On the Expanding Zoo of Lattice Assumptions

Russell W. F. Lai

Aalto University

Helsinki Algorithms and Theory Days, 29-30.08.2024

Cryptographers need computational assumptions

Cryptography is like a religion.

Minimum faith required:

symmetric-key crypto One-way functions (OWF)

public-key crypto OWF over algebraic structure, e.g. RSA, discrete logarithm (DLOG), SIS, LWE

(Relatively) unstructured assumptions
e.g. RSA, DLOG, SIS, LWE

$\Downarrow$

Basic cryptographic primitives
e.g. encryption, signatures, etc.

Structured and/or hinted assumptions
e.g. Strong RSA, One-More DLOG, Vanishing SIS, Evasive LWE

$\Downarrow$

Advanced properties
e.g. succinctness, quasi-linear time, etc.

Cryptographers need computational assumptions

Cryptography is like a religion.

Minimum faith required:

symmetric-key crypto One-way functions (OWF)

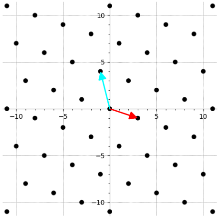
public-key crypto OWF over algebraic structure, e.g. RSA, discrete logarithm (DLOG), SIS, LWE

(Relatively) unstructured assumptions e.g. RSA, DLOG, SIS, LWE	Structured and/or hinted assumptions e.g. Strong RSA, One-More DLOG, Vanishing SIS, Evasive LWE
$\Downarrow$	$\Downarrow$
Basic cryptographic primitives e.g. encryption, signatures, etc.	Advanced properties e.g. succinctness, quasi-linear time, etc.

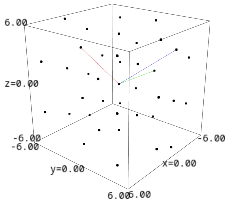
(Euclidean) Lattices

For basis $\mathbf{B} \in \mathbb{R}^{n \times k}$ with $k \leq n$, the lattice spanned by $\mathbf{B}$ is

$$\mathcal{L}(\mathbf{B}) := \left\{ \mathbf{Bz} : \mathbf{z} \in \mathbb{Z}^k \right\} \subseteq \mathbb{R}^n$$



An $n = 2$ dimensional example



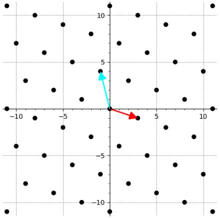
An $n = 3$ dimensional example

General believe: Arithmetic problems = easy, Geometric problems = hard

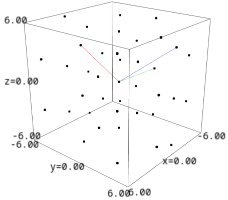
(Euclidean) Lattices

For basis $\mathbf{B} \in \mathbb{R}^{n \times k}$ with $k \leq n$, the lattice spanned by $\mathbf{B}$ is

$$\mathcal{L}(\mathbf{B}) := \left\{ \mathbf{B}\mathbf{z} : \mathbf{z} \in \mathbb{Z}^k \right\} \subseteq \mathbb{R}^n$$



An $n = 2$ dimensional example



An $n = 3$ dimensional example

General believe: Arithmetic problems = easy, Geometric problems = hard

Lattice-based cryptography

Lattice-based crypto = crypto based on hardness of lattice problems

Why lattice-based crypto?

- Conjectured **post-quantum** security
- Security (of most constructions) based on hardness of **worst-case** lattice problems
  i.e. there exist **worst-case to average-case reductions** between hard problems
- Enabling unique functionalities, e.g. fully homomorphic encryption

Goal of this talk

- Overview of old and new lattice-based assumptions
- Highlight gaps from foundational perspective

Basics: Successive minima

Successive minima $\lambda_1(\mathcal{L}), \ldots, \lambda_n(\mathcal{L})$

$\lambda_i(\mathcal{L})$ = Radius of smallest *n*-dim ball containing *i* linearly independent lattice vectors.

