption scheme

- **Parameters**: n, m, q, α.
- **Keys**: sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$
- **ENC**$(M \in \{0,1\})$**:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rfloor \cdot M.$$

- **DEC**$(\mathbf{u}, v)$: Compute $v - \mathbf{u}^T\mathbf{s}$ (modulo q).

$$\mathbf{r}^T \left[\mathbf{A}\mathbf{s} + \mathbf{e} \right] + \lfloor q/2 \rfloor \cdot M - \mathbf{r}^T \mathbf{A} \mathbf{s} = \text{small} + \lfloor q/2 \rfloor \cdot M$$

If it's close to 0, output 0, else output 1.

Decryption correctness

Correctness

Assume that $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$.
Then, with probability $\geq 1 - n^{-\omega(1)}$, it correctly decrypts.

We have

$$v - \mathbf{u}^T \mathbf{s} \; = \; \mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M \mod q.$$

As $\mathbf{e} \sim D^m_{\mathbb{Z},\alpha q}$, we expect $\langle \mathbf{r}, \mathbf{e} \rangle$ to behave like $D_{\|\mathbf{r}\|\alpha q}$.

As $\|\mathbf{r}\| \leq \sqrt{m}$, we have $\|\mathbf{r}\|\alpha q \leq o(\frac{q}{\sqrt{\log n}})$, and
a sample from $D_{\|\mathbf{r}\|\alpha q}$ is $< q/8$ with probability $\geq 1 - n^{-\omega(1)}$.

Decryption correctness

Correctness

Assume that $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$.
Then, with probability $\geq 1 - n^{-\omega(1)}$, it correctly decrypts.

We have

$$v - \mathbf{u}^T \mathbf{s} \; = \; \mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M \quad \bmod q.$$

As $\mathbf{e} \sim D^m_{\mathbb{Z},\alpha q}$, we expect $\langle \mathbf{r}, \mathbf{e} \rangle$ to behave like $D_{\|\mathbf{r}\|\alpha q}$.

As $\|\mathbf{r}\| \leq \sqrt{m}$, we have $\|\mathbf{r}\|\alpha q \leq o(\frac{q}{\sqrt{\log n}})$, and
a sample from $D_{\|\mathbf{r}\|\alpha q}$ is $< q/8$ with probability $\geq 1 - n^{-\omega(1)}$.

$\Rightarrow$ We know $\mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M$ over the integers.

Decryption correctness

Correctness

Assume that $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$.
Then, with probability $\geq 1 - n^{-\omega(1)}$, it correctly decrypts.

We have

$$v - \mathbf{u}^T \mathbf{s} \; = \; \mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M \mod q.$$

As $\mathbf{e} \sim D^m_{\mathbb{Z},\alpha q}$, we expect $\langle \mathbf{r}, \mathbf{e} \rangle$ to behave like $D_{\|\mathbf{r}\|\alpha q}$.

As $\|\mathbf{r}\| \leq \sqrt{m}$, we have $\|\mathbf{r}\|\alpha q \leq o(\frac{q}{\sqrt{\log n}})$, and
a sample from $D_{\|\mathbf{r}\|\alpha q}$ is $< q/8$ with probability $\geq 1 - n^{-\omega(1)}$.

$\Rightarrow$ We know $\mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M$ over the integers.

Decryption correctness

Correctness

Assume that $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$.
Then, with probability $\geq 1 - n^{-\omega(1)}$, it correctly decrypts.

We have

$$v - \mathbf{u}^T \mathbf{s} \; = \; \mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M \mod q.$$

As $\mathbf{e} \sim D^m_{\mathbb{Z},\alpha q}$, we expect $\langle \mathbf{r}, \mathbf{e} \rangle$ to behave like $D_{\|\mathbf{r}\|\alpha q}$.

As $\|\mathbf{r}\| \leq \sqrt{m}$, we have $\|\mathbf{r}\|\alpha q \leq o(\frac{q}{\sqrt{\log n}})$, and
a sample from $D_{\|\mathbf{r}\|\alpha q}$ is $< q/8$ with probability $\geq 1 - n^{-\omega(1)}$.

$\Rightarrow$ We know $\mathbf{r}^T \mathbf{e} + \lfloor q/2 \rfloor M$ over the integers.

IND-CPA Security

Security

Assume that $m = \Omega(n \log q)$. Then any (IND-CPA) attacker may be turned into an algorithm for $\mathrm{LWE}_{n,q,\alpha}$.

Fake security experiment

Challenger uses and gives to the attacker a uniform pair $(\mathbf{A}, \mathbf{b})$ (instead of $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$).

1. If attacker behaves differently than in real security experiment, it can be used to solve LWE.

IND-CPA Security

Security

Assume that $m = \Omega(n \log q)$. Then any (IND-CPA) attacker may be turned into an algorithm for $\mathrm{LWE}_{n,q,\alpha}$.

Fake security experiment

Challenger uses and gives to the attacker a uniform pair $(\mathbf{A}, \mathbf{b})$ (instead of $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$).

