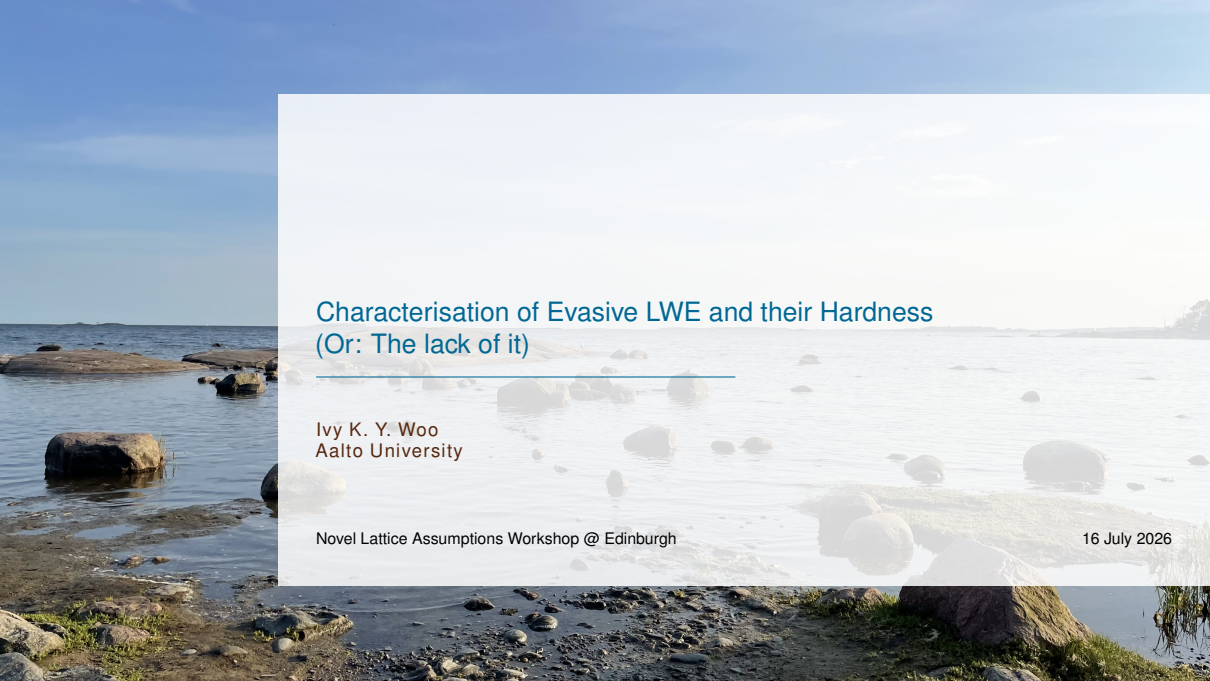


Characterisation of Evasive LWE and their Hardness (Or: The lack of it)

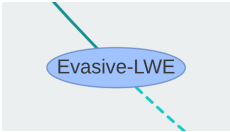
Ivy K. Y. Woo
Aalto University

Novel Lattice Assumptions Workshop @ Edinburgh

16 July 2026

Updates in the Zoo

The animal “Evasive LWE” (and its mutations) is now in the Zoo.



This topic is sometimes controversial. Vision of the page:

- Summary of major results and developments. Pointers to references with more details.
- Be factual.
- Not an exhaustive list of mutations.
  (If your favourite one is missing and you want it there, make a pull request)

LWE, and LWE given preimages

LWE

Given random wide $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$, sample $\mathbf{c} \in \mathbb{Z}_q^n$, hard to decide if $\mathbf{c}^\mathsf{T}$ is

$$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}^\mathsf{T} \bmod q \qquad \text{or} \qquad \text{random}$$

where $\mathbf{s} \leftarrow\!\$\ \mathbb{Z}_q^n$ LWE secret, $\mathbf{e} \approx \mathbf{0}$ short error.

- Advanced constructions may involve short Gaussian preimages $\mathbf{X}$ s.t.

$$\mathbf{A} \cdot \mathbf{X} = \mathbf{P} \bmod q$$

for $\mathbf{P}$ following specific (usually highly structured) distributions

- For many target $\mathbf{P}$, unclear how to simulate such $\mathbf{X}$ in security proof

(A Simple) Evasive LWE

Evasive LWE (informal) [Wee22]

For random wide $\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times m}$ and any $\mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$,

$$\begin{array}{lllll} \text{If} & (\mathbf{A}, & \mathbf{P}, & \mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T}, & \mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T}) \approx_c (\mathbf{A}, & \mathbf{P}, & \$, & \$) \\ \text{Then} & (\mathbf{A}, & \mathbf{P}, & \mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T}, & \mathbf{X}) \approx_c (\mathbf{A}, & \mathbf{P}, & \$, & \mathbf{X}) \end{array}$$

where $\mathbf{X} \leftarrow\!\!\$$ Gaussian s.t. $\mathbf{A} \cdot \mathbf{X} = \mathbf{P} \bmod q$, and $\mathbf{e}_A, \mathbf{e}_P$ Gaussian errors.

(A Simple) Evasive LWE

Evasive LWE (informal) [Wee22]

For random wide $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$ and any $\mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$,

If	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T})$
Then	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{X})$

$\approx_c$ $(\mathbf{A},$ $\mathbf{P},$ $\$,$ $\$)$

$\approx_c$ $(\mathbf{A},$ $\mathbf{P},$ $\$,$ $\mathbf{X})$

where $\mathbf{X} \leftarrow\!\$$ Gaussian s.t. $\mathbf{A} \cdot \mathbf{X} = \mathbf{P} \bmod q$, and $\mathbf{e}_A, \mathbf{e}_P$ Gaussian errors.

- Intuition: No meaningful use of preimage $\mathbf{X}$ in "Then", except right-multiply to get

$$(\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T}) \cdot \mathbf{X} = \mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}^\mathsf{T}\mathbf{X} \bmod q$$

  $\rightarrow$ modelled as $\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T} \bmod q$ in "If"

(A Simple) Evasive LWE

Evasive LWE (informal) [Wee22]

For random wide $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$ and any $\mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$,

If	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T})$
Then	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{X})$

$\approx_c$ $(\mathbf{A},$ $\mathbf{P},$ $\$,$ $\$)$

$\approx_c$ $(\mathbf{A},$ $\mathbf{P},$ $\$,$ $\mathbf{X})$

where $\mathbf{X} \leftarrow\!\$$ Gaussian s.t. $\mathbf{A} \cdot \mathbf{X} = \mathbf{P} \bmod q$, and $\mathbf{e}_A, \mathbf{e}_P$ Gaussian errors.

- Intuition: No meaningful use of preimage $\mathbf{X}$ in "Then", except right-multiply to get

$$(\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T}) \cdot \mathbf{X} = \mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}^\mathsf{T}\mathbf{X} \bmod q$$

  $\rightarrow$ modelled as $\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T} \bmod q$ in "If"

- Usefulness: In security proof, suffices to argue "if" holds (No preimages anymore)

Witness encryption and null-IO from evasive LWE
V Vaikuntanathan, H Wee, D Wichs - … on the Theory and Application of …, 2022 - Springer
… We will need to rely on a version of **evasive LWE** where \(\textbf{P}\) is … **evasive LWE** assumption to argue that (2) holds in this case as well. Unfortunately, we show that the **evasive LWE** …
☆ Save 99 Cite Cited by 85 Related articles All 6 versions

Optimal broadcast encryption and CP-ABE from evasive lattice assumptions
H Wee - Annual International Conference on the Theory and …, 2022 - Springer
… We prove selective security of our scheme assuming **evasive LWE**, a non-standard variant of the **LWE** assumption where the distinguisher additionally receives short Gaussian pre-…
☆ Save 99 Cite Cited by 117 Related articles All 5 versions

A general framework for lattice-based ABE using evasive inner-product functional encryption
YC Hsieh, H Lin, J Luo - Annual International Conference on the Theory …, 2024 - Springer
… random \(\textbf{s}\) (eg, \(\{\textbf{u}=\textbf{s}=\textbf{s}\textbf{t}\}\)), then we can base the security of **evasive** IPFE on variants of **evasive LWE**. All ABE constructions in this work uses …
☆ Save 99 Cite Cited by 25 Related articles All 3 versions

Compact pseudorandom functional encryption from evasive LWE
S Agrawal, S Kumari, S Yamada - Cryptology ePrint Archive, 2024 - eprint.iacr.org
… (private coin) **evasive LWE** and **LWE** assumptions. Intuitively, … depth, from just the **LWE** and **evasive LWE** assumptions. This … the assumption of circular **evasive LWE** used in the work of …
☆ Save 99 Cite Cited by 14 Related articles »

Attribute based encryption for turing machines from lattices
S Agrawal, S Kumari, S Yamada - Annual International Cryptology …, 2024 - Springer
… Below, we describe the **evasive** and circular tensor **LWE** assumptions. Below, we adopt the convention by Wee [30] and let the underline denote that noise is added to the term, whose …
☆ Save 99 Cite Cited by 29 Related articles All 4 versions

Adaptively sound zero-knowledge SNARKs for UP
S Mathialagan, S Peters, V Vaikuntanathan - Annual International …, 2024 - Springer
… We defer the discussion of how to achieve this guarantee from **evasive LWE** (and **LWE**) to the next subsection; in the remainder of this one, we describe how to use it to construct a …
☆ Save 99 Cite Cited by 35 Related articles All 3 versions

Multi-authority ABE from lattices without random oracles
B Waters, H Wee, DJ Wu - Theory of Cryptography Conference, 2022 - Springer
… the recently-introduced **evasive LWE** assumption by Wee [Wee22] and Tsabury [Tsa22]. **Evasive LWE**. We start by describing a variant of the **evasive LWE** assumption introduced by …
☆ Save 99 Cite Cited by 70 Related articles All 11 versions

Pseudorandom multi-input functional encryption and applications
S Agrawal, S Kumari, S Yamada - Cryptology ePrint Archive, 2024 - eprint.iacr.org
… Assuming **evasive LWE** and **LWE**, we construct a multi-input predicate … of Tensor **LWE** in addition to **LWE** and **evasive LWE**. … Assuming a stronger variant of **evasive LWE** and **LWE**, we …
☆ Save 99 Cite Cited by 13 Related articles »

Constant input attribute based (and predicate) encryption from evasive and tensor LWE
S Agrawal, M Rossi, A Yadav, S Yamada - Annual International Cryptology …, 2023 - Springer
… However, we are unable to prove security of this scheme based on the **evasive**/tensor \(\textsf{**LWE**}\) assumption. This is because the **evasive** \(\textsf{**LWE**}\) assumption …
☆ Save 99 Cite Cited by 32 Related articles All 7 versions

(only showing some top results)

Writing this formally...

