Relating different Polynomial-LWE problems

Mădălina Bolboceanu

SECITC 2018

Bitdefender®

This work

- We give relations between the hardness of PLWE^f and PLWE^h for different polynomials f and h.

- We find a polynomial f for which:

PLWE^f at least as hard as PLWE^h for exponentially many polynomials h

Outline

Lattice

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be linearly independent vectors from $\mathbb{R}^m$. Then

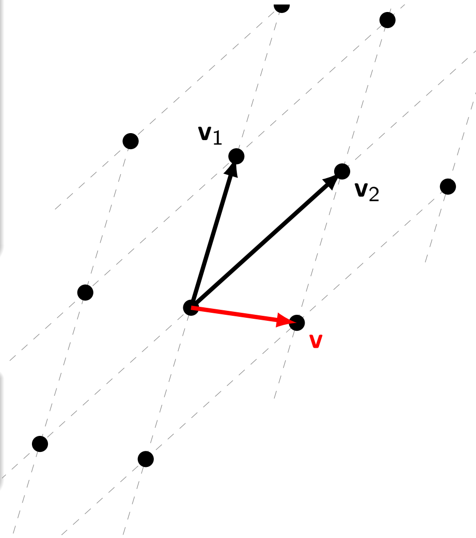
$$L = L(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \{\sum_{i=1}^{n} a_i \mathbf{v}_i | a_i \in \mathbb{Z}\}$$

is the lattice generated by them.

$\lambda_1(L) :=$ the length of a shortest nonzero vector from L.

ApproxSVP$_\gamma$

Find a nonzero vector $\mathbf{x} \in L$ s.t. $\|\mathbf{x}\| \le \gamma \lambda_1(L)$.

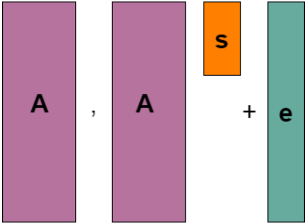


Learning with Errors [?]

Let $\mathbf{s} \in \mathbb{Z}_q^n$, $m \geq n$, $\alpha q > \sqrt{n}$

$$\begin{cases} \mathbf{A} \overset{u}{\hookleftarrow} \mathbb{Z}_q^{m \times n} \\ \mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q} \end{cases}$$

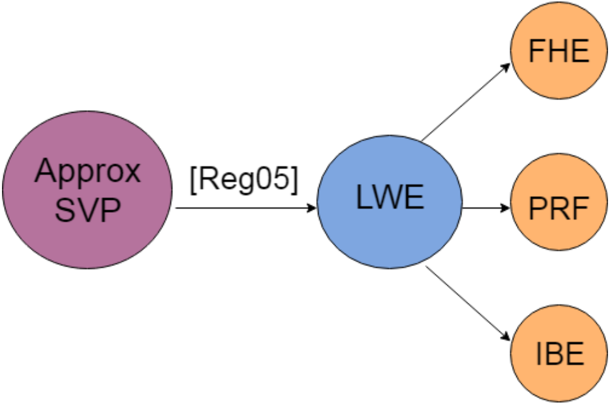
$\mathrm{LWE}_{q,\alpha q}$ distribution:



Search: Given LWE samples, find $\mathbf{s}$.
Decision: Distinguish LWE samples from uniform samples.

[?]: Solve **Search**-$\mathrm{LWE}_{q,\alpha q}$ $\xrightarrow{\text{quantum}}$ Solve $\mathrm{ApproxSVP}_\gamma$, for $\gamma \leq \mathrm{poly}(n)$.

LWE in crypto



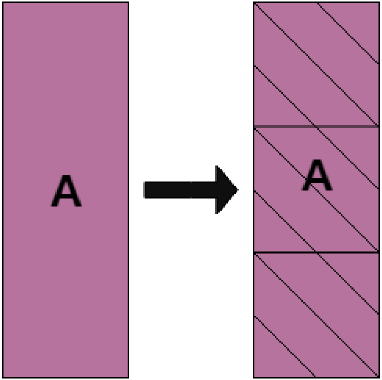
✓ **quantum resistant**

✓ all known algorithms of ApproxSVP are exponential in n.