1. If attacker behaves differently than in real security experiment, it can be used to solve LWE.
2. In fake experiment, $(\mathbf{A}, \mathbf{b}, \mathbf{r}^T\mathbf{A}, \mathbf{r}^T\mathbf{b})$ is $\approx$ uniform, hence $\textsc{Enc}(0)$ and $\textsc{Enc}(1)$ follow ($\approx$) the same distribution.

IND-CPA Security

Security

Assume that $m = \Omega(n \log q)$. Then any (IND-CPA) attacker may be turned into an algorithm for $\mathrm{LWE}_{n,q,\alpha}$.

Fake security experiment

Challenger uses and gives to the attacker a uniform pair $(\mathbf{A}, \mathbf{b})$ (instead of $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$).

1. If attacker behaves differently than in real security experiment, it can be used to solve LWE.
2. In fake experiment, $(\mathbf{A}, \mathbf{b}, \mathbf{r}^T\mathbf{A}, \mathbf{r}^T\mathbf{b})$ is $\approx$ uniform, hence $\textsc{Enc}(0)$ and $\textsc{Enc}(1)$ follow ($\approx$) the same distribution.

IND-CPA Security

Security

Assume that $m = \Omega(n \log q)$. Then any (IND-CPA) attacker may be turned into an algorithm for $\mathrm{LWE}_{n,q,\alpha}$.

Fake security experiment

Challenger uses and gives to the attacker a uniform pair $(\mathbf{A}, \mathbf{b})$ (instead of $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$).

1. If attacker behaves differently than in real security experiment, it can be used to solve LWE.
2. In fake experiment, $(\mathbf{A}, \mathbf{b}, \mathbf{r}^T\mathbf{A}, \mathbf{r}^T\mathbf{b})$ is $\approx$ uniform, hence $\textsc{Enc}(0)$ and $\textsc{Enc}(1)$ follow ($\approx$) the same distribution.

Setting the parameters: n, m, α, q

- Correctness: $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$
- Reducing LWE to IND-CPA security: $m \geq \Omega(n \log q)$

1. Set α as large as possible (α impacts security)
2. Set m as small as possible (m impacts efficiency)
3. Set n and q so that $\mathrm{LWE}_{n,q,\alpha}$ is sufficiently hard to solve

Here: $\alpha = \widetilde{\Theta}(\sqrt{n})$, $m = \widetilde{\Theta}(n)$ and $q = \widetilde{\Theta}(n)$.

This is not very practical... ciphertext expansion: $\widetilde{\Theta}(n)$.

Setting the parameters: n, m, α, q

- Correctness: $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$
- Reducing LWE to IND-CPA security: $m \geq \Omega(n \log q)$

1. Set α as large as possible (α impacts security)
2. Set m as small as possible (m impacts efficiency)
3. Set n and q so that $\mathrm{LWE}_{n,q,\alpha}$ is sufficiently hard to solve

Here: $\alpha = \widetilde{\Theta}(\sqrt{n})$, $m = \widetilde{\Theta}(n)$ and $q = \widetilde{\Theta}(n)$.

This is not very practical... ciphertext expansion: $\widetilde{\Theta}(n)$.

Setting the parameters: n, m, α, q

- Correctness: $\alpha \leq o(\frac{1}{\sqrt{m \log n}})$
- Reducing LWE to IND-CPA security: $m \geq \Omega(n \log q)$

1. Set α as large as possible (α impacts security)
2. Set m as small as possible (m impacts efficiency)
3. Set n and q so that $\mathrm{LWE}_{n,q,\alpha}$ is sufficiently hard to solve

Here: $\alpha = \widetilde{\Theta}(\sqrt{n})$, $m = \widetilde{\Theta}(n)$ and $q = \widetilde{\Theta}(n)$.

This is not very practical... ciphertext expansion: $\widetilde{\Theta}(n)$.

Multi-bit Regev

- **Parameters**: n, m, q, α, ℓ.
- **Keys**: sk $= \mathbf{S} \in \mathbb{Z}_q^{n\times\ell}$ and pk $= (\mathbf{A}, \mathbf{B})$, with $\mathbf{B} = \mathbf{A}\mathbf{S} + \mathbf{E}$
- **ENC**$(\mathbf{M} \in \{0,1\}^\ell)$**:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad \mathbf{v}^T = \mathbf{r}^T \mathbf{B} + \lfloor q/2 \rfloor \cdot \mathbf{M}^T.$$

- **DEC**$(\mathbf{u}, \mathbf{v})$: Compute $\mathbf{v}^T - \mathbf{u}^T\mathbf{S}$ (modulo q).

Asymptotic performance, for $\ell = n$

- Ciphertext expansion: $\widetilde{\Theta}(1)$
- Processing time: $\widetilde{\Theta}(n)$ per message bit
- Key size: $\widetilde{\Theta}(n^2)$

Multi-bit Regev

- **Parameters**: n, m, q, α, ℓ.
- **Keys**: sk $=$ $\mathbf{S} \in \mathbb{Z}_q^{n \times \ell}$ and pk $= (\mathbf{A}, \mathbf{B})$, with $\mathbf{B} = \mathbf{A}\mathbf{S} + \mathbf{E}$
- **ENC($\mathbf{M} \in \{0,1\}^\ell$):** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad \mathbf{v}^T = \mathbf{r}^T \mathbf{B} + \lfloor q/2 \rfloor \cdot \mathbf{M}^T.$$

- **DEC($\mathbf{u}, \mathbf{v}$)**: Compute $\mathbf{v}^T - \mathbf{u}^T\mathbf{S}$ (modulo q).

