Evasive LWE Assumptions: Definitions, Classes, and Counterexamples

Chris Brzuska[1], Akin Ünal[2], **Ivy K. Y. Woo**[1]

[1] Aalto University, Finland
[2] ISTA, Austria

Asiacrypt @ Kolkata, 12 Dec 2024

LWE, and LWE given preimages

Learning with Errors (LWE) Assumption

For random wide matrix $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$ and sample $\mathbf{c} \in \mathbb{Z}_q^n$, hard to decide if $\mathbf{c}^\top$ equals

$\mathbf{s}^\top\mathbf{B} + \mathbf{e}^\top \bmod q$ or random

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

LWE, and LWE given preimages

Learning with Errors (LWE) Assumption

For random wide matrix $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$,

$$(\mathbf{B}, \quad \underset{\sim}{\mathbf{s}^\top \mathbf{B}}) \qquad \approx_c \qquad (\mathbf{B}, \quad \text{random})$$

where $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$ a uniform LWE secret.

- Notation:
  - $\underset{\sim}{\cdot}$ hides error term, $\underset{\sim}{\mathbf{s}^\top \mathbf{B}} = \mathbf{s}^\top \mathbf{B} + \mathbf{e}^\top \bmod q$

LWE, and LWE given preimages

Learning with Errors (LWE) Assumption

For random wide matrix $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$,

$$(\mathbf{B}, \quad \underset{\sim}{\mathbf{s}^\top\mathbf{B}}) \qquad \approx_c \qquad (\mathbf{B}, \quad \text{random})$$

where $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$ a uniform LWE secret.

- Notation:
  - $\underset{\sim}{\cdot}$ hides error term, $\underset{\sim}{\mathbf{s}^\top\mathbf{B}} = \mathbf{s}^\top\mathbf{B} + \mathbf{e}^\top \bmod q$
  - For arbitrary $\mathbf{P}$, write $\mathbf{B}^{-1}(\mathbf{P})$ for short (Gaussian) preimages s.t. $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P} \bmod q$

LWE, and LWE given preimages

Learning with Errors (LWE) Assumption

For random wide matrix $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n \times m}$,

$$(\mathbf{B}, \quad \underset{\sim}{\mathbf{s}^\top \mathbf{B}}) \qquad \approx_c \qquad (\mathbf{B}, \quad \text{random})$$

where $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$ a uniform LWE secret.

- Notation:
  - $\underset{\sim}{\cdot}$ hides error term, $\underset{\sim}{\mathbf{s}^\top \mathbf{B}} = \mathbf{s}^\top \mathbf{B} + \mathbf{e}^\top \bmod q$
  - For arbitrary $\mathbf{P}$, write $\mathbf{B}^{-1}(\mathbf{P})$ for short (Gaussian) preimages s.t. $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P} \bmod q$
- What if an (advanced) scheme requires leaking some short preimages $\mathbf{B}^{-1}(\mathbf{P})$?
- For many target $\mathbf{P}$, unclear how to simulate $\mathbf{B}^{-1}(\mathbf{P})$ in security proof

Evasive LWE

Evasive LWE Assumption (informal) [Wee22]

For random wide matrix $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any PPT generated $\mathbf{P}$,

$$\text{If} \quad (\mathbf{B}, \mathbf{P}, \underset{\sim}{\mathbf{s}^\top\mathbf{B}}, \underset{\sim}{\mathbf{s}^\top\mathbf{P}}) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \text{random})$$

$$\text{Then} \quad (\mathbf{B}, \mathbf{P}, \underset{\sim}{\mathbf{s}^\top\mathbf{B}}, \mathbf{B}^{-1}(\mathbf{P})) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \mathbf{B}^{-1}(\mathbf{P}))$$

Evasive LWE

Evasive LWE Assumption (informal) [Wee22]