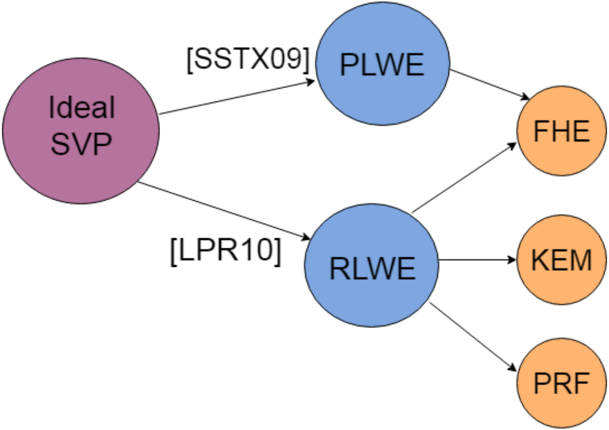
✗ large size of keys

✗ slow computations

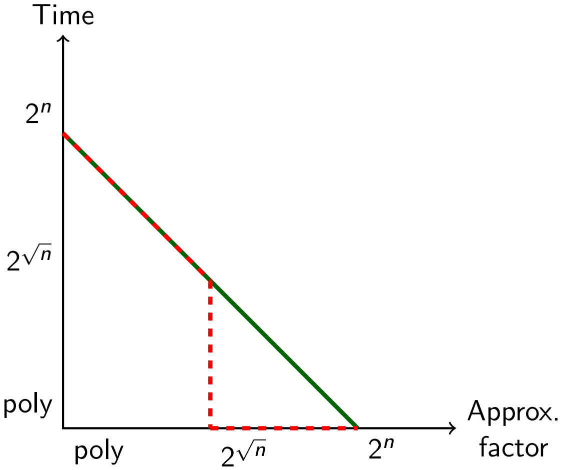
Take structured matrices!



Towards efficiency



SVP in general and ideal lattices ([? ?])



Possible approaches

- A new problem which is at least as hard as exponentially many PLWE problems
  Middle Product Learning with Errors (MP-LWE) [?]

MP-LWE at least as hard as PLWE^f
for exponentially many polynomials f

- The hardest instances of PLWE

Possible approaches

- A new problem which is at least as hard as exponentially many PLWE problems
  Middle Product Learning with Errors (MP-LWE) [**?**]

MP-LWE **at least as hard as** PLWE^f
for exponentially many polynomials f

- **The hardest instances of PLWE**

Outline

Our results

- We find a reduction from PLWE^f to $\mathrm{PLWE}^{f \circ g}$, for arbitrary monic polynomials f and g in $\mathbb{Z}[X]$.

- We notice interesting consequences of this reduction involving cyclotomic polynomials.

Polynomial LWE [?]

$f \in \mathbb{Z}[X]$, monic, $\deg f = n$, q prime.
$R := \mathbb{Z}[X]/(f)$, $R_q := R/qR \simeq \mathbb{Z}_q[X]/(f)$.

Let $s \in R_q$.

$$\text{PLWE}^f_{q,D_{\alpha q}} \text{ distribution : } \begin{cases} a \overset{u}{\hookleftarrow} R_q \\ e \hookleftarrow D_{\alpha q} \text{ over } \mathbb{R}^n \simeq \mathbb{R}[X]/(f) \\ \text{output: } (a, a \cdot s + e \bmod qR) \end{cases}$$

Search: Given PLWE samples, find s.
Decision: Distinguish PLWE samples from uniform samples.

Reduction from PLWE^f to PLWE$^{f \circ g}$

$f, g \in \mathbb{Z}[X]$, monic, deg $f = m$, deg $g = n$.
We consider the $mn \times mn$ matrix:

$$\mathbf{T}_g = \begin{pmatrix} 1 & \dots & g^{m-1} & X & \dots & Xg^{m-1} & \dots & X^{n-1} & \dots & X^{n-1}g^{m-1} \end{pmatrix}$$

Our main result

$\mathrm{PLWE}^{f \circ g}_{q, D_{\alpha q \sqrt{\mathbf{T}_g \mathbf{T}_g^t}}}$ given k samples **at least as hard as** $\mathrm{PLWE}^{f}_{q, D_{\alpha q}}$ given $k + n - 1$ samples

- It holds both in search and decision variants.