Asymptotic performance, for $\ell = n$

- Ciphertext expansion: $\widetilde{\Theta}(1)$
- Processing time: $\widetilde{\Theta}(n)$ per message bit
- Key size: $\widetilde{\Theta}(n^2)$

More on Regev's encryption

- This scheme is homomorphic for addition: add ciphertexts
- IAnd also for multiplication: tensor ciphertexts

⇒ Can be turned into FHE [Br12]

- Enc and KeyGen may be swapped: dual-Regev [GePeVa08]

⇒ This allows ID-based encryption, and more

May be turned into a practical scheme [Pe14]

- Use Ring-LWE rather than LWE: more efficient
- Ciphertext expansion can be lowered to essentially 1
- IND-CCA security can be achieved efficiently in the ROM

More on Regev's encryption

- This scheme is homomorphic for addition: add ciphertexts
- IAnd also for multiplication: tensor ciphertexts

$\Rightarrow$ Can be turned into FHE [Br12]

- Enc and KeyGen may be swapped: dual-Regev [GePeVa08]

$\Rightarrow$ This allows ID-based encryption, and more

May be turned into a practical scheme [Pe14]

- Use Ring-LWE rather than LWE: more efficient
- Ciphertext expansion can be lowered to essentially 1
- IND-CCA security can be achieved efficiently in the ROM

More on Regev's encryption

- This scheme is homomorphic for addition: add ciphertexts
- IAnd also for multiplication: tensor ciphertexts

$\Rightarrow$ Can be turned into FHE [Br12]

- Enc and KeyGen may be swapped: dual-Regev [GePeVa08]

$\Rightarrow$ This allows ID-based encryption, and more

May be turned into a practical scheme [Pe14]

- Use Ring-LWE rather than LWE: more efficient
- Ciphertext expansion can be lowered to essentially 1
- IND-CCA security can be achieved efficiently in the ROM

Road-map

- Definition of the LWE problem
- Regev's encryption scheme
- **Lattice problems**
- Hardness of LWE
- Equivalent problems

Euclidean lattices

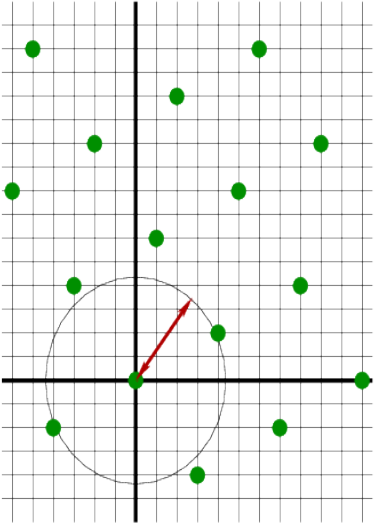
Lattice $L = \sum_{i=1}^{n} \mathbb{Z}\mathbf{b}_i \ \subset \mathbb{R}^n$,

for some linearly indep. $\mathbf{b}_i$'s.

Minimum $\lambda(L) = \min\left(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0}\right)$.

SVP$_\gamma$: Given as input a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

BDD$_\gamma$: Given as input a basis of L, and a vector $\mathbf{t}$ s.t. $\mathrm{dist}(\mathbf{t}, L) < \frac{1}{2\gamma} \cdot \lambda(L)$, find $\mathbf{b} \in L$ minimizing $\|\mathbf{b} - \mathbf{t}\|$.



Euclidean lattices

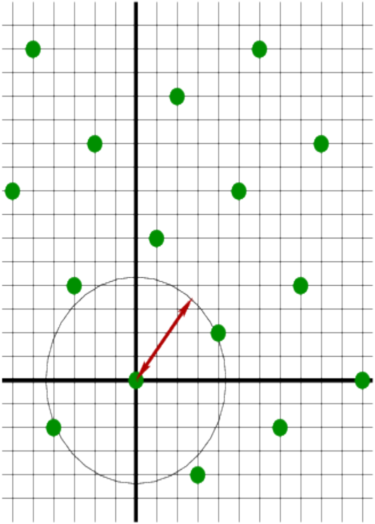
Lattice $L = \sum_{i=1}^{n} \mathbb{Z}\mathbf{b}_i \subset \mathbb{R}^n$,

for some linearly indep. $\mathbf{b}_i$'s.

Minimum $\lambda(L) = \min\left(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0}\right)$.

SVP$_\gamma$: Given as input a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

BDD$_\gamma$: Given as input a basis of L, and a vector $\mathbf{t}$ s.t. $\mathrm{dist}(\mathbf{t}, L) < \frac{1}{2\gamma} \cdot \lambda(L)$, find $\mathbf{b} \in L$ minimizing $\|\mathbf{b} - \mathbf{t}\|$.