Worst-case problems: SIVP, GapSVP

SIVP_γ: Shortest Independent Vector Problem

Given $\mathcal{L} \subseteq \mathbb{R}^n$, find linearly independent $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\} \subseteq \mathcal{L}$ such that $\max_i \|\mathbf{z}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L})$.

GapSVP_γ: Decision Shortest Vector Problem

Given lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and a real $d > 0$, decide whether $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > \gamma \cdot d$.

The function $\gamma = \gamma(n)$ is the **approximation factor**. It plays a significant role in hardness.

Worst-case problems: SIVP, GapSVP

SIVP_γ: Shortest Independent Vector Problem

Given $\mathcal{L} \subseteq \mathbb{R}^n$, find linearly independent $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\} \subseteq \mathcal{L}$ such that $\max_i \|\mathbf{z}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L})$.

GapSVP_γ: Decision Shortest Vector Problem

Given lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and a real $d > 0$, decide whether $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > \gamma \cdot d$.

The function $\gamma = \gamma(n)$ is the **approximation factor**. It plays a significant role in hardness.

Worst-case problems: SIVP, GapSVP

SIVP_γ: Shortest Independent Vector Problem

Given $\mathcal{L} \subseteq \mathbb{R}^n$, find linearly independent $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\} \subseteq \mathcal{L}$ such that $\max_i \|\mathbf{z}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L})$.

GapSVP_γ: Decision Shortest Vector Problem

Given lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and a real $d > 0$, decide whether $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > \gamma \cdot d$.

The function $\gamma = \gamma(n)$ is the **approximation factor**. It plays a significant role in hardness.

Worst-case problems: Sliding scale of approximation factors

Known hardness results for GapSVP_γ:

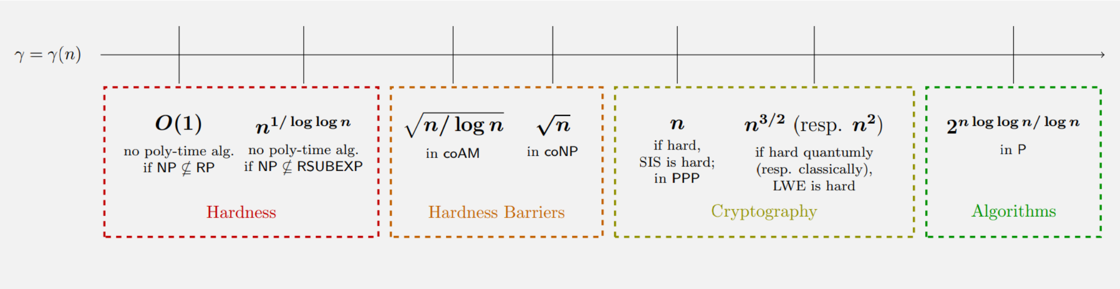


Figure from “The Complexity of the Shortest Vector Problem” by Huck Bennett, 2023.

Average-case problems: SIS, LWE

Let $n \leq m \leq \mathrm{poly}(n)$, $\beta \leq q \leq 2^{O(n)}$.

$\mathrm{SIS}_{n,m,q,\beta}$: Short Integer Solution [Ajtai96]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$, find $\mathbf{x} \in \mathbb{Z}^m$ with $\mathbf{Ax} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathrm{LWE}_{n,m,q,\chi}$: Learning with Errors [Regev05]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$ and sample $\mathbf{b} \in \mathbb{Z}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\top \approx \mathbf{s}^\top \mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$.

† Without norm constraint or noise $\implies$ linear algebra

† Geometry seems to make the problems much harder!

Average-case problems: SIS, LWE

Let $n \leq m \leq \mathrm{poly}(n)$, $\beta \leq q \leq 2^{O(n)}$.

$\mathsf{SIS}_{n,m,q,\beta}$: Short Integer Solution [Ajtai96]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$, find $\mathbf{x} \in \mathbb{Z}^m$ with $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathsf{LWE}_{n,m,q,\chi}$: Learning with Errors [Regev05]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$ and sample $\mathbf{b} \in \mathbb{Z}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\top \approx \mathbf{s}^\top \mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$.