Proof (sketch)

Main idea: a map T sending PLWE^f to $\mathrm{PLWE}^{f \circ g}$ and uniform to uniform

- $\{(a_i^*, b_i^*)\}_{i \in [n-1]} \hookleftarrow \mathrm{PLWE}^f$ or uniform
- $\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_{n-1} \overset{u}{\hookleftarrow} \mathbb{Z}_q[X]/(f)$

$$(a_j, b_j) \xrightarrow{T} (\tilde{a}_j, \tilde{b}_j)$$

$$\tilde{a}_j = a_j \circ g + X a_1^* \circ g + \ldots + X^{n-1} a_{n-1}^* \circ g$$

$$\tilde{b}_j = b_j \circ g + X b_1^* \circ g + \ldots + X^{n-1} b_{n-1}^* \circ g + \tilde{a}_j \sum_{i \in [n-1]} X^i \tilde{s}_i \circ g$$

⋆ uniform $\xrightarrow{T}$ uniform

⋆ $\mathrm{PLWE}^f_{q, D_{\alpha q}}(s) \xrightarrow{T} \mathrm{PLWE}^{f \circ g}_{D_{q, \alpha q \sqrt{\mathbf{T}_g \mathbf{T}_g^t}}}(\tilde{s})$

Outline

1. Lattices in cryptography
2. Contribution
3. Impact

Relating PLWE^f for cyclotomic f's

- cyclotomics in crypto: e.g. homomorphic schemes [?], [?], key exchange schemes [?]

- $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$,
  $\phi_n(X) = \prod_{k \in \mathbb{Z}_n^*} (X - \zeta_n^k) \in \mathbb{Z}[X]$
- $\text{rad}(n) := p_1 p_2 \cdot \ldots \cdot p_r$,
  if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$

⋆ Using $\phi_n(X) = \phi_{\text{rad}(n)}(X^{n/\text{rad}(n)})$

$\text{PLWE}^{\phi_n}_{q,D_{\alpha q}}$ given k samples **at least as hard as** $\text{PLWE}^{\phi_{\text{rad}(n)}}_{q,D_{\alpha q}}$ given $k + \frac{n}{\text{rad}(n)} - 1$ samples

⋆ Using $\phi_n(X) = \phi_p(X^{n/p})$, for $n = p^r$, p prime

$\text{PLWE}^{\phi_n}_{q,D_{\alpha q}}$ given k samples **at least as hard as** $\text{PLWE}^{\phi_p}_{q,D_{\alpha q}}$ given $k + \frac{n}{p} - 1$ samples

Reductions to PLWE$^{\phi_n}$

- $\beta \in \mathbb{Z}[\zeta_n]$, $f_\beta :=$ the minimal polynomial of β over $\mathbb{Q}$, $f_\beta \in \mathbb{Z}[X]$
  $g_\beta \in \mathbb{Z}[X]$ s.t. $\beta = g_\beta(\zeta_n)$

PLWE$^{\phi_n}_{q,D_{\alpha q\sqrt{T_{g_\beta} T^t_{g_\beta}}}}$ given k samples **at least as hard as** PLWE$^{f_\beta}_{q,D_{\alpha q}}$ given $k + \deg g_\beta - 1$ samples for any $\beta \in \mathbb{Z}[\zeta_n]$ s.t. $\phi_n = f_\beta \circ g_\beta$

- Example of β's: $n = 2^t$, $\beta = \zeta_n^{2^u}$. Then $f_\beta = \phi_{2^{t-u}}$ and $g_\beta = X^{2^u}$, so $\phi_n = f_\beta \circ g_\beta$.
- In general, $\phi_n | f_\beta \circ g_\beta$.

In the case of power-of-two cyclotomic ϕ_n:

- Let $\mathbf{A}$ be a $\varphi(n) \times d$ matrix, $d \geq \varphi(n)$,

$$\mathbf{A}_{i,j} = \begin{cases} (-1)^k \text{ if } j = \varphi(n) \cdot k + i \\ 0 \text{ else} \end{cases}$$

$\mathrm{PLWE}^{\phi_n}_{D_{q,\alpha q\sqrt{\mathbf{G}\mathbf{G}^t}}}$ given k samples $\mathbf{G} := \mathbf{A}\mathbf{T}_{g_\beta}$	at least as hard as	$\mathrm{PLWE}^{f_\beta}_{D_{q,\alpha q}}$ given $k + \deg f_\beta \circ g_\beta - 1$ samples for any $\beta \in \mathbb{Z}[\zeta_n]$ s.t. g_β is monic

Conclusions and future work

- PLWE$^{f \circ g}$ is at least as hard as PLWE^{f}, for any monic $f, g \in \mathbb{Z}[X]$
- PLWE$^{\phi_n}$ is at least as hard as exponentially many PLWE^{f}, in the case of power-of-two cyclotomic polynomial ϕ_n

⋆ characterize $\beta \in \mathbb{Z}[\zeta_n]$ s.t. $\phi_n = f_\beta \circ g_\beta$

⋆ find $\beta \in \mathbb{Z}[\zeta_n]$ for which the matrix $\mathbf{AT}_{g_\beta}$ has small norm

⋆ find the hardest instance of PLWE

Questions?

Thank you.