Euclidean lattices

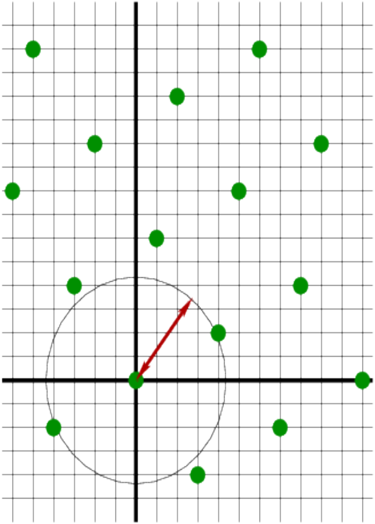
Lattice $L = \sum_{i=1}^{n} \mathbb{Z}\mathbf{b}_i \subset \mathbb{R}^n$,

for some linearly indep. $\mathbf{b}_i$'s.

Minimum $\lambda(L) = \min\left(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0}\right)$.

SVP$_\gamma$: Given as input a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

BDD$_\gamma$: Given as input a basis of L, and a vector $\mathbf{t}$ s.t. $\mathrm{dist}(\mathbf{t}, L) < \frac{1}{2\gamma} \cdot \lambda(L)$, find $\mathbf{b} \in L$ minimizing $\|\mathbf{b} - \mathbf{t}\|$.



Best known (classical/quantum) algorithms

SVP$_\gamma$: Given L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.
BDD$_\gamma$: Given L and $\mathbf{t} \in \mathbb{R}^n$ s.t. $\mathrm{dist}(\mathbf{t}, L) < \frac{1}{2\gamma} \cdot \lambda(L)$,
find $\mathbf{b} \in L$ minimizing $\|\mathbf{b} - \mathbf{t}\|$.

For small γ: [AgDaReSD15]

- Time $2^{n/2}$.
- In practice: up to $n \approx 120$ (with other algorithms).

For $\gamma = n^{\Omega(1)}$: BKZ [ScEu91,HaPuSt11]

- Time $\left(\frac{n}{\log \gamma}\right)^{\mathcal{O}\left(\frac{n}{\log \gamma}\right)}$.
- In practice, we can reach $\gamma \approx 1.01^n$ [ChNg11].

`https://github.com/dstehle/fplll`

Best known (classical/quantum) algorithms

SVP$_\gamma$: Given L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.
BDD$_\gamma$: Given L and $\mathbf{t} \in \mathbb{R}^n$ s.t. $\mathrm{dist}(\mathbf{t}, L) < \frac{1}{2\gamma} \cdot \lambda(L)$,
find $\mathbf{b} \in L$ minimizing $\|\mathbf{b} - \mathbf{t}\|$.

For small γ: [AgDaReSD15]

- Time $2^{n/2}$.
- In practice: up to $n \approx 120$ (with other algorithms).

For $\gamma = n^{\Omega(1)}$: BKZ [ScEu91,HaPuSt11]

- Time $\left(\frac{n}{\log \gamma}\right)^{\mathcal{O}\left(\frac{n}{\log \gamma}\right)}$.
- In practice, we can reach $\gamma \approx 1.01^n$ [ChNg11].

https://github.com/dstehle/fplll

Best known (classical/quantum) algorithms

SVP$_\gamma$: Given L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.
BDD$_\gamma$: Given L and $\mathbf{t} \in \mathbb{R}^n$ s.t. $\mathrm{dist}(\mathbf{t}, L) < \frac{1}{2\gamma} \cdot \lambda(L)$,
find $\mathbf{b} \in L$ minimizing $\|\mathbf{b} - \mathbf{t}\|$.

For small γ: [AgDaReSD15]

- Time $2^{n/2}$.
- In practice: up to $n \approx 120$ (with other algorithms).

For $\gamma = n^{\Omega(1)}$: BKZ [ScEu91,HaPuSt11]

- Time $\left(\frac{n}{\log \gamma}\right)^{\mathcal{O}\left(\frac{n}{\log \gamma}\right)}$.
- In practice, we can reach $\gamma \approx 1.01^n$ [ChNg11].

https://github.com/dstehle/fplll

Hardness of SVP

GapSVP$_\gamma$

Given a basis of a lattice L and $d > 0$, assess whether

$$\lambda(L) \leq d \quad \text{or} \quad \lambda(L) > \gamma \cdot d.$$

- **NP-hard** when $\gamma \leq \mathcal{O}(1)$ (random. red.) [Aj98,HaRe07]
- **In NP$\cap$coNP** when $\gamma \geq \sqrt{n}$ [GoGo98,AhRe04]
- **In P** when $\gamma \geq \exp\left(n \cdot \frac{\log \log n}{\log n}\right)$ (BKZ)

Hardness of SVP

GapSVP_γ

Given a basis of a lattice L and $d > 0$, assess whether

$$\lambda(L) \leq d \quad \text{or} \quad \lambda(L) > \gamma \cdot d.$$

- **NP-hard** when $\gamma \leq \mathcal{O}(1)$ (random. red.) [Aj98,HaRe07]
- **In NP∩coNP** when $\gamma \geq \sqrt{n}$ [GoGo98,AhRe04]
- **In P** when $\gamma \geq \exp\left(n \cdot \frac{\log \log n}{\log n}\right)$ (BKZ)

Road-map

- Definition of the LWE problem
- Regev's encryption scheme
- Lattice problems
- **Hardness of LWE**
- Equivalent problems

Each LWE sample gives $\approx \log_2 \frac{1}{\alpha}$ bits of data on secret $\mathbf{s}$.