† Without norm constraint or noise $\implies$ linear algebra

† Geometry seems to make the problems much harder!

Average-case problems: SIS, LWE

Let $n \leq m \leq \mathrm{poly}(n)$, $\beta \leq q \leq 2^{O(n)}$.

$\mathsf{SIS}_{n,m,q,\beta}$: Short Integer Solution [Ajtai96]

Given uniformly random $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$, find $\mathbf{x} \in \mathbb{Z}^m$ with $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathsf{LWE}_{n,m,q,\chi}$: Learning with Errors [Regev05]

Given uniformly random $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$ and sample $\mathbf{b} \in \mathbb{Z}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\top \approx \mathbf{s}^\top\mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\!\$\ \mathbb{Z}_q^n$.

† Without norm constraint or noise $\implies$ linear algebra

† Geometry seems to make the problems much harder!

Reductions

Hardness of SIS and LWE are relatively well understood.

$$\begin{tikzcd}
\text{SIVP} \arrow[r, shift left] \arrow[dr, dashed] & \text{SIS} \arrow[l, dotted, shift left] \arrow[d, dashed, shift left] \\
\text{GapSVP} \arrow[u] \arrow[ur] \arrow[r] & \text{LWE} \arrow[u, dotted, shift left]
\end{tikzcd}$$

- † $A \rightarrow B$: Classical reduction from A to B (Dotted = Trivial)
- † $A \dashrightarrow B$: Quantum reduction from A to B

Structured and/or hinted SIS and LWE

Recall: Stronger assumptions $\implies$ Fancier functionalities (generally)

How to make stronger variants of SIS and LWE, i.e. add adjectives?

- Additional structure, e.g.:
  - matrices and vectors over number rings $\mathcal{R}$ instead of $\mathbb{Z}$
  - structured matrix **A**, e.g. Vandermonde
- Give hints, e.g. for given $\mathbf{y}$, short vector $\mathbf{x}$ such that $\mathbf{Ax} = \mathbf{y} \bmod q$ and $\|\mathbf{x}\| \leq \beta$, denoted

$$\mathbf{x} \leftarrow\!\!\$\; \mathbf{A}_\beta^{-1}(\mathbf{y})$$

  We say "$\mathbf{x}$ is a preimage of $\mathbf{y}$ w.r.t. $\mathbf{A}$".

What to research about these assumptions?

- Applications to cryptographic constructions
- **Cryptanalysis**, i.e. find algorithms
- **Reductions**

Structured and/or hinted SIS and LWE

Recall: Stronger assumptions $\implies$ Fancier functionalities (generally)

How to make stronger variants of SIS and LWE, i.e. add adjectives?

- Additional structure, e.g.:
  - matrices and vectors over number rings $\mathcal{R}$ instead of $\mathbb{Z}$
  - structured matrix **A**, e.g. Vandermonde
- Give hints, e.g. for given **y**, short vector **x** such that $\mathbf{Ax} = \mathbf{y} \bmod q$ and $\|\mathbf{x}\| \leq \beta$, denoted

$$\mathbf{x} \leftarrow\!\!\$\ \mathbf{A}_\beta^{-1}(\mathbf{y})$$

  We say "**x** is a preimage of **y** w.r.t. **A**".

What to research about these assumptions?

- Applications to cryptographic constructions
- **Cryptanalysis**, i.e. find algorithms
- **Reductions**

Structured and/or hinted SIS and LWE

Recall: Stronger assumptions $\implies$ Fancier functionalities (generally)

How to make stronger variants of SIS and LWE, i.e. add adjectives?