If (Pre):	$(\mathbf{A}, \mathbf{P}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_A^\intercal, \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_P^\intercal)$	$\approx_c$	$(\mathbf{A}, \mathbf{P}, \$, \$)$
Then (Post):	$(\mathbf{A}, \mathbf{P}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_A^\intercal, \mathbf{X})$	$\approx_c$	$(\mathbf{A}, \mathbf{P}, \$, \mathbf{X})$

[Wee22]:
$\forall$ PPT $\mathbf{P} \in \mathbb{Z}_q^{m \times k} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$ and $\mathcal{B}$, $\exists$ PPT $\mathcal{A}$, polynomial $p(\lambda)$, negl. function $\epsilon(\lambda)$ s.t.

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{Post}}(\lambda) \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Pre}}(\lambda)/p(\lambda) - \epsilon(\lambda)$$

$\mathsf{Pre}_{\mathcal{A}}^b(1^\lambda)$

$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$; $\mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

$\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$, $\mathbf{e}_A \leftarrow\$ \mathcal{D}_{\mathbb{Z}, \chi_A}^m$, $\mathbf{e}_P \leftarrow\$ \mathcal{D}_{\mathbb{Z}, \chi_P}^k$

if $b = 0$ **then**

$\mathbf{c}_A^\intercal := \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_A^\intercal \bmod q$

$\mathbf{c}_P^\intercal := \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_P^\intercal \bmod q$

if $b = 1$ **then**

$\mathbf{c}_A \leftarrow\$ \mathbb{Z}_q^m$; $\mathbf{c}_P \leftarrow\$ \mathbb{Z}_q^k$

return $\mathcal{A}(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{c}_P, \mathsf{rand})$

$\mathsf{Post}_{\mathcal{B}}^b(1^\lambda)$

$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$: $\mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

$\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$, $\mathbf{e}_A \leftarrow\$ \mathcal{D}_{\mathbb{Z}, \chi_A}^m$

if $b = 0$ **then**

$\mathbf{c}_A^\intercal := \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_A^\intercal \bmod q$

$\mathbf{X} \leftarrow\$ \mathcal{D}_{\Lambda_q^{\mathbf{P}}(\mathbf{A}), \sigma}$

if $b = 1$ **then**

$\mathbf{c}_A \leftarrow\$ \mathbb{Z}_q^m$; $\mathbf{X} \leftarrow\$ \mathcal{D}_{\Lambda_q^{\mathbf{P}}(\mathbf{A}), \sigma}$

return $\mathcal{B}(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{X}, \mathsf{rand})$

But... They are almost always different

Assumption 3.16 (Evasive LWE). Let λ be a security parameter, and let $n = n(\lambda), m = m(\lambda), q = q(\lambda), \chi = \chi(\lambda)$, $s = s(\lambda)$ with $s \geq O(\sqrt{m \log q})$. Let Samp be an algorithm that takes the security parameter 1^λ as input and outputs a matrix $\mathbf{B} \in \mathbb{Z}_q^{n\ell \times m'}$, a set of ℓ target matrices $\mathbf{P}_1 \in \mathbb{Z}_q^{n \times N_1}, \ldots, \mathbf{P}_\ell \in \mathbb{Z}_q^{n \times N_\ell}$, and auxiliary information $\mathsf{aux} \in \{0,1\}^*$. Then, for adversaries $\mathcal{A}_0$ and $\mathcal{A}_1$, we define advantage functions

$$\begin{aligned}
\mathsf{Adv}^{(\mathrm{PRE})}_{\mathcal{A}_0}(\lambda) &:= \Big| \Pr\left[\mathcal{A}_0(\{(\mathbf{A}_i, \mathbf{s}_i^\intercal \mathbf{A}_i + \mathbf{e}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_2^\intercal, \{\mathbf{s}_i^\intercal \mathbf{P}_i + \mathbf{e}_{3,i}^\intercal\}_{i\in[\ell]}, \mathsf{aux}) = 1\right] \\
&\quad - \Pr\left[\mathcal{A}_0(\{(\mathbf{A}_i, \mathbf{u}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{u}_2^\intercal, \{\mathbf{u}_{3,i}^\intercal\}_{i\in[\ell]}, \mathsf{aux}) = 1\right]\Big| \\
\mathsf{Adv}^{(\mathrm{POST})}_{\mathcal{A}_1}(\lambda) &:= \Big| \Pr\left[\mathcal{A}_1(\{(\mathbf{A}_i, \mathbf{s}_i^\intercal \mathbf{A}_i + \mathbf{e}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_2^\intercal, \{\mathbf{K}_i\}_{i\in[\ell]}, \mathsf{aux}) = 1\right] \\
&\quad - \Pr\left[\mathcal{A}_1(\{(\mathbf{A}_i, \mathbf{u}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{u}_2^\intercal, \{\mathbf{K}_i\}_{i\in[\ell]}, \mathsf{aux}) = 1\right]\Big|,
\end{aligned}$$

where

$$\begin{aligned}
&(\mathbf{B}, \mathbf{P}_1, \ldots, \mathbf{P}_\ell, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda), \\
&\mathbf{A}_1, \ldots, \mathbf{A}_\ell \xleftarrow{R} \mathbb{Z}_q^{n \times m}, \\
&\mathbf{s}_1, \ldots, \mathbf{s}_\ell \xleftarrow{R} \mathbb{Z}_q^n, \mathbf{s}^\intercal \leftarrow [\mathbf{s}_1^\intercal \mid \cdots \mid \mathbf{s}_\ell^\intercal] \in \mathbb{Z}_q^{n\ell}, \\
&\mathbf{u}_{1,i} \xleftarrow{R} \mathbb{Z}_q^m, \mathbf{e}_{1,i} \leftarrow D_{\mathbb{Z},\chi}^m \ \forall i \in [\ell], \\
&\mathbf{u}_2 \xleftarrow{R} \mathbb{Z}_q^{m'}, \mathbf{e}_2 \leftarrow D_{\mathbb{Z},\chi}^{m'}, \\
&\mathbf{u}_{3,i} \xleftarrow{R} \mathbb{Z}_q^{N_i}, \mathbf{e}_{3,i} \leftarrow D_{\mathbb{Z},\chi}^{N_i} \ \forall i \in [\ell], \\
&\mathbf{K}_i \leftarrow (\mathbf{A}_i)_{\mathbf{s}}^{-1}(\mathbf{P}_i) \ \forall i \in [\ell].
\end{aligned}$$

We say that the evasive LWE assumption holds if for every efficient sampler Samp and every efficient adversary $\mathcal{A}_1$, there exists an efficient algorithm $\mathcal{A}_0$, polynomial $\mathrm{poly}(\cdot)$, and negligible function $\mathrm{negl}(\cdot)$ such that for all $\lambda \in \mathbb{N}$,

$$\mathsf{Adv}^{(\mathrm{PRE})}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{(\mathrm{POST})}_{\mathcal{A}_1}(\lambda)/\mathrm{poly}(\lambda) - \mathrm{negl}(\lambda).$$

But... They are almost always different

Assumption 3.16 (Evasive LWE). Let λ be a security parameter, and let $n = n(\lambda), m = m(\lambda), q = q(\lambda), \chi = \chi(\lambda)$, $s = s(\lambda)$ with $s \geq O(\sqrt{m \log q})$. Let Samp be an algorithm that takes the security parameter 1^λ as input and outputs a matrix $\mathbf{B} \in \mathbb{Z}_q^{n\ell \times m'}$, a set of ℓ target matrices $\mathbf{P}_1 \in \mathbb{Z}_q^{n \times N_1}, \ldots, \mathbf{P}_\ell \in \mathbb{Z}_q^{n \times N_\ell}$, and auxiliary information $\mathsf{aux} \in \{0,1\}^*$. Then, for adversaries $\mathcal{A}_0$ and $\mathcal{A}_1$, we define advantage functions

$$\mathsf{Adv}^{(\mathrm{PRE})}_{\mathcal{A}_0}(\lambda) := \Big|\Pr\Big[\mathcal{A}_0(\{(\mathbf{A}_i, \mathbf{s}_i^\intercal \mathbf{A}_i + \mathbf{e}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_2^\intercal, \{\mathbf{s}_i^\intercal \mathbf{P}_i + \mathbf{e}_{3,i}^\intercal\}_{i\in[\ell]}, \mathsf{aux}) = 1\Big] - \Pr\Big[\mathcal{A}_0(\{(\mathbf{A}_i, \mathbf{u}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{u}_2^\intercal, \{\mathbf{u}_{3,i}^\intercal\}_{i\in[\ell]}, \mathsf{aux}) = 1\Big]\Big|$$

$$\mathsf{Adv}^{(\mathrm{POST})}_{\mathcal{A}_1}(\lambda) := \Big|\Pr\Big[\mathcal{A}_1(\{(\mathbf{A}_i, \mathbf{s}_i^\intercal \mathbf{A}_i + \mathbf{e}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_2^\intercal, \{\mathbf{K}_i\}_{i\in[\ell]}, \mathsf{aux}) = 1\Big] - \Pr\Big[\mathcal{A}_1(\{(\mathbf{A}_i, \mathbf{u}_{1,i}^\intercal)\}_{i\in[\ell]}, \mathbf{B}, \mathbf{u}_2^\intercal, \{\mathbf{K}_i\}_{i\in[\ell]}, \mathsf{aux}) = 1\Big]\Big|,$$

where

$$(\mathbf{B}, \mathbf{P}_1, \ldots, \mathbf{P}_\ell, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda),$$
$$\mathbf{A}_1, \ldots, \mathbf{A}_\ell \xleftarrow{R} \mathbb{Z}_q^{n\times m},$$
$$\mathbf{s}_1, \ldots, \mathbf{s}_\ell \xleftarrow{R} \mathbb{Z}_q^n, \mathbf{s}^\intercal \leftarrow [\mathbf{s}_1^\intercal \mid \cdots$$
$$\mathbf{u}_{1,i} \xleftarrow{R} \mathbb{Z}_q^m, \mathbf{e}_{1,i} \leftarrow D^m_{\mathbb{Z},\chi} \ \forall i \in [\ell$$
$$\mathbf{u}_2 \xleftarrow{R} \mathbb{Z}_q^{m'}, \mathbf{e}_2 \leftarrow D^{m'}_{\mathbb{Z},\chi'}$$
$$\mathbf{u}_{3,i} \xleftarrow{R} \mathbb{Z}_q^{N_i}, \mathbf{e}_{3,i} \leftarrow D^{N_i}_{\mathbb{Z},\chi} \ \forall i \in [\ell$$
$$\mathbf{K}_i \leftarrow (\mathbf{A}_i)_s^{-1}(\mathbf{P}_i) \ \forall i \in [\ell].$$