With a few samples, $\mathbf{s}$ is uniquely specified. How to find it?

Exhaustive search

Assume we are given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, for some $\mathbf{e}$ whose entries are $\approx \alpha q$.
We want to find $\mathbf{s}$.

1st variant:

- Try all the possible $\mathbf{s} \in \mathbb{Z}_q^n$.
- Test if $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ is small.

$\Rightarrow$ Cost $\approx q^n$.

2nd variant:

- Try all the possible n first error terms.
- Recover the corresponding $\mathbf{s}$, by linear algebra.
- Test if $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ is small.

$\Rightarrow$ Cost $\approx (\alpha q \sqrt{\log n})^n$.

Exhaustive search

Assume we are given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, for some $\mathbf{e}$ whose entries are $\approx \alpha q$.
We want to find $\mathbf{s}$.

1st variant:

- Try all the possible $\mathbf{s} \in \mathbb{Z}_q^n$.
- Test if $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ is small.

$\Rightarrow$ Cost $\approx q^n$.

2nd variant:

- Try all the possible n first error terms.
- Recover the corresponding $\mathbf{s}$, by linear algebra.
- Test if $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ is small.

$\Rightarrow$ Cost $\approx (\alpha q \sqrt{\log n})^n$.

Solving LWE with BKZ (1/2)

Assume we are given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, for some $\mathbf{e}$ whose entries are $\approx \alpha q$.
We want to find $\mathbf{s}$.

Let $\quad L_{\mathbf{A}} = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n, \mathbf{x} = \mathbf{A}\mathbf{s} \ [q]\} \ = \ \mathbf{A}\mathbb{Z}_q^n + q\mathbb{Z}^m.$

- $L_{\mathbf{A}}$ is a lattice of dimension m.
- Whp, its minimum satisfies $\lambda(L) \approx \sqrt{m} \cdot q^{1-\frac{n}{m}}$.
- We have $\mathrm{dist}(\mathbf{b}, L) = \|\mathbf{e}\| \approx \sqrt{m}\alpha q$.

LWE reduces to BDD

This is a BDD instance in dim m with $\gamma \approx q^{-\frac{n}{m}}/\alpha$.

Solving LWE with BKZ (1/2)

Assume we are given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, for some $\mathbf{e}$ whose entries are $\approx \alpha q$.
We want to find $\mathbf{s}$.

Let $L_{\mathbf{A}} = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n, \mathbf{x} = \mathbf{A}\mathbf{s}\ [q]\} = \mathbf{A}\mathbb{Z}_q^n + q\mathbb{Z}^m$.

- $L_{\mathbf{A}}$ is a lattice of dimension m.
- Whp, its minimum satisfies $\lambda(L) \approx \sqrt{m} \cdot q^{1-\frac{n}{m}}$.
- We have $\mathrm{dist}(\mathbf{b}, L) = \|\mathbf{e}\| \approx \sqrt{m}\alpha q$.

LWE reduces to BDD

This is a BDD instance in dim m with $\gamma \approx q^{-\frac{n}{m}}/\alpha$.

Solving LWE with BKZ (1/2)

Assume we are given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, for some $\mathbf{e}$ whose entries are $\approx \alpha q$.
We want to find $\mathbf{s}$.

Let $L_{\mathbf{A}} = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n, \mathbf{x} = \mathbf{A}\mathbf{s}\ [q]\} \ = \ \mathbf{A}\mathbb{Z}_q^n + q\mathbb{Z}^m$.

- $L_{\mathbf{A}}$ is a lattice of dimension m.
- Whp, its minimum satisfies $\lambda(L) \approx \sqrt{m} \cdot q^{1-\frac{n}{m}}$.
- We have $\mathrm{dist}(\mathbf{b}, L) = \|\mathbf{e}\| \approx \sqrt{m}\alpha q$.

LWE reduces to BDD

This is a BDD instance in dim m with $\gamma \approx q^{-\frac{n}{m}}/\alpha$.

Solving LWE with BKZ (1/2)

Assume we are given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, for some $\mathbf{e}$ whose entries are $\approx \alpha q$.
We want to find $\mathbf{s}$.

$$\text{Let} \quad L_{\mathbf{A}} = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n, \mathbf{x} = \mathbf{A}\mathbf{s}\ [q]\} \ = \ \mathbf{A}\mathbb{Z}_q^n + q\mathbb{Z}^m.$$

- $L_{\mathbf{A}}$ is a lattice of dimension m.
- Whp, its minimum satisfies $\lambda(L) \approx \sqrt{m} \cdot q^{1-\frac{n}{m}}$.
- We have $\mathrm{dist}(\mathbf{b}, L) = \|\mathbf{e}\| \approx \sqrt{m}\alpha q$.