- Additional structure, e.g.:
  - matrices and vectors over number rings $\mathcal{R}$ instead of $\mathbb{Z}$
  - structured matrix $\mathbf{A}$, e.g. Vandermonde
- Give hints, e.g. for given $\mathbf{y}$, short vector $\mathbf{x}$ such that $\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$ and $\|\mathbf{x}\| \leq \beta$, denoted

$$\mathbf{x} \leftarrow\$ \mathbf{A}_{\beta}^{-1}(\mathbf{y})$$

  We say "$\mathbf{x}$ is a preimage of $\mathbf{y}$ w.r.t. $\mathbf{A}$".

What to research about these assumptions?

- Applications to cryptographic constructions
- **Cryptanalysis**, i.e. find algorithms
- **Reductions**

Ring/module SIS and LWE – “Structure from the inside”

Typical setting: Let $\mathcal{R} = \mathbb{Z}[\zeta]$ where $\zeta \in \mathbb{C}$ is a root of unity.

$\mathsf{SIS}_{\mathcal{R},n,m,q,\beta}$: Ring/Module Short Integer Solution [Peikert-Rosen06, Lyubashevsky-Micciancio06]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{n\times m}$, find $\mathbf{x} \in \mathcal{R}^m$ with $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathsf{LWE}_{\mathcal{R},n,m,q,\chi}$: Ring/Module Learning with Errors [Lyubashevsky-Peikert-Regev10]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{n\times m}$ and sample $\mathbf{b} \in \mathcal{R}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\mathsf{T} \approx \mathbf{s}^\mathsf{T}\mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\$ \mathcal{R}_q^n$.

† If $\mathcal{R} = \mathbb{Z} \implies$ Standard SIS and LWE

† $n = 1$: “ring” setting

† $n > 1$: “module” setting

Ring/module SIS and LWE – “Structure from the inside”

Typical setting: Let $\mathcal{R} = \mathbb{Z}[\zeta]$ where $\zeta \in \mathbb{C}$ is a root of unity.

$\mathsf{SIS}_{\mathcal{R},n,m,q,\beta}$: Ring/Module Short Integer Solution [Peikert-Rosen06, Lyubashevsky-Micciancio06]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{n \times m}$, find $\mathbf{x} \in \mathcal{R}^m$ with $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathsf{LWE}_{\mathcal{R},n,m,q,\chi}$: Ring/Module Learning with Errors [Lyubashevsky-Peikert-Regev10]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{n \times m}$ and sample $\mathbf{b} \in \mathcal{R}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\top \approx \mathbf{s}^\top \mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\$ \mathcal{R}_q^n$.

† If $\mathcal{R} = \mathbb{Z} \implies$ Standard SIS and LWE

† $n = 1$: “ring” setting

† $n > 1$: “module” setting

Ring/module SIS and LWE – "Structure from the inside"

Typical setting: Let $\mathcal{R} = \mathbb{Z}[\zeta]$ where $\zeta \in \mathbb{C}$ is a root of unity.

$\mathsf{SIS}_{\mathcal{R},n,m,q,\beta}$: Ring/Module Short Integer Solution [Peikert-Rosen06, Lyubashevsky-Micciancio06]

Given uniformly random $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n\times m}$, find $\mathbf{x} \in \mathcal{R}^m$ with $\mathbf{Ax} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathsf{LWE}_{\mathcal{R},n,m,q,\chi}$: Ring/Module Learning with Errors [Lyubashevsky-Peikert-Regev10]

Given uniformly random $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n\times m}$ and sample $\mathbf{b} \in \mathcal{R}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\top \approx \mathbf{s}^\top\mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\!\!\$\ \mathcal{R}_q^n$.

- † If $\mathcal{R} = \mathbb{Z} \implies$ Standard SIS and LWE
- † $n = 1$: "ring" setting
- † $n > 1$: "module" setting

Ring/module SIS and LWE – "Structure from the inside"

Typical setting: Let $\mathcal{R} = \mathbb{Z}[\zeta]$ where $\zeta \in \mathbb{C}$ is a root of unity.

$\mathsf{SIS}_{\mathcal{R},n,m,q,\beta}$: Ring/Module Short Integer Solution [Peikert-Rosen06, Lyubashevsky-Micciancio06]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{n\times m}$, find $\mathbf{x} \in \mathcal{R}^m$ with $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$.