We say that the evasive LWE assumption holds if for every efficient s there exists an efficient algorithm $\mathcal{A}_0$, polynomial $\mathrm{poly}(\cdot)$, and negli

$$\mathsf{Adv}^{(\mathrm{PRE})}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{(\mathrm{POST})}_{\mathcal{A}_1}(\lambda)/\mathrm{poly}(\lambda) - \mathrm{negl}(\lambda).$$

Assumption 3.1 (Evasive LWE). Let $n, m, t, m', q \in \mathbb{N}$ be parameters and λ be a security parameter. Let χ and χ' be parameters for Gaussian distributions. Let Samp be a PPT algorithm that outputs

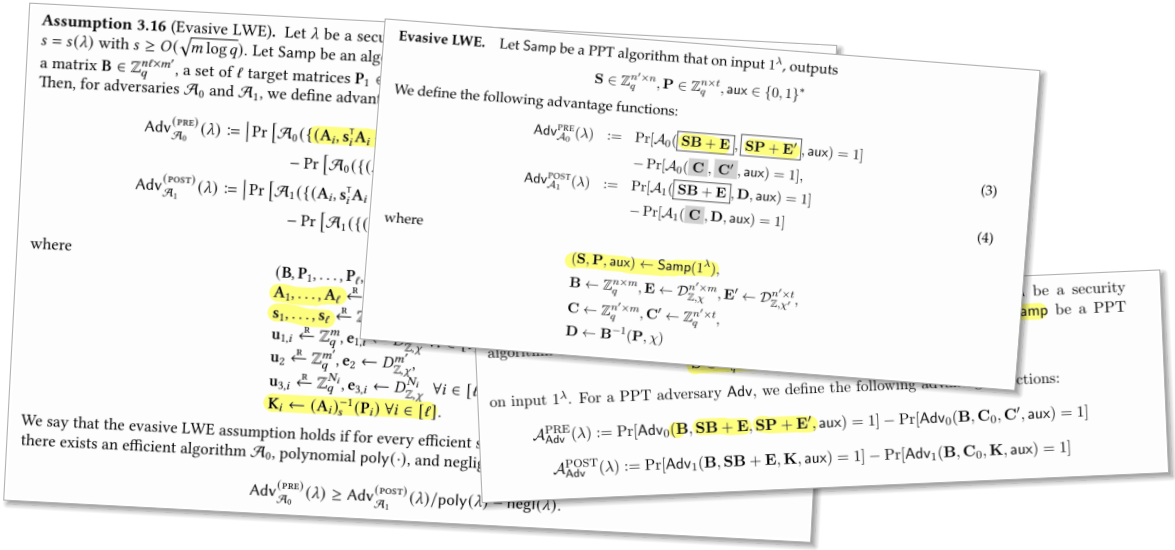
$$\mathbf{S} \in \mathbb{Z}_q^{m' \times n}, \mathbf{P} \in \mathbb{Z}_q^{n \times t}, \mathsf{aux} \in \{0,1\}^*$$

on input 1^λ. For a PPT adversary Adv, we define the following advantage functions:

$$\mathcal{A}^{\mathrm{PRE}}_{\mathsf{Adv}}(\lambda) := \Pr[\mathsf{Adv}_0(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) = 1] - \Pr[\mathsf{Adv}_0(\mathbf{B}, \mathbf{C}_0, \mathbf{C}', \mathsf{aux}) = 1]$$

$$\mathcal{A}^{\mathrm{POST}}_{\mathsf{Adv}}(\lambda) := \Pr[\mathsf{Adv}_1(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{K}, \mathsf{aux}) = 1] - \Pr[\mathsf{Adv}_1(\mathbf{B}, \mathbf{C}_0, \mathbf{K}, \mathsf{aux}) = 1]$$

But... They are almost always different



Assumption 3.16 (Evasive LWE). Let λ be a secu
$s = s(\lambda)$ with $s \geq O(\sqrt{m \log q})$. Let Samp be an alg
a matrix $\mathbf{B} \in \mathbb{Z}_q^{n\ell \times m'}$, a set of ℓ target matrices $\mathbf{P}_1 \in$
Then, for adversaries $\mathcal{A}_0$ and $\mathcal{A}_1$, we define advan

$$\mathsf{Adv}^{(\mathrm{PRE})}_{\mathcal{A}_0}(\lambda) := \left|\Pr\left[\mathcal{A}_0(\{(\mathbf{A}_i, \mathbf{s}_i^\intercal \mathbf{A}_i$$
$$- \Pr\left[\mathcal{A}_0(\{($$
$$\mathsf{Adv}^{(\mathrm{POST})}_{\mathcal{A}_1}(\lambda) := \left|\Pr\left[\mathcal{A}_1(\{(\mathbf{A}_i, \mathbf{s}_i^\intercal \mathbf{A}_i$$
$$- \Pr\left[\mathcal{A}_1(\{($$

where

$$(\mathbf{B}, \mathbf{P}_1, \ldots, \mathbf{P}_{\ell}$$
$$\mathbf{A}_1, \ldots, \mathbf{A}_\ell \xleftarrow{R}$$
$$\mathbf{s}_1, \ldots, \mathbf{s}_\ell \xleftarrow{R}$$
$$\mathbf{u}_{1,i} \xleftarrow{R} \mathbb{Z}_q^m, \mathbf{e}_{1,i}$$
$$\mathbf{u}_2 \xleftarrow{R} \mathbb{Z}_q^{m'}, \mathbf{e}_2 \leftarrow D^{m'}_{\mathbb{Z},\chi},$$
$$\mathbf{u}_{3,i} \xleftarrow{R} \mathbb{Z}_q^{N_i}, \mathbf{e}_{3,i} \leftarrow D^{N_i}_{\mathbb{Z},\chi} \quad \forall i \in [\ell$$
$$\mathbf{K}_i \leftarrow (\mathbf{A}_i)_s^{-1}(\mathbf{P}_i) \; \forall i \in [\ell].$$

We say that the evasive LWE assumption holds if for every efficient s
there exists an efficient algorithm $\mathcal{A}_0$, polynomial $\mathrm{poly}(\cdot)$, and negli

$$\mathsf{Adv}^{(\mathrm{PRE})}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{(\mathrm{POST})}_{\mathcal{A}_1}(\lambda)/\mathrm{poly}(\lambda) - \mathrm{negl}(\lambda).$$

Evasive LWE. Let Samp be a PPT algorithm that on input 1^λ, outputs

$$\mathbf{S} \in \mathbb{Z}_q^{n' \times n}, \mathbf{P} \in \mathbb{Z}_q^{n \times t}, \mathsf{aux} \in \{0,1\}^*$$

We define the following advantage functions:

$$\mathsf{Adv}^{\mathrm{PRE}}_{\mathcal{A}_0}(\lambda) := \Pr[\mathcal{A}_0(\boxed{\mathbf{SB} + \mathbf{E}}, \boxed{\mathbf{SP} + \mathbf{E}'}, \mathsf{aux}) = 1]$$
$$- \Pr[\mathcal{A}_0(\boxed{\mathbf{C}}, \boxed{\mathbf{C}'}, \mathsf{aux}) = 1],$$
$$\mathsf{Adv}^{\mathrm{POST}}_{\mathcal{A}_1}(\lambda) := \Pr[\mathcal{A}_1(\boxed{\mathbf{SB} + \mathbf{E}}, \mathbf{D}, \mathsf{aux}) = 1] \quad (3)$$
$$- \Pr[\mathcal{A}_1(\boxed{\mathbf{C}}, \mathbf{D}, \mathsf{aux}) = 1]$$

where (4)

$$(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda),$$
$$\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{E} \leftarrow \mathcal{D}^{n' \times m}_{\mathbb{Z},\chi}, \mathbf{E}' \leftarrow \mathcal{D}^{n' \times t}_{\mathbb{Z},\chi'},$$
$$\mathbf{C} \leftarrow \mathbb{Z}_q^{n' \times m}, \mathbf{C}' \leftarrow \mathbb{Z}_q^{n' \times t},$$
$$\mathbf{D} \leftarrow \mathbf{B}^{-1}(\mathbf{P}, \chi)$$

algorithm

be a security
amp be a PPT

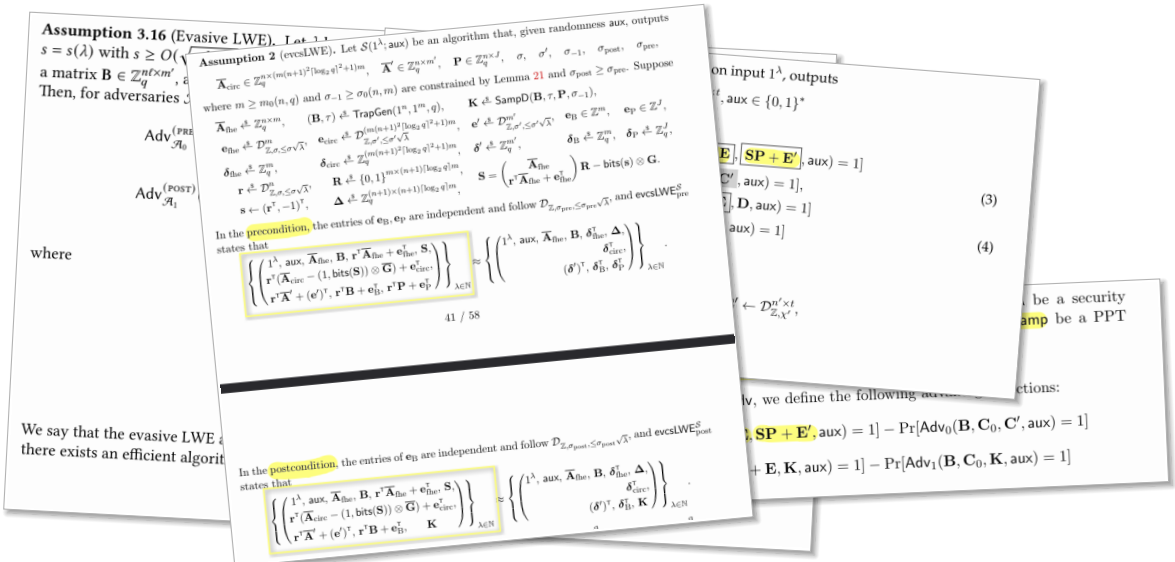
on input 1^λ. For a PPT adversary Adv, we define the following

ctions:

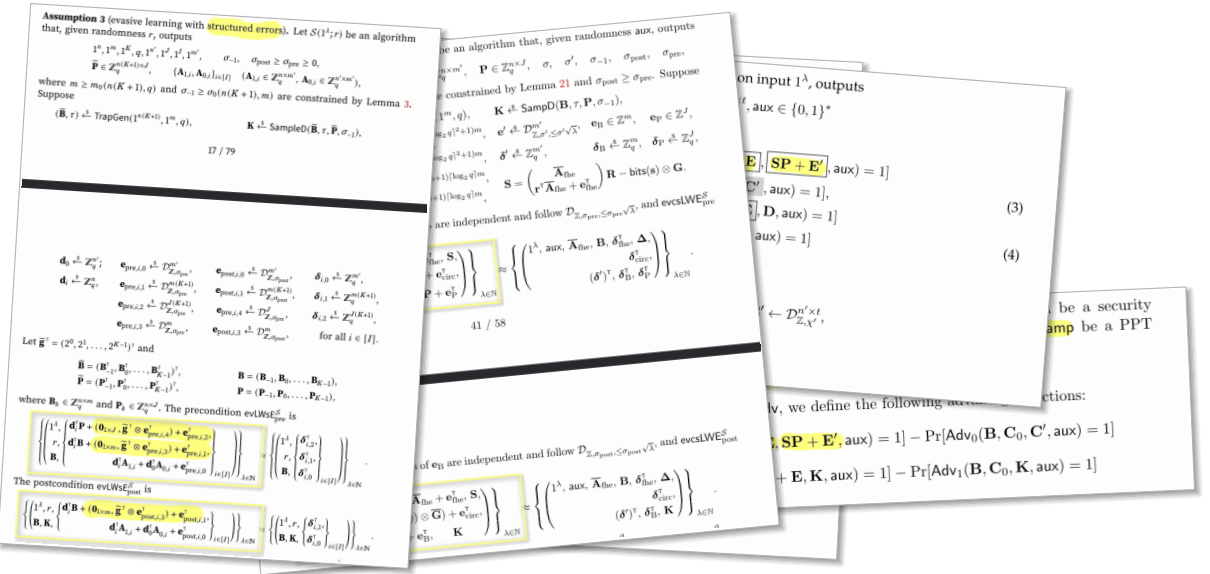
$$\mathcal{A}^{\mathrm{PRE}}_{\mathsf{Adv}}(\lambda) := \Pr[\mathsf{Adv}_0(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) = 1] - \Pr[\mathsf{Adv}_0(\mathbf{B}, \mathbf{C}_0, \mathbf{C}', \mathsf{aux}) = 1]$$

$$\mathcal{A}^{\mathrm{POST}}_{\mathsf{Adv}}(\lambda) := \Pr[\mathsf{Adv}_1(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{K}, \mathsf{aux}) = 1] - \Pr[\mathsf{Adv}_1(\mathbf{B}, \mathbf{C}_0, \mathbf{K}, \mathsf{aux}) = 1]$$