LWE reduces to BDD

This is a BDD instance in dim m with $\gamma \approx q^{-\frac{n}{m}}/\alpha$.

Solving LWE with BKZ (2/2)

LWE reduces to BDD

This is a BDD instance in dim m with $\gamma \approx q^{-\frac{n}{m}}/\alpha$.

Cost of BKZ: $\left(\frac{m}{\log\gamma}\right)^{\mathcal{O}\left(\frac{m}{\log\gamma}\right)}$, with $\frac{\log\gamma}{m} = \frac{1}{m}\log\frac{1}{\alpha} - \frac{n\log q}{m^2}$.

Cost is minimized for $m \approx \frac{2n\log q}{\log\frac{1}{\alpha}}$.

Cost of BKZ to solve LWE

$$\text{Time: } \left(\frac{n\log q}{\log^2\alpha}\right)^{\mathcal{O}\left(\frac{n\log q}{\log^2\alpha}\right)}.$$

Solving LWE with BKZ (2/2)

LWE reduces to BDD

This is a BDD instance in dim m with $\gamma \approx q^{-\frac{n}{m}}/\alpha$.

Cost of BKZ: $(\frac{m}{\log\gamma})^{\mathcal{O}(\frac{m}{\log\gamma})}$, with $\frac{\log\gamma}{m} = \frac{1}{m}\log\frac{1}{\alpha} - \frac{n\log q}{m^2}$.

Cost is minimized for $m \approx \frac{2n\log q}{\log\frac{1}{\alpha}}$.

Cost of BKZ to solve LWE

$$\text{Time: } \left(\frac{n\log q}{\log^2\alpha}\right)^{\mathcal{O}\left(\frac{n\log q}{\log^2\alpha}\right)}.$$

Hardness results on LWE

Assume that $\alpha q \geq 2\sqrt{n}$.

[Re05]

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP**$_\gamma$ in **dim** n to LWE$_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

[BrLaPeReSt13]

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP**$_\gamma$ in **dim** $\sqrt{n}$ to LWE$_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- The two results are incomparable.
- Best achievable γ here: n.
- In the case of Regev's encryption, we get $\gamma \approx n^{3/2}$.
- One can use BDD$_\gamma$ instead (with a different γ).

Hardness results on LWE

Assume that $\alpha q \geq 2\sqrt{n}$.

[Re05]

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP$_\gamma$** in **dim** n to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

[BrLaPeReSt13]

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP$_\gamma$** in **dim** $\sqrt{n}$ to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- The two results are incomparable.
- Best achievable γ here: n.
- In the case of Regev's encryption, we get $\gamma \approx n^{3/2}$.
- One can use BDD_γ instead (with a different γ).

Hardness results on LWE

Assume that $\alpha q \geq 2\sqrt{n}$.

[Re05]

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP**$_\gamma$ in **dim** n to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

[BrLaPeReSt13]

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP**$_\gamma$ in **dim** $\sqrt{n}$ to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- The two results are incomparable.
- Best achievable γ here: n.
- In the case of Regev's encryption, we get $\gamma \approx n^{3/2}$.
- One can use BDD_γ instead (with a different γ).

Road-map

- Definition of the LWE problem
- Regev's encryption scheme
- Lattice problems
- Hardness of LWE
- **Equivalent problems**

LWE variants

Numerous variants have been showed to be at least as hard as LWE, up to polynomial factors in the noise rate α:

(Polynomial in n, $\log q$ and possibly in the number of samples m.)

- When $\mathbf{s}$ is distributed from the error distribution.
- When $\mathbf{s}$ is binary with sufficient entropy.
- When $\mathbf{e}$ is uniform in a hypercube.
- When $\mathbf{e}$ corresponds to a deterministic rounding of $\mathbf{As}$.
- When $\mathbf{A}$ is binary (modulo q).
- When some extra information on $\mathbf{e}$ is provided.
- When the first component of $\mathbf{e}$ is zero.

LWE in dimension 1

1-dimensional LWE [BoVe96]

With non-negl. prob. over $s \hookleftarrow U(\mathbb{Z}_q)$: distinguish between

$$(a, a \cdot s + e) \text{ and } (a, b) \qquad (\text{over } \mathbb{Z}_q^2),$$

where $a, b \hookleftarrow U(\mathbb{Z}_q)$, $e \hookleftarrow D_{\mathbb{Z},\alpha q}$.

Hardness of 1-dim LWE [BrLaPeReSt13]

For any n, q, n', q' with $n \log q \leq n' \log q'$:
there exists a polynomial-time reduction from $\mathrm{LWE}_{n,q,\alpha}$ to $\mathrm{LWE}_{n',q',\alpha'}$ for some $\alpha' \leq \alpha \cdot (n \log q)^{O(1)}$.

$\Rightarrow$ LWE_{1,q^n} is no easier than $\mathrm{LWE}_{n,q}$.

Approximate gcd

$\mathrm{AGCD}_{\mathcal{D},N,\alpha}$ [HG01]

With non-negl. prob. over $p \hookleftarrow \mathcal{D}$, distinguish between

$$u \quad \text{and} \quad q \cdot p + r \qquad (\text{over } \mathbb{Z}),$$

where $u \hookleftarrow U([0,N))$, $q \hookleftarrow U([0,\frac{N}{p}))$, $r \hookleftarrow \lfloor D_{\alpha p} \rceil$.