$\mathsf{LWE}_{\mathcal{R},n,m,q,\chi}$: Ring/Module Learning with Errors [Lyubashevsky-Peikert-Regev10]

Given uniformly random $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{n\times m}$ and sample $\mathbf{b} \in \mathcal{R}_q^m$, decide whether $\mathbf{b}$ is uniformly random or $\mathbf{b}^\intercal \approx \mathbf{s}^\intercal\mathbf{A} \bmod q$ for uniformly random $\mathbf{s} \leftarrow\$ \mathcal{R}_q^n$.

† If $\mathcal{R} = \mathbb{Z} \implies$ Standard SIS and LWE

† $n = 1$: "ring" setting

† $n > 1$: "module" setting

Reductions over rings and modules

Most existing reductions over $\mathbb{Z}$ generalise to ring/module settings.

$$
\begin{tikzcd}
\mathsf{SIVP}_{\mathcal{R}} \arrow[r, shift left] \arrow[dr, dashed] & \mathsf{SIS}_{\mathcal{R}} \arrow[l, dotted, shift left] \arrow[d, dashed, shift left] \\
\mathsf{GapSVP}_{\mathcal{R}} \arrow[u] \arrow[ur] & \mathsf{LWE}_{\mathcal{R}} \arrow[u, dotted, shift left]
\end{tikzcd}
$$

- † $A \rightarrow B$: Classical reduction from A to B (Dotted = Trivial)
- † $A \dashrightarrow B$: Quantum reduction from A to B

Issues:

- † Classical reduction from $\mathsf{GapSVP}_{\mathcal{R}}$ to $\mathsf{LWE}_{\mathcal{R}}$ missing (literature: restricted parameters, omitted)
- † $\mathsf{GapSVP}_{\mathcal{R}}$ easy in ring setting, i.e. $n = 1$

Reductions over rings and modules

Most existing reductions over $\mathbb{Z}$ generalise to ring/module settings.

$$\begin{tikzcd}
\mathrm{SIVP}_{\mathcal{R}} \arrow[r, shift left] \arrow[dr, dashed] & \mathrm{SIS}_{\mathcal{R}} \arrow[l, dotted, shift left] \arrow[d, dashed, shift left] \\
\mathrm{GapSVP}_{\mathcal{R}} \arrow[u] \arrow[ur] & \mathrm{LWE}_{\mathcal{R}} \arrow[u, dotted, shift left]
\end{tikzcd}$$

- † $A \rightarrow B$: Classical reduction from A to B (Dotted = Trivial)
- † $A \dashrightarrow B$: Quantum reduction from A to B

Issues:

- † Classical reduction from $\mathrm{GapSVP}_{\mathcal{R}}$ to $\mathrm{LWE}_{\mathcal{R}}$ missing (literature: restricted parameters, omitted)
- † $\mathrm{GapSVP}_{\mathcal{R}}$ easy in ring setting, i.e. $n = 1$

Polynomials and rational functions – "Structure from the outside"

Vanishing SIS [Cini-**L**-Malavolta23]

SIS but matrix **A** consists of rational functions evaluations at random points, e.g. Vandermonde

$$\mathbf{A} = \begin{pmatrix} 1 & a_1 & \dots & a_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \dots & a_n^{m-1} \end{pmatrix}.$$

In other words, given random points $a_1, \dots, a_n$, find degree-m polynomial with short coefficients which vanish at these points.

Current hardness status:

- † Worst-to-average reduction for constant degree polynomials [Preprint, **L**-Jykinen]
- † (Speculation) Worst-to-average reduction for constant individual-degree polynomials

Polynomials and rational functions – "Structure from the outside"

Vanishing SIS [Cini-**L**-Malavolta23]

SIS but matrix **A** consists of rational functions evaluations at random points, e.g. Vandermonde

$$\mathbf{A} = \begin{pmatrix} 1 & a_1 & \dots & a_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \dots & a_n^{m-1} \end{pmatrix}.$$

In other words, given random points $a_1, \dots, a_n$, find degree-m polynomial with short coefficients which vanish at these points.