But... They are almost always different



But... They are almost always different



But... They are almost always different

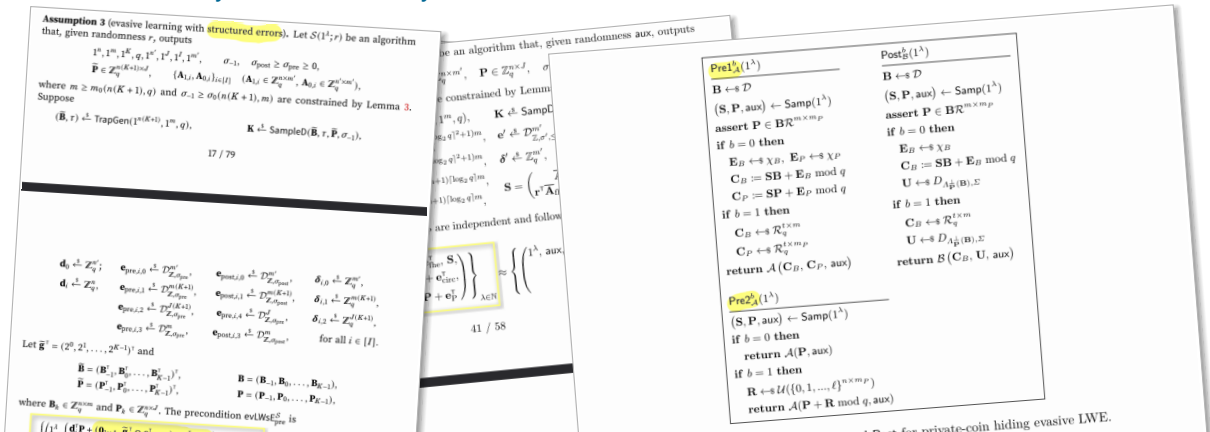

Assumption 3 (evasive learning with structured errors). Let $\mathcal{S}(1^\lambda; r)$ be an algorithm that, given randomness r, outputs
$1^n, 1^m, 1^K, q, 1^{n'}, 1^{I'}, 1^{m'}, \quad \sigma_{-1}, \quad \sigma_{\text{post}} \geq \sigma_{\text{pre}} \geq 0,$
$\overline{\mathbf{P}} \in \mathbb{Z}_q^{m(K+1)\times I}, \quad \{\mathbf{A}_{i,l}, \mathbf{A}_{0,l}\}_{i\in[I]} \quad \{\mathbf{A}_{i,l} \in \mathbb{Z}_q^{n\times m}, \mathbf{A}_{0,l} \in \mathbb{Z}_q^{n'\times m}\},$
where $m \geq m_0(n(K+1), q)$ and $\sigma_{-1} \geq \sigma_0(n(K+1), m)$ are constrained by Lemma 3. Suppose
$(\overline{\mathbf{B}}, \tau) \xleftarrow{\$} \mathsf{TrapGen}(1^{n(K+1)}, 1^m, q), \qquad \mathbf{K} \xleftarrow{\$} \mathsf{SampleD}(\overline{\mathbf{B}}, \tau, \overline{\mathbf{P}}, \sigma_{-1}),$
17 / 79
$\mathbf{d}_0 \xleftarrow{\$} \mathbb{Z}_q^{m'}; \quad \mathbf{e}_{\text{pre},l,0} \xleftarrow{\$} \mathcal{D}^{m'}_{\mathbb{Z},\sigma_{\text{pre}}}, \quad \mathbf{e}_{\text{post},l,0} \xleftarrow{\$} \mathcal{D}^{m'}_{\mathbb{Z},\sigma_{\text{post}}}, \quad \boldsymbol{\delta}_{l,0} \xleftarrow{\$} \mathbb{Z}_q^{m'},$
$\mathbf{d}_i \xleftarrow{\$} \mathbb{Z}_q^n, \quad \mathbf{e}_{\text{pre},i,1} \xleftarrow{\$} \mathcal{D}^{m(K+1)}_{\mathbb{Z},\sigma_{\text{pre}}}, \quad \mathbf{e}_{\text{post},i,1} \xleftarrow{\$} \mathcal{D}^{m(K+1)}_{\mathbb{Z},\sigma_{\text{post}}}, \quad \boldsymbol{\delta}_{i,1} \xleftarrow{\$} \mathbb{Z}_q^{m(K+1)},$
$\mathbf{e}_{\text{pre},i,2} \xleftarrow{\$} \mathcal{D}^{d(K+1)}_{\mathbb{Z},\sigma_{\text{pre}}}, \quad \mathbf{e}_{\text{pre},i,4} \xleftarrow{\$} \mathcal{D}^{d}_{\mathbb{Z},\sigma_{\text{pre}}}, \quad \boldsymbol{\delta}_{i,2} \xleftarrow{\$} \mathbb{Z}_q^{d(K+1)},$
$\mathbf{e}_{\text{pre},i,3} \xleftarrow{\$} \mathcal{D}^{m}_{\mathbb{Z},\sigma_{\text{pre}}}, \quad \mathbf{e}_{\text{post},i,3} \xleftarrow{\$} \mathcal{D}^{m}_{\mathbb{Z},\sigma_{\text{post}}}, \quad \text{for all } i \in [I].$
Let $\overline{\mathbf{g}}^\top = (2^0, 2^1, \ldots, 2^{K-1})^\top$ and
$\overline{\mathbf{B}} = (\mathbf{B}^\top_{-1}, \mathbf{B}^\top_0, \ldots, \mathbf{B}^\top_{K-1})^\top, \qquad \mathbf{B} = (\mathbf{B}_{-1}, \mathbf{B}_0, \ldots, \mathbf{B}_{K-1}),$
$\overline{\mathbf{P}} = (\mathbf{P}^\top_{-1}, \mathbf{P}^\top_0, \ldots, \mathbf{P}^\top_{K-1})^\top, \qquad \mathbf{P} = (\mathbf{P}_{-1}, \mathbf{P}_0, \ldots, \mathbf{P}_{K-1}),$
where $\mathbf{B}_k \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{P}_k \in \mathbb{Z}_q^{n\times I}$. The precondition $\mathsf{evLWSE}^{\mathcal{S}}_{\text{pre}}$ is
$\left\{\left(1^\lambda, \begin{matrix} \mathbf{d}_i^\top\mathbf{P} + (\mathbf{0}_{1\times m}, \overline{\mathbf{g}}^\top \otimes \mathbf{e}^\top_{\text{pre},i,4}) + \mathbf{e}^\top_{\text{pre},i,2} \\ \mathbf{d}_i^\top\mathbf{B} + (\mathbf{0}_{1\times m}, \overline{\mathbf{g}}^\top \otimes \mathbf{e}^\top_{\text{pre},i,3}) + \mathbf{e}^\top_{\text{pre},i,1} \end{matrix}, \begin{matrix} r, \\ \mathbf{B}, \end{matrix} \begin{matrix} \mathbf{d}_i^\top\mathbf{A}_{i,l} + \mathbf{d}_0^\top\mathbf{A}_{0,l} + \mathbf{e}^\top_{\text{pre},i,0} \\ \end{matrix}_{i\in[I]}\right)\right\}_{\lambda\in\mathbb{N}} \approx \left\{\left(1^\lambda, \begin{matrix} \boldsymbol{\delta}_{i,2}^\top, \\ \boldsymbol{\delta}_{i,1}^\top, \\ \boldsymbol{\delta}_{i,0}^\top \end{matrix}_{i\in[I]}, \begin{matrix} r, \\ \mathbf{B}, \end{matrix} \begin{matrix} \boldsymbol{\delta}_{i,2}^\top, \\ \boldsymbol{\delta}_{i,1}^\top, \\ \boldsymbol{\delta}_{i,0}^\top \end{matrix}_{i\in[I]}\right)\right\}_{\lambda\in\mathbb{N}}.$
The postcondition $\mathsf{evLWSE}^{\mathcal{S}}_{\text{post}}$ is
$\left\{\left(1^\lambda, r, \begin{matrix} \mathbf{d}_i^\top\mathbf{B} + (\mathbf{0}_{1\times m}, \overline{\mathbf{g}}^\top \otimes \mathbf{e}^\top_{\text{post},i,3}) + \mathbf{e}^\top_{\text{post},i,1} \\ \mathbf{d}_i^\top\mathbf{A}_{i,l} + \mathbf{d}_0^\top\mathbf{A}_{0,l} + \mathbf{e}^\top_{\text{post},i,0} \end{matrix}_{i\in[I]}\right)\right\}_{\lambda\in\mathbb{N}} \approx \left\{\left(1^\lambda, r, \begin{matrix} \boldsymbol{\delta}_{i,2}^\top, \\ \boldsymbol{\delta}_{i,0}^\top \end{matrix}_{i\in[I]}\right)\right\}_{\lambda\in\mathbb{N}}.$
be an algorithm that, given randomness aux, outputs
$\mathbf{P} \in \mathbb{Z}_q^{m\times I}, \quad \sigma$
constrained by Lemm
$\mathbf{K} \xleftarrow{\$} \mathsf{SampD}$
$\mathbf{e}' \xleftarrow{\$} \mathcal{D}^{m'}_{\mathbb{Z},\sigma'}$
$\boldsymbol{\delta}' \xleftarrow{\$} \mathbb{Z}_q^{m'},$
$\mathbf{S} = \begin{pmatrix} \mathbf{r}^\top\overline{\mathbf{A}}_{\text{fl}} \end{pmatrix}$
are independent and follow
$\left\{\begin{matrix} \overline{\mathbf{A}}_{\text{fl}}, \mathbf{S}, \\ \mathbf{r}^\top\overline{\mathbf{B}}, \\ \mathbf{r}^\top\overline{\mathbf{P}} + \mathbf{e}^\top_{\text{fl},\text{sec}}, \\ \mathbf{K} \end{matrix}\right\}_{\lambda\in\mathbb{N}} \approx \left\{\left(1^\lambda, \text{aux}, \right.\right.$
41 / 58
of $\mathbf{e}_{\text{fl}}$ are independent and follow
$\left\{\begin{matrix} \overline{\mathbf{A}}_{\text{fl}}, \mathbf{S}, \\ \mathbf{r}^\top\overline{\mathbf{B}}, \\ \mathbf{r}^\top\overline{\mathbf{P}} + \mathbf{e}^\top_{\text{fl},\text{sec}}, \\ \mathbf{K} \end{matrix}\right\}_{\lambda\in\mathbb{N}} \approx \left\{\left(1^\lambda, \text{au}\right.\right.$
$\mathsf{Pre1}^{\mathcal{A}}_{\mathcal{A}}(1^\lambda)$
$\mathbf{B} \leftarrow\!\$\ \mathcal{D}$
$(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$
assert $\mathbf{P} \in \mathbb{B}\mathcal{R}^{m\times m}$
if $b = 0$ then
$\mathbf{E}_B \leftarrow\!\$\ \chi_B$, $\mathbf{E}_P \leftarrow\!\$\ \chi_P$
$\mathbf{C}_B := \mathbf{SB} + \mathbf{E}_B \bmod q$
$\mathbf{C}_P := \mathbf{SP} + \mathbf{E}_P \bmod q$
if $b = 1$ then
$\mathbf{C}_B \leftarrow\!\$\ \mathcal{R}_q^{t\times m}$
$\mathbf{C}_P \leftarrow\!\$\ \mathcal{R}_q^{t\times m_P}$
return $\mathcal{A}(\mathbf{C}_B, \mathbf{C}_P, \text{aux})$
$\mathsf{Pre2}^{b}_{\mathcal{A}}(1^\lambda)$
$(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$
if $b = 0$ then
return $\mathcal{A}(\mathbf{P}, \text{aux})$
if $b = 1$ then
$\mathbf{R} \leftarrow\!\$\ \mathcal{U}(\{0,1,\ldots,\ell\}^{n\times m_P})$
return $\mathcal{A}(\mathbf{P} + \mathbf{R} \bmod q, \text{aux})$
$\mathsf{Post}^{b}_{\mathcal{B}}(1^\lambda)$
$\mathbf{B} \leftarrow\!\$\ \mathcal{D}$
$(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$
assert $\mathbf{P} \in \mathbb{B}\mathcal{R}^{m\times m_P}$
if $b = 0$ then
$\mathbf{E}_B \leftarrow\!\$\ \chi_B$
$\mathbf{C}_B := \mathbf{SB} + \mathbf{E}_B \bmod q$
$\mathbf{U} \leftarrow\!\$\ D_{\Lambda^\perp_{\mathbf{B}}(\mathbf{B}),\Sigma}$
if $b = 1$ then
$\mathbf{C}_B \leftarrow\!\$\ \mathcal{R}_q^{t\times m}$
$\mathbf{U} \leftarrow\!\$\ D_{\Lambda^\perp_{\mathbf{B}}(\mathbf{B}),\Sigma}$
return $\mathcal{B}(\mathbf{C}_B, \mathbf{U}, \text{aux})$

Fig. 4: Experiments Pre1, Pre2 and Post for private-coin hiding evasive LWE.

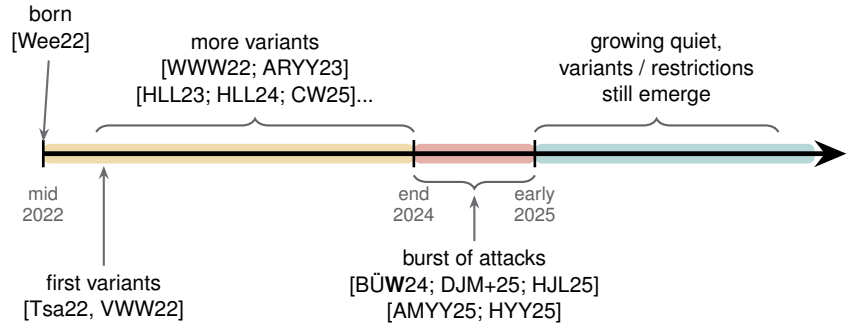
$$\mathsf{Adv}^{\mathsf{Post}}_{\mathcal{B}}(\lambda) := \left|\Pr\left[\mathsf{Post}^0_{\mathcal{B}}(1^\lambda) = 1\right] - \Pr\left[\mathsf{Post}^1_{\mathcal{B}}(1^\lambda) = 1\right]\right|.$$

The $\mathsf{PrivateHideEvLWE}_{\mathsf{param}}$ *assumption states that for any PPT* Samp *and* $\mathcal{B}$ *there exists a PPT* $\mathcal{A}$ *such that* $\mathsf{Adv}^{\mathsf{Pre1}}_{\mathcal{A}}(\lambda) + \mathsf{Adv}^{\mathsf{Pre2}}_{\mathcal{A}}(\lambda) \geq \mathsf{Adv}^{\mathsf{Post}}_{\mathcal{B}}(\lambda)/\mathsf{poly}(\lambda) - \mathsf{negl}(\lambda)$.

This talk

- Brief summary of development
- An example attack
- On relating different evasive LWE variants
- A specific variant + target **P** of interest
- Characterisation?

Timeline



- Why so many variants:
  Many applications define their own specific “if–then pair”, each induces a new variant

Status

- Many variants in the literature, some broken, some not
  - Additional LWE samples in both “if” and “then” [Wee22]
  - “Private-coin” variants [VWW22; Tsa22; ARYY23; BÜ**W**24]
  - Circular variants [HLL23; CW25]
  - Multiple tuples of $(\mathbf{A}_i, \mathbf{P}_i)$ + their LWE samples/ preimages [WWW22; CL**W**24]
  - Structured LWE errors [HLL24]
  - .....