Hardness of AD (Informal) [ChSt15]

$\mathrm{AGCD}_{\mathcal{D},N,\alpha}$ is computationally equivalent to $\mathrm{LWE}_{n,q,\alpha}$, for some $\mathcal{D}$ of mean $\approx q^n$ and some $N \approx q^{2n}$.

Conclusion

LWE:

- LWE is hard for almost all instances.
- It seems exponentially hard to solve, even quantumly.
- It is a rich/expressive problem, convenient for cryptographic design.

Lattices:

- LWE hardness comes from lattice problems.
- We can design lattice-based cryptosystems without knowing lattices!

Exciting topics I did not mention

- The Small Integer Solution problem (SIS)
  $\Rightarrow$ Digital signatures.

- Ideal lattices, Ring-LWE, Ring-SIS, NTRU
  $\Rightarrow$ Using polynomial rings (a.k.a. structured matrices) to get more efficient constructions.
- Implementation of lattice-based primitives.

These will be addressed in Léo's talk (Friday morning), my second talk (Friday afternoon) and Tim's talk (Friday afternoon).

Open problems: foundations

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP**$_\gamma$ in **dim** n to LWE$_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP**$_\gamma$ in **dim** $\sqrt{n}$ to LWE$_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- Does there exist a classical reduction from n-dimensional SVP$_\gamma$/BDD$_\gamma$ to LWE$_{n,q,\alpha}$?
- Does there exist a quantum algorithm for LWE$_{n,q,\alpha}$ that runs in time $2^{\sqrt{n}}$ (when $q \leq n^{\mathcal{O}(1)}$)?
- Is LWE easy for some $\alpha = 1 \ / \ n^{\mathcal{O}(1)}$?
- Can we reduce factoring/DL to LWE?

Open problems: foundations

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP**$_\gamma$ in **dim** n to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP**$_\gamma$ in **dim** $\sqrt{n}$ to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- Does there exist a classical reduction from n-dimensional $\mathrm{SVP}_\gamma/\mathrm{BDD}_\gamma$ to $\mathrm{LWE}_{n,q,\alpha}$?
- Does there exist a quantum algorithm for $\mathrm{LWE}_{n,q,\alpha}$ that runs in time $2^{\sqrt{n}}$ (when $q \leq n^{\mathcal{O}(1)}$)?
- Is LWE easy for some $\alpha = 1 \,/\, n^{\mathcal{O}(1)}$?
- Can we reduce factoring/DL to LWE?

Open problems: foundations

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP**$_\gamma$ in **dim** n to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP**$_\gamma$ in **dim** $\sqrt{n}$ to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- Does there exist a classical reduction from n-dimensional $\mathrm{SVP}_\gamma/\mathrm{BDD}_\gamma$ to $\mathrm{LWE}_{n,q,\alpha}$?
- Does there exist a quantum algorithm for $\mathrm{LWE}_{n,q,\alpha}$ that runs in time $2^{\sqrt{n}}$ (when $q \leq n^{\mathcal{O}(1)}$)?
- Is LWE easy for some $\alpha = 1 \ / \ n^{\mathcal{O}(1)}$?
- Can we reduce factoring/DL to LWE?

Open problems: foundations

If q is prime and $\leq n^{\mathcal{O}(1)}$, then there exists a **quantum** polynomial-time reduction from **SVP**$_\gamma$ in **dim** n to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

If q is $\leq n^{\mathcal{O}(1)}$, then there exists a **classical** polynomial-time reduction from **GapSVP**$_\gamma$ in **dim** $\sqrt{n}$ to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.

- Does there exist a classical reduction from n-dimensional $\mathrm{SVP}_\gamma/\mathrm{BDD}_\gamma$ to $\mathrm{LWE}_{n,q,\alpha}$?
- Does there exist a quantum algorithm for $\mathrm{LWE}_{n,q,\alpha}$ that runs in time $2^{\sqrt{n}}$ (when $q \leq n^{\mathcal{O}(1)}$)?
- Is LWE easy for some $\alpha = 1 \,/\, n^{\mathcal{O}(1)}$?
- Can we reduce factoring/DL to LWE?

Open problems: cryptanalysis

LWE-based cryptography is based on GapSVP_γ for $\gamma \geq n$.
No NP-hardness here...

- Can we solve SVP_γ in poly(n)-time for some $\gamma = n^{\mathcal{O}(1)}$?
- And with a quantum computer?
- Can we do better than BKZ's $\left(\frac{n}{\log\gamma}\right)^{\mathcal{O}\left(\frac{n}{\log\gamma}\right)}$ run-time, for some γ?
- What are the practical limits?

http://www.latticechallenge.org

Open problems: cryptanalysis

LWE-based cryptography is based on GapSVP$_\gamma$ for $\gamma \geq n$.
No NP-hardness here...