Current hardness status:

† Worst-to-average reduction for constant degree polynomials [Preprint, **L**-Jykinen]

† (Speculation) Worst-to-average reduction for constant individual-degree polynomials

SIS and LWE with hints

Some (oversimplified) examples:

Evasive LWE [Wee22]

If LWE w.r.t. matrix $(\mathbf{A} \| \mathbf{P})$ is hard, then LWE w.r.t. matrix $\mathbf{A}$ given $\mathbf{A}_\beta^{-1}(\mathbf{P})$ as hints is hard.

One-More Inhomogeneous SIS (OM-ISIS) [Agrawal-Kirshanova-Stehlé-Yadav22]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$, k-time oracle access to $\mathbf{A}_\beta^{-1}(\cdot)$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y}_i)$ for random $\mathbf{y}_1, \ldots, \mathbf{y}_{k+1}$.

Current hardness status:

No result

SIS and LWE with hints

Some (oversimplified) examples:

Evasive LWE [Wee22]

If LWE w.r.t. matrix $(\mathbf{A} \| \mathbf{P})$ is hard, then LWE w.r.t. matrix $\mathbf{A}$ given $\mathbf{A}_\beta^{-1}(\mathbf{P})$ as hints is hard.

One-More Inhomogeneous SIS (OM-ISIS) [Agrawal-Kirshanova-Stehlé-Yadav22]

Given $\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times m}$, k-time oracle access to $\mathbf{A}_\beta^{-1}(\cdot)$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y}_i)$ for random $\mathbf{y}_1, \ldots, \mathbf{y}_{k+1}$.

Current hardness status:

No result

New source of hardness?

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-L-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

Current hardness status:

Assuming sub-exponential-secure OWF, as hard as SIS in $2^{O(m)}$ time and $m^{O(1)}$ memory [Preprint, Albrecht-**L**-Postlethwaite]

† Current best attack against SIS takes either

- ‡ enumeration: $2^{O(m \log m)}$ time and $m^{O(1)}$ memory, or
- ‡ sieving: $2^{O(m)}$ time and $2^{O(m)}$ memory, or
- ‡ interpolation of above

† Basing security on exponential-time-hardness or memory-hardness is rare.

New source of hardness?

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-L-Postlethwaite]

Given $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\!\$\ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

Current hardness status:

Assuming sub-exponential-secure OWF, as hard as SIS in $2^{O(m)}$ time and $m^{O(1)}$ memory [Preprint, Albrecht-**L**-Postlethwaite]

† Current best attack against SIS takes either

- ‡ enumeration: $2^{O(m \log m)}$ time and $m^{O(1)}$ memory, or
- ‡ sieving: $2^{O(m)}$ time and $2^{O(m)}$ memory, or
- ‡ interpolation of above

† Basing security on exponential-time-hardness or memory-hardness is rare.

New source of hardness?

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-L-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

Current hardness status:

Assuming sub-exponential-secure OWF, as hard as SIS in $2^{O(m)}$ time and $m^{O(1)}$ memory [Preprint, Albrecht-**L**-Postlethwaite]

- Current best attack against SIS takes either
  - enumeration: $2^{O(m \log m)}$ time and $m^{O(1)}$ memory, or
  - sieving: $2^{O(m)}$ time and $2^{O(m)}$ memory, or
  - interpolation of above
- Basing security on exponential-time-hardness or memory-hardness is rare.

Reduction Template

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-**L**-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

- Reduction from \$kHSIS to kHISIS
  \$kHSIS: Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, output highly entropic sample of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- Run \$kHSIS algorithm $2^{O(m)}$ times to produce a list of $2^{O(m)}$ samples of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- Argue existence of close pairs in list, close = $\|\mathbf{u} - \mathbf{v}\| < \beta$.
- Take differences of close pairs to get improved hints.
- Caution: Need to generate lists pseudorandomly, otherwise need $2^{O(m)}$ memory.
- Feed improved hints back to the \$kHSIS algorithm. Repeat.