Status

- Many variants in the literature, some broken, some not
  - Additional LWE samples in both “if” and “then” [Wee22]
  - “Private-coin” variants [VWW22; Tsa22; ARYY23; BÜ**W**24]
  - Circular variants [HLL23; CW25]
  - Multiple tuples of $(\mathbf{A}_i, \mathbf{P}_i)$ + their LWE samples/ preimages [WWW22; CL**W**24]
  - Structured LWE errors [HLL24]
  - .....
- Attacks are variant-specific

  $\Longrightarrow$ No clear explanation to why some broken, some not (or not yet?)
- IMO: We do not have an answer...
  - Are there plausible variants, if so which ones?
  - How to reasonably characterise these variants?

Quick note on “public-” and “private-”coin

- Common in literature to distinguish “public-coin” and “private-coin”
- “Private-coin” introduced in [VWW22] in form of discussion. Actual assumption:
  (1) Randomness used to sample $\mathbf{P}$ is withheld, i.e. “private-coin Samp”, and
  (2) Involves correlated $(\mathbf{s}, \mathbf{P}, \text{aux})$ in problem instance

Quick note on “public-” and “private-”coin

- Common in literature to distinguish “public-coin” and “private-coin”
- “Private-coin” introduced in [VWW22] in form of discussion. Actual assumption:
  (1) Randomness used to sample $\mathbf{P}$ is withheld, i.e. “private-coin Samp”, and
  (2) Involves correlated $(\mathbf{s}, \mathbf{P}, \text{aux})$ in problem instance
- “Public-coin”: $\neg(1)$ or $\neg(2)$ or both? Interpretation differed in literature
- Possible to interpret some variants / attacks as either (e.g. [HLL23; BÜW24; AMYY25]...)
- Lack of precision (e.g. “public-coin” = many incomparable definitions)

Quick note on “public-” and “private-”coin

- Common in literature to distinguish “public-coin” and “private-coin”
- “Private-coin” introduced in [VWW22] in form of discussion. Actual assumption:
  (1) Randomness used to sample **P** is withheld, i.e. “private-coin Samp”, and
  (2) Involves correlated $(\mathbf{s}, \mathbf{P}, \mathsf{aux})$ in problem instance
- “Public-coin”: $\neg(1)$ or $\neg(2)$ or both? Interpretation differed in literature
- Possible to interpret some variants / attacks as either (e.g. [HLL23; BÜW24; AMYY25]...)
- Lack of precision (e.g. “public-coin” = many incomparable definitions)
- This talk: These prefixes / terminologies will not be used
  A variant is stated whenever referred to, not classified by a name

(Will get back to this towards the end)

Attack = disproving asserted implication

Recap:
$\forall$ PPT Samp, PPT $\mathcal{B}$,
$\exists$ PPT $\mathcal{A}$, polynomial $p(\lambda)$, negl. function $\epsilon(\lambda)$ s.t.

$$\mathsf{Adv}^{\mathsf{Post}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{Pre}}_{\mathcal{A}}(\lambda)/p(\lambda) - \epsilon(\lambda).$$

$\mathsf{Pre}^b_{\mathcal{A}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{P}, \ldots) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

if $b = 0$ **then** $\ldots$

if $b = 1$ **then** $\ldots$

/ Distinguishing problem w/o preimages

return $\mathcal{A}\left(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{c}_P, \ldots\right)$

$\mathsf{Post}^b_{\mathcal{B}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{P}, \ldots) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

if $b = 0$ **then** $\ldots$

if $b = 1$ **then** $\ldots$

/ Distinguishing problem w. preimages

return $\mathcal{B}\left(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{X}, \ldots\right)$

Attack = disproving asserted implication

Recap:
$\forall$ PPT Samp, PPT $\mathcal{B}$,
$\exists$ PPT $\mathcal{A}$, polynomial $p(\lambda)$, negl. function $\epsilon(\lambda)$ s.t.

$$\mathsf{Adv}^{\mathsf{Post}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{Pre}}_{\mathcal{A}}(\lambda)/p(\lambda) - \epsilon(\lambda).$$

$\mathsf{Pre}^b_{\mathcal{A}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{P}, \ldots) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

if $b = 0$ **then** $\ldots$

if $b = 1$ **then** $\ldots$

/ Distinguishing problem w/o preimages

return $\mathcal{A}\left(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{c}_P, \ldots\right)$

$\mathsf{Post}^b_{\mathcal{B}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{P}, \ldots) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

if $b = 0$ **then** $\ldots$

if $b = 1$ **then** $\ldots$

/ Distinguishing problem w. preimages

return $\mathcal{B}\left(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{X}, \ldots\right)$

Pre is hard (i.e. “if” holds) $\Longrightarrow$ Post is hard (i.e. “then” holds)

evLWE

Attack = disproving asserted implication

Recap:
$\forall$ PPT Samp, PPT $\mathcal{B}$,
$\exists$ PPT $\mathcal{A}$, polynomial $p(\lambda)$, negl. function $\epsilon(\lambda)$ s.t.

$$\mathsf{Adv}^{\mathsf{Post}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{Pre}}_{\mathcal{A}}(\lambda)/p(\lambda) - \epsilon(\lambda).$$

$\mathsf{Pre}^b_{\mathcal{A}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{P}, \ldots) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

if $b = 0$ **then** ...

if $b = 1$ **then** ...

/ Distinguishing problem w/o preimages

return $\mathcal{A}\,(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{c}_P, \ldots)$

$\mathsf{Post}^b_{\mathcal{B}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$

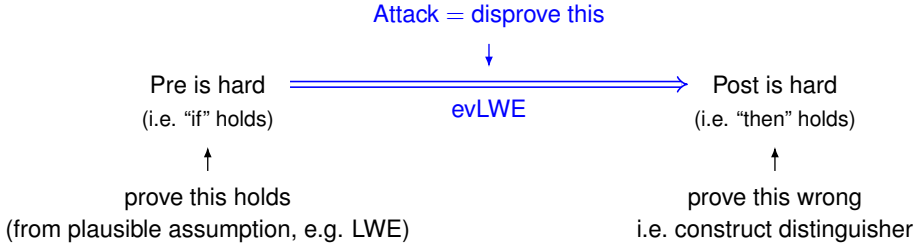
$(\mathbf{P}, \ldots) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

if $b = 0$ **then** ...

if $b = 1$ **then** ...

/ Distinguishing problem w. preimages

return $\mathcal{B}\,(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{X}, \ldots)$



Example Attack (adapted from [DJM+25])

(Variant adapted from [BÜW24]) For all $(\mathbf{s}, \mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}(1^\lambda; \text{rand})$,

Pre:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	\$,	\$, aux)
Post:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{X},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	\$,	$\mathbf{X}$, aux)

Example Attack (adapted from [DJM+25])

(Variant adapted from [BÜW24]) For all $(\mathbf{s}, \mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}(1^\lambda; \text{rand})$,

Pre:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	$\$,$	$\$,$	aux)
Post:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{X},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	$\$,$	$\mathbf{X},$	aux)

- Idea: Let $\mathbf{s}, \mathbf{P}$ uniform, leak LSB of $\mathbf{s}^\mathsf{T}\mathbf{P} \bmod q$ via aux.

$$\text{aux} := \mathbf{s}^\mathsf{T}\mathbf{P} - 2\mathbf{t}^\mathsf{T} \bmod q, \quad \mathbf{t} \leftarrow\$ \{0, \ldots, \lfloor q/2 \rfloor\}^k, \quad q \text{ odd}$$

Example Attack (adapted from [DJM+25])

(Variant adapted from [BÜW24]) For all $(\mathbf{s}, \mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}(1^\lambda; \text{rand})$,

Pre:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	$\$,$	$\$,$	aux)
Post:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{X},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	$\$,$	$\mathbf{X},$	aux)

- Idea: Let $\mathbf{s}, \mathbf{P}$ uniform, leak LSB of $\mathbf{s}^\mathsf{T}\mathbf{P} \bmod q$ via aux.

$$\text{aux} := \mathbf{s}^\mathsf{T}\mathbf{P} - 2\mathbf{t}^\mathsf{T} \bmod q, \quad \mathbf{t} \leftarrow\$ \{0, \ldots, \lfloor q/2 \rfloor\}^k, \quad q \text{ odd}$$

1. Pre indistinguishable under LWE:

   LWE + noise-flooding: $(\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},\ \mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T},\ \text{aux}) \approx_c (\$_A^\mathsf{T},\ \$_P^\mathsf{T} + \mathbf{e}_P^\mathsf{T},\ \$_P^\mathsf{T} - 2\mathbf{t}^\mathsf{T})$

   Next $(\$_P + \mathbf{e}_P, \$_P - 2\mathbf{t}) \approx_s (\$_P - 2\mathbf{t} + 2\mathbf{t} + \mathcal{U}(\{0,1\}^k) + \mathbf{e}_P, \$_P - 2\mathbf{t}) \approx_s (\$, \$_P - 2\mathbf{t})$

Example Attack (adapted from [DJM+25])

(Variant adapted from [BÜW24]) For all $(\mathbf{s}, \mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}(1^\lambda; \text{rand})$,

Pre:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	$\$,$	$\$,$	aux)
Post:	$(\mathbf{A},$	$\mathbf{P},$	$\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},$	$\mathbf{X},$	aux)	$\approx_c$	$(\mathbf{A},$	$\mathbf{P},$	$\$,$	$\mathbf{X},$	aux)

- Idea: Let $\mathbf{s}, \mathbf{P}$ uniform, leak LSB of $\mathbf{s}^\mathsf{T}\mathbf{P} \bmod q$ via aux.

$$\text{aux} := \mathbf{s}^\mathsf{T}\mathbf{P} - 2\mathbf{t}^\mathsf{T} \bmod q, \quad \mathbf{t} \leftarrow\$ \{0, \ldots, \lfloor q/2 \rfloor\}^k, \quad q \text{ odd}$$

1. Pre indistinguishable under LWE:

   LWE + noise-flooding: $(\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T},\ \mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T},\ \text{aux}) \approx_c (\$_A^\mathsf{T},\ \$_P^\mathsf{T} + \mathbf{e}_P^\mathsf{T},\ \$_P^\mathsf{T} - 2\mathbf{t}^\mathsf{T})$