- Can we solve SVP$_\gamma$ in poly(n)-time for some $\gamma = n^{\mathcal{O}(1)}$?
- And with a quantum computer?
- Can we do better than BKZ's $\left(\frac{n}{\log \gamma}\right)^{\mathcal{O}\left(\frac{n}{\log \gamma}\right)}$ run-time, for some γ?
- What are the practical limits?

http://www.latticechallenge.org

Open problems: cryptanalysis

LWE-based cryptography is based on GapSVP_γ for $\gamma \geq n$.
No NP-hardness here...

- Can we solve SVP_γ in poly(n)-time for some $\gamma = n^{\mathcal{O}(1)}$?
- And with a quantum computer?
- Can we do better than BKZ's $\left(\frac{n}{\log \gamma}\right)^{\mathcal{O}\left(\frac{n}{\log \gamma}\right)}$ run-time, for some γ?
- What are the practical limits?

http://www.latticechallenge.org

Open problems: cryptanalysis

LWE-based cryptography is based on GapSVP_γ for $\gamma \geq n$.
No NP-hardness here...

- Can we solve SVP_γ in poly(n)-time for some $\gamma = n^{\mathcal{O}(1)}$?
- And with a quantum computer?
- Can we do better than BKZ's $(\frac{n}{\log\gamma})^{\mathcal{O}(\frac{n}{\log\gamma})}$ run-time, for some γ?
- What are the practical limits?

http://www.latticechallenge.org

Open problems: practice

There exist practical lattice-based signature and encryption schemes.

- Can lattice-based primitives outperform other approaches in some contexts?
- What about side-channel cryptanalysis?
- Can advanced lattice-based primitives be made practical? Attribute-based encryption? Homomorphic encryption?

Open problems: practice

There exist practical lattice-based signature and encryption schemes.

- Can lattice-based primitives outperform other approaches in some contexts?
- What about side-channel cryptanalysis?
- Can advanced lattice-based primitives be made practical? Attribute-based encryption? Homomorphic encryption?

Open problems: practice

There exist practical lattice-based signature and encryption schemes.

- Can lattice-based primitives outperform other approaches in some contexts?
- What about side-channel cryptanalysis?
- Can advanced lattice-based primitives be made practical? Attribute-based encryption? Homomorphic encryption?

Open problems: practice

There exist practical lattice-based signature and encryption schemes.

- Can lattice-based primitives outperform other approaches in some contexts?
- What about side-channel cryptanalysis?
- Can advanced lattice-based primitives be made practical? Attribute-based encryption? Homomorphic encryption?

Bibliography

AhRe04 D. Aharonov, O. Regev: Lattice problems in NP cap coNP. J. ACM 52(5): 749-765 (2005).

AjDw97 M. Ajtai, C. Dwork: A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence. STOC 1997: 284-293.

Aj98 M. Ajtai: The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions (Extended Abstract). STOC 1998: 10-19.

AgDaReSD15 D. Aggarwal, D. Dadush, O. Regev, N. Stephens-Davidowitz: Solving the Shortest Vector Problem in 2^n Time via Discrete Gaussian Sampling. Available on ARXIV.

BoVe96 D. Boneh, R. Venkatesan: Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes. CRYPTO 1996: 129-142.

Br12 Z. Brakerski: Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. CRYPTO 2012: 868-886.

BrLaPeReSt13 Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé: Classical hardness of learning with errors. STOC 2013: 575-584.

BrVa11 Z. Brakerski, V. Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. SIAM J. Comput. 43(2): 831-871 (2014).

ChNg11 Y. Chen, P. Nguyen: BKZ 2.0: Better Lattice Security Estimates. ASIACRYPT 2011: 1-20.

ChSt15 J. H. Cheon, D. Stehlé: Fully Homomophic Encryption over the Integers Revisited. EUROCRYPT 2015.

Bibliography

GePeVa08 C. Gentry, C. Peikert, V. Vaikuntanathan: Trapdoors for hard lattices and new cryptographic constructions. STOC 2008: 197-206.

GoGo98 O. Goldreich, S. Goldwasser: On the Limits of Nonapproximability of Lattice Problems. J. Comput. Syst. Sci. 60(3): 540-563 (2000).

GoVaWe13 S. Gorbunov, V. Vaikuntanathan, H. Wee: Attribute-based encryption for circuits. STOC 2013: 545-554.

HaPuSt11 G. Hanrot, X. Pujol, D. Stehlé: Analyzing Blockwise Lattice Algorithms Using Dynamical Systems. CRYPTO 2011: 447-464.

HaRe07 I. Haviv, O. Regev: Tensor-based Hardness of the Shortest Vector Problem to within Almost Polynomial Factors. Theory of Computing 8(1): 513-531 (2012).

HG01 N. Howgrave-Graham: Approximate Integer Common Divisors. CaLC 2001: 51-66.

Pe14 C. Peikert: Lattice Cryptography for the Internet. PQCrypto 2014: 197-219.

Re03 O. Regev: New lattice-based cryptographic constructions. J. ACM 51(6): 899-942 (2004).

Re05 O. Regev: On lattices, learning with errors, random linear codes, and cryptography. J. ACM 56(6) (2009).

ScEu91 C.-P. Schnorr, M. Euchner: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Math. Program. 66: 181-199 (1994).