Reduction Template

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-**L**-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

† Reduction from \$kHSIS to kHISIS
\$kHSIS: Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, output highly entropic sample of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.

† Run \$kHSIS algorithm $2^{O(m)}$ times to produce a list of $2^{O(m)}$ samples of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.

† Argue existence of close pairs in list, close = $\|\mathbf{u} - \mathbf{v}\| < \beta$.

† Take differences of close pairs to get improved hints.

† Caution: Need to generate lists pseudorandomly, otherwise need $2^{O(m)}$ memory.

† Feed improved hints back to the \$kHSIS algorithm. Repeat.

Reduction Template

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-L-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

- Reduction from \$kHSIS to kHISIS
  \$kHSIS: Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, output highly entropic sample of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- Run \$kHSIS algorithm $2^{O(m)}$ times to produce a list of $2^{O(m)}$ samples of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- Argue existence of close pairs in list, close = $\|\mathbf{u} - \mathbf{v}\| < \beta$.
- Take differences of close pairs to get improved hints.
- Caution: Need to generate lists pseudorandomly, otherwise need $2^{O(m)}$ memory.
- Feed improved hints back to the \$kHSIS algorithm. Repeat.

Reduction Template

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-**L**-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

- Reduction from \$kHSIS to kHISIS
  \$kHSIS: Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, output highly entropic sample of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- Run \$kHSIS algorithm $2^{O(m)}$ times to produce a list of $2^{O(m)}$ samples of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- Argue existence of close pairs in list, close = $\|\mathbf{u} - \mathbf{v}\| < \beta$.
- Take differences of close pairs to get improved hints.
- Caution: Need to generate lists pseudorandomly, otherwise need $2^{O(m)}$ memory.
- Feed improved hints back to the \$kHSIS algorithm. Repeat.

Reduction Template

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-**L**-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

† Reduction from \$kHSIS to kHISIS
\$kHSIS: Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, output highly entropic sample of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.

† Run \$kHSIS algorithm $2^{O(m)}$ times to produce a list of $2^{O(m)}$ samples of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.

† Argue existence of close pairs in list, close = $\|\mathbf{u} - \mathbf{v}\| < \beta$.

† Take differences of close pairs to get improved hints.

† Caution: Need to generate lists pseudorandomly, otherwise need $2^{O(m)}$ memory.

† Feed improved hints back to the \$kHSIS algorithm. Repeat.

Reduction Template

k-Hint Inhomogeneous SIS (kHISIS, i.e. selective OM-ISIS) [Preprint, Albrecht-**L**-Postlethwaite]

Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, k independent samples $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, find $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{y})$ for random $\mathbf{y}$.

- † Reduction from \$kHSIS to kHISIS
  \$kHSIS: Given $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow\$ \mathbf{A}_\beta^{-1}(\mathbf{0})$, output highly entropic sample of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- † Run \$kHSIS algorithm $2^{O(m)}$ times to produce a list of $2^{O(m)}$ samples of $\mathbf{A}_{O(\beta)}^{-1}(\mathbf{0})$.
- † Argue existence of close pairs in list, close = $\|\mathbf{u} - \mathbf{v}\| < \beta$.
- † Take differences of close pairs to get improved hints.
- † Caution: Need to generate lists pseudorandomly, otherwise need $2^{O(m)}$ memory.
- † Feed improved hints back to the \$kHSIS algorithm. Repeat.

Summary

- How hard are structured and hinted variants of SIS and LWE?
- Attacks? (Even sub-exponential attacks are interesting)
- Reductions from standard SIS and LWE?
- Worst-case to average-case reductions?
- More foundational work needed!

Russell W. F. Lai

Aalto University, Finland

russell.lai@aalto.fi

russell-lai.hk

research.cs.aalto.fi/crypto

Thank You!