   Next $(\$_P + \mathbf{e}_P, \$_P - 2\mathbf{t}) \approx_s (\$_P - 2\mathbf{t} + 2\mathbf{t} + \mathcal{U}(\{0,1\}^k) + \mathbf{e}_P, \$_P - 2\mathbf{t}) \approx_s (\$, \$_P - 2\mathbf{t})$

2. Post distinguishable:

   LHS: $(\mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T}) \cdot \mathbf{X} - \text{aux} \bmod q = \mathbf{e}_A^\mathsf{T}\mathbf{X} + 2\mathbf{t}^\mathsf{T} \bmod q = \mathbf{e}_A^\mathsf{T}\mathbf{X} + 2\mathbf{t}^\mathsf{T}$ w.h.p. (no wrap-around)

   Take mod2 $\implies$ quantity in row span of $\mathbf{X}$ mod 2

Other variants and attacks (not exhaustive)

Variant	Applications	Attack on		Application from other assumptions*
		Assumption	Scheme	
[Wee22]	CP-ABE	No	No	Yes#
[Tsa22]	WE	Yes [BÜW24]	No	No
[VWW22]	WE, null-iO	Yes [BÜW24]	No	No
[WWW22]	MA-ABE (subset policy)	No	No	No
[ARYY23]	MI-ABE	Yes [BÜW24]	No	No
[HLL23]	unbounded-depth ABE	Yes [AMYY25]	No	No
[BÜW24]	–	Yes [DJM+25]	–	–
[BDJ+25]	pseudorandom iO	Yes [AMYY25]	Yes	No
[AKY25]	pseudorandom FE	Yes [AMYY25] → No	Yes → No	No
⋮	⋮	⋮	⋮	⋮

Table: Evasive LWE variants and attacks (not exhaustive). $*$: Counts only lattice-based results, excludes "assume construction is secure". $\#$: from succinct/decomposed LWE. Yes → No: Attacked then patched.

- Assumption quantifies over all $\mathbf{P}$ (maybe also $\mathbf{s}$, aux) / "for all $(\mathbf{P}, \ldots) \leftarrow$ Samp, it holds ..."

  $\Longrightarrow$ Attack on assumption does not necessarily break its application

Questions

- More **attacks**: On standing variants / with new techniques
- **Reduction** between variants $\Longrightarrow$ narrow down landscape
- Analysis to **justify standing variant** (possibly on specific target **P**)
- Meaningful **characterisation**
  - Capture existing variants + consistent with known knowledge
  - Answer to settings where assumption is broken but its application not
- Achieve **applications from better assumptions**

On relating evasive LWE variants

Suppose want to show:

Assume Variant-A holds, then Variant-B holds.

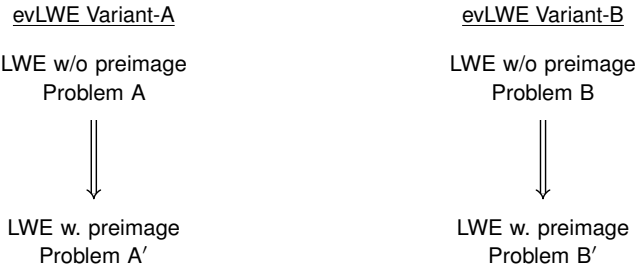
- Same Pre and Post games, only quantifiers differ (easy)
  E.g. Variant-A: "For all $(\mathbf{P}, \text{aux}) \leftarrow \text{Samp}$", Variant-B: "For all $\mathbf{P} \leftarrow \text{Samp}$"

On relating evasive LWE variants

Suppose want to show:

Assume Variant-A holds, then Variant-B holds.

- Same Pre and Post games, only quantifiers differ (easy)
  E.g. Variant-A: "For all $(\mathbf{P}, \text{aux}) \leftarrow \text{Samp}$", Variant-B: "For all $\mathbf{P} \leftarrow \text{Samp}$"
- Different Pre and Post games $\implies$ Need to relate four different problems

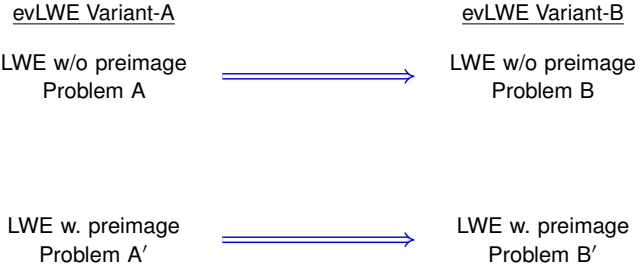


On relating evasive LWE variants

Suppose want to show:

Assume Variant-A holds, then Variant-B holds.

- Same Pre and Post games, only quantifiers differ (easy)
  E.g. Variant-A: "For all $(\mathbf{P}, \text{aux}) \leftarrow \text{Samp}$", Variant-B: "For all $\mathbf{P} \leftarrow \text{Samp}$"
- Different Pre and Post games $\implies$ Need to relate four different problems
  Naive idea that does **not** work:

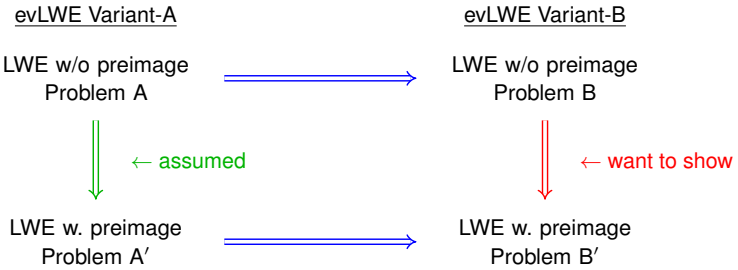


On relating evasive LWE variants

Suppose want to show:

Assume Variant-A holds, then Variant-B holds.

- Same Pre and Post games, only quantifiers differ (easy)
  E.g. Variant-A: "For all $(\mathbf{P}, \mathsf{aux}) \leftarrow \mathsf{Samp}$", Variant-B: "For all $\mathbf{P} \leftarrow \mathsf{Samp}$"
- Different Pre and Post games $\implies$ Need to relate four different problems
  Naive idea that does **not** work:



Any particular interesting variant / target?

Any particular interesting variant / target?

Recap of [Wee22,Wee24]:

$\mathsf{Pre}^b_{\mathcal{A}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m};\ \mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

$\mathbf{s} \leftarrow\!\$\ \mathbb{Z}_q^n,\ \mathbf{e}_A \leftarrow\!\$\ \mathcal{D}^m_{\mathbb{Z},\chi_A},\ \mathbf{e}_P \leftarrow\!\$\ \mathcal{D}^k_{\mathbb{Z},\chi_P}$

if $b = 0$ **then**

$\mathbf{c}_A^\mathsf{T} \coloneqq \mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T} \bmod q$

$\mathbf{c}_P^\mathsf{T} \coloneqq \mathbf{s}^\mathsf{T}\mathbf{P} + \mathbf{e}_P^\mathsf{T} \bmod q$

if $b = 1$ **then**

$\mathbf{c}_A \leftarrow\!\$\ \mathbb{Z}_q^m;\ \mathbf{c}_P \leftarrow\!\$\ \mathbb{Z}_q^k$

return $\mathcal{A}\left(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{c}_P, \mathsf{rand}\right)$

$\mathsf{Post}^b_{\mathcal{B}}(1^\lambda)$

$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}:\ \mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

$\mathbf{s} \leftarrow\!\$\ \mathbb{Z}_q^n,\ \mathbf{e}_A \leftarrow\!\$\ \mathcal{D}^m_{\mathbb{Z},\chi_A}$

if $b = 0$ **then**

$\mathbf{c}_A^\mathsf{T} \coloneqq \mathbf{s}^\mathsf{T}\mathbf{A} + \mathbf{e}_A^\mathsf{T} \bmod q$

$\mathbf{X} \leftarrow\!\$\ \mathcal{D}_{\Lambda^{\mathbf{P}}_q(\mathbf{A}),\sigma}$

if $b = 1$ **then**

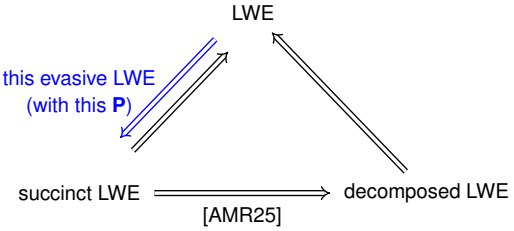
$\mathbf{c}_A \leftarrow\!\$\ \mathbb{Z}_q^m,\ \mathbf{X} \leftarrow\!\$\ \mathcal{D}_{\Lambda^{\mathbf{P}}_q(\mathbf{A}),\sigma}$

return $\mathcal{B}\left(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{X}, \mathsf{rand}\right)$

- No known attack on this (relatively simple) version
- Above + standard LWE $\implies$ succinct LWE [Wee24]

Evasive LWE vs. succinct LWE vs. decomposed LWE

- Evasive LWE: Pre $\implies$ Post (for any $\mathbf{P}$)
- Let $\mathbf{P} = [\mathbf{W}_1\mathbf{R}, \ldots, \mathbf{W}_\ell\mathbf{R}]$, where $\mathbf{W}_i \leftarrow\$ \mathbb{Z}_q^{n\times m}\ \ \forall i \in [\ell]$, $\mathbf{R} \leftarrow\$ \mathcal{D}_{\mathbb{Z},\sigma}^{n\times 2\ell m}$
- [Wee24] showed: LWE $\implies$ Pre with this $\mathbf{P}$; Post with this $\mathbf{P}$ $\implies$ ℓ-succinct LWE



$\mathsf{Pre}^b_{\mathcal{A}}(1^\lambda)$

$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m};\ \mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

$\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n,\ \mathbf{e}_A \leftarrow\$ \mathcal{D}_{\mathbb{Z},\chi_A}^m,\ \mathbf{e}_P \leftarrow\$ \mathcal{D}_{\mathbb{Z},\chi_P}^k$

if $b = 0$ **then**

$\mathbf{c}_A^\intercal := \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_A^\intercal \bmod q$

$\mathbf{c}_P^\intercal := \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_P^\intercal \bmod q$

if $b = 1$ **then**

$\mathbf{c}_A \leftarrow\$ \mathbb{Z}_q^m,\ \mathbf{c}_P \leftarrow\$ \mathbb{Z}_q^k$

return $\mathcal{A}(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{c}_P, \mathsf{rand})$

$\mathsf{Post}^b_{\mathcal{B}}(1^\lambda)$

$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}:\ \mathbf{P} \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{rand})$

$\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n,\ \mathbf{e}_A \leftarrow\$ \mathcal{D}_{\mathbb{Z},\chi_A}^m$

if $b = 0$ **then**

$\mathbf{c}_A^\intercal := \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_A^\intercal \bmod q$

$\mathbf{X} \leftarrow\$ \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),\sigma}$

if $b = 1$ **then**

$\mathbf{c}_A \leftarrow\$ \mathbb{Z}_q^m;\ \mathbf{X} \leftarrow\$ \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),\sigma}$

return $\mathcal{B}(\mathbf{A}, \mathbf{P}, \mathbf{c}_A, \mathbf{X}, \mathsf{rand})$

Mutation 101

- Not “private-coin” (independent sampling of **S** and **P**)
- Not “public-coin” (coins not required to be given) ← as with all natural lattice assumptions

$\underline{\mathsf{Pre}^b_{\mathcal{A}}(1^\lambda)}$

$\mathbf{A} \leftarrow\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{S}, \mathsf{aux}_S) \leftarrow \mathsf{SampS}(1^\lambda)$

$(\mathbf{P}, \mathsf{aux}_P) \leftarrow \mathsf{SampP}(1^\lambda)$

$\mathbf{E}_A \leftarrow\$\ \mathcal{D}^{t\times m}_{\mathbb{Z},\chi_A};\ \mathbf{E}_P \leftarrow\$\ \mathcal{D}^{t\times k}_{\mathbb{Z},\chi_P}$

if $b = 0$ **then**

$\quad \mathbf{C}_A := \mathbf{SA} + \mathbf{E}_A \bmod q$

$\quad \mathbf{C}_P := \mathbf{SP} + \mathbf{E}_P \bmod q$

if $b = 1$ **then**

$\quad \mathbf{C}_A \leftarrow\$\ \mathbb{Z}_q^{t\times m};\ \mathbf{C}_P \leftarrow\$\ \mathbb{Z}_q^{t\times k}$

return $\mathcal{A}\left(\mathbf{A}, \mathbf{P}, \mathbf{C}_A, \mathbf{C}_P, \mathsf{aux}_S, \mathsf{aux}_P\right)$

$\underline{\mathsf{Post}^b_{\mathcal{B}}(1^\lambda)}$

$\mathbf{A} \leftarrow\$\ \mathbb{Z}_q^{n\times m}$

$(\mathbf{S}, \mathsf{aux}_S) \leftarrow \mathsf{SampS}(1^\lambda)$

$(\mathbf{P}, \mathsf{aux}_P) \leftarrow \mathsf{SampP}(1^\lambda)$

$\mathbf{E}_A \leftarrow\$\ \mathcal{D}^{t\times m}_{\mathbb{Z},\chi_A}$

if $b = 0$ **then**

$\quad \mathbf{C}_A := \mathbf{SA} + \mathbf{E}_A \bmod q$

$\quad \mathbf{X} \leftarrow\$\ \mathcal{D}_{\Lambda^{\mathbf{P}}_q(\mathbf{A}),\sigma}$

if $b = 1$ **then**

$\quad \mathbf{C}_A \leftarrow\$\ \mathbb{Z}_q^{t\times m};\ \mathbf{X} \leftarrow\$\ \mathcal{D}_{\Lambda^{\mathbf{P}}_q(\mathbf{A}),\sigma}$

return $\mathcal{B}\left(\mathbf{A}, \mathbf{P}, \mathbf{C}_A, \mathbf{X}, \mathsf{aux}_S, \mathsf{aux}_P\right)$

Afaik no attack. Wanted: Break it.
Or draw reductions, or reprove some orphan applications.

Thanks to Hoeteck Wee and Russell Lai for helpful discussions.

Summary

This talk:

- Background, example attack, on relating variants, relation to succinct LWE, Mutation 101

Wanted:

- **Attacks**: on standing variants / with new techniques
- **Reductions** between variants
- Analysis to **justify specific variant**/target **P**
- Meaningful **characterisation**, or, **kill Mutation 101**
- Applications from **better assumptions**

Others: Evasive SIS, check out Assumption Zoo

Ivy K. Y. Woo
Aalto University, Finland
ivy.woo@aalto.fi
ivyw.ooo

Thank You!

References I

[AKY25] Shweta Agrawal, Simran Kumari, and Shota Yamada. "Pseudorandom FE, iO and Applications". In: *TCC 2025, Part II*. Ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16269. LNCS. Springer, Cham, Dec. 2025, pp. 222–258. DOI: 10.1007/978-3-032-12293-3_8.

[AMR25] Damiano Abram, Giulio Malavolta, and Lawrence Roy. "Key-Homomorphic Computations for RAM: Fully Succinct Randomised Encodings and More". In: *CRYPTO 2025, Part III*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16002. LNCS. Springer, Cham, Aug. 2025, pp. 236–268. DOI: 10.1007/978-3-032-01881-6_8.

[AMYY25] Shweta Agrawal, Anuja Modi, Anshu Yadav, and Shota Yamada. "Zeroizing Attacks Against Evasive and Circular Evasive LWE". In: *TCC 2025, Part II*. Ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16269. LNCS. Springer, Cham, Dec. 2025, pp. 259–290. DOI: 10.1007/978-3-032-12293-3_9.

References II

[ARYY23] Shweta Agrawal, Mélissa Rossi, Anshu Yadav, and Shota Yamada. "Constant Input Attribute Based (and Predicate) Encryption from Evasive and Tensor LWE". In: *CRYPTO 2023, Part IV*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14084. LNCS. Springer, Cham, Aug. 2023, pp. 532–564. DOI: 10.1007/978-3-031-38551-3_17.

[BDJ+25] Pedro Branco, Nico Döttling, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, Spencer Peters, and Vinod Vaikuntanathan. "Pseudorandom Obfuscation and Applications". In: *CRYPTO 2025, Part V*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16004. LNCS. Springer, Cham, Aug. 2025, pp. 663–698. DOI: 10.1007/978-3-032-01901-1_21.

[BÜW24] Chris Brzuska, Akin Ünal, and Ivy K. Y. Woo. "Evasive LWE Assumptions: Definitions, Classes, and Counterexamples". In: *ASIACRYPT 2024, Part IV*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15487. LNCS. Springer, Singapore, Dec. 2024, pp. 418–449. DOI: 10.1007/978-981-96-0894-2_14.

[CW25] Valerio Cini and Hoeteck Wee. "Faster ABE for Turing Machines from Circular Evasive LWE". In: *EUROCRYPT 2025, Part III*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15603. LNCS. Springer, Cham, May 2025, pp. 94–125. DOI: 10.1007/978-3-031-91131-6_4.

References III

[DJM+25] Nico Döttling, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, and Vinod Vaikuntanathan. "Simple and General Counterexamples for Private-Coin Evasive LWE". In: *CRYPTO 2025, Part VII*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16006. LNCS. Springer, Cham, Aug. 2025, pp. 73–92. DOI: 10.1007/978-3-032-01907-3_3.

[HHY25] Tzu-Hsiang Huang, Wei-Hsiang Hung, and Shota Yamada. *A Note on Obfuscation-based Attacks on Private-coin Evasive LWE*. Cryptology ePrint Archive, Report 2025/421. 2025.

[HJL25] Yao-Ching Hsieh, Aayush Jain, and Huijia Lin. "Lattice-Based Post-quantum iO from Circular Security with Random Opening Assumption". In: *CRYPTO 2025, Part VII*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16006. LNCS. Springer, Cham, Aug. 2025, pp. 3–38. DOI: 10.1007/978-3-032-01907-3_1.

[HLL23] Yao-Ching Hsieh, Huijia Lin, and Ji Luo. "Attribute-Based Encryption for Circuits of Unbounded Depth from Lattices". In: *64th FOCS*. IEEE Computer Society Press, Nov. 2023, pp. 415–434. DOI: 10.1109/FOCS57990.2023.00031.

References IV

[HLL24] Yao-Ching Hsieh, Huijia Lin, and Ji Luo. "A General Framework for Lattice-Based ABE Using Evasive Inner-Product Functional Encryption". In: *EUROCRYPT 2024, Part II*. Ed. by Marc Joye and Gregor Leander. Vol. 14652. LNCS. Springer, Cham, May 2024, pp. 433–464. DOI: 10.1007/978-3-031-58723-8_15.

[Tsa22] Rotem Tsabary. "Candidate Witness Encryption from Lattice Techniques". In: *CRYPTO 2022, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. LNCS. Springer, Cham, Aug. 2022, pp. 535–559. DOI: 10.1007/978-3-031-15802-5_19.

[VWW22] Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. "Witness Encryption and Null-IO from Evasive LWE". In: *ASIACRYPT 2022, Part I*. Ed. by Shweta Agrawal and Dongdai Lin. Vol. 13791. LNCS. Springer, Cham, Dec. 2022, pp. 195–221. DOI: 10.1007/978-3-031-22963-3_7.

[Wee22] Hoeteck Wee. "Optimal Broadcast Encryption and CP-ABE from Evasive Lattice Assumptions". In: *EUROCRYPT 2022, Part II*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13276. LNCS. Springer, Cham, May 2022, pp. 217–241. DOI: 10.1007/978-3-031-07085-3_8.

References V

[Wee24] Hoeteck Wee. "Circuit ABE with poly(depth, λ)-Sized Ciphertexts and Keys from Lattices". In: *CRYPTO 2024, Part III*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14922. LNCS. Springer, Cham, Aug. 2024, pp. 178–209. DOI: 10.1007/978-3-031-68382-4_6.

[WWW22] Brent Waters, Hoeteck Wee, and David J. Wu. "Multi-authority ABE from Lattices Without Random Oracles". In: *TCC 2022, Part I*. Ed. by Eike Kiltz and Vinod Vaikuntanathan. Vol. 13747. LNCS. Springer, Cham, Nov. 2022, pp. 651–679. DOI: 10.1007/978-3-031-22318-1_23.