For random wide matrix $\mathbf{B} \leftarrow\!\!\$\ \mathbb{Z}_q^{n\times m}$, and any PPT generated $\mathbf{P}$,

$$\begin{array}{llllllllll}
\text{If} & (\mathbf{B}, & \mathbf{P}, & \mathbf{s}^{\top}\mathbf{B}, & \mathbf{s}^{\top}\mathbf{P}) & \approx_c & (\mathbf{B}, & \mathbf{P}, & \text{random}, & \text{random}) \\
\text{Then} & (\mathbf{B}, & \mathbf{P}, & \mathbf{s}^{\top}\mathbf{B}, & \mathbf{B}^{-1}(\mathbf{P})) & \approx_c & (\mathbf{B}, & \mathbf{P}, & \text{random}, & \mathbf{B}^{-1}(\mathbf{P}))
\end{array}$$

- Intuition:

No other meaningful use of short preimage $\mathbf{B}^{-1}(\mathbf{P})$,

except right-multiplying to $\mathbf{s}^{\top}\mathbf{B}$ to obtain $\mathbf{s}^{\top}\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{s}^{\top}\mathbf{P} + \underbrace{\mathbf{e}^{\top} \cdot \mathbf{B}^{-1}(\mathbf{P})}_{\textit{short}} = \mathbf{s}^{\top}\mathbf{P}$

Evasive LWE

Evasive LWE Assumption (informal) [Wee22]

For random wide matrix $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any PPT generated $\mathbf{P}$,

$$\begin{array}{llllllllll} \text{If} & (\mathbf{B}, & \mathbf{P}, & \mathbf{s}^\top\mathbf{B}, & \mathbf{s}^\top\mathbf{P}) & \approx_c & (\mathbf{B}, & \mathbf{P}, & \text{random}, & \text{random}) \\ \text{Then} & (\mathbf{B}, & \mathbf{P}, & \mathbf{s}^\top\mathbf{B}, & \mathbf{B}^{-1}(\mathbf{P})) & \approx_c & (\mathbf{B}, & \mathbf{P}, & \text{random}, & \mathbf{B}^{-1}(\mathbf{P})) \end{array}$$

- Intuition:

No other meaningful use of short preimage $\mathbf{B}^{-1}(\mathbf{P})$,

except right-multiplying to $\mathbf{s}^\top\mathbf{B}$ to obtain $\mathbf{s}^\top\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{s}^\top\mathbf{P} + \underbrace{\mathbf{e}^\top \cdot \mathbf{B}^{-1}(\mathbf{P})}_{\textit{short}} = \mathbf{s}^\top\mathbf{P}$

- Usefulness: In security proof, suffices to argue pseudorandomness of $\mathbf{s}^\top\mathbf{B}$, $\mathbf{s}^\top\mathbf{P}$
(No preimages involved anymore)
- [Wee22] Achieves first lattice-based ciphertext-policy attribute-based encryption (CP-ABE) with $|\text{ctxt}|$ independent of policy size

What Evasive LWE brings

Lattice-based primitives achieved from evasive LWE (+ LWE or other assumptions):

- CP-ABE [Wee22]
- Multi-authority ABE [WWW22;CL**W**24]
- Multi-input ABE [ARYY23]
- ABE for unbounded-depth circuits [HLL23; AKY24]
- Witness encryption [Tsa22; VWW22]
- Obfuscation for null-circuits [VWW22]
- Designated-verifier zkSNARK for UP [MPV24]
- Obfuscation for pseudorandom functions [BDJM+24]

... and more

A Closer Look at Evasive LWE(s)

1. [Wee22]:

For random $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}({}_{\mathit{rand}})$ from randomness ${}_{\mathit{rand}}$,

$$
\begin{array}{lllllll}
\text{If} & (\mathbf{B}, & \mathbf{P}, & \mathbf{s}^\top\mathbf{B}, & \mathbf{s}^\top\mathbf{P}, & \text{aux}, & {}_{\mathit{rand}}) \approx_c (\mathbf{B}, \ \mathbf{P}, \ \text{random}, \ \text{random}, \ \text{aux}, \ {}_{\mathit{rand}}) \\
\text{Then} & (\mathbf{B}, & \mathbf{P}, & \mathbf{s}^\top\mathbf{B}, & \mathbf{B}^{-1}(\mathbf{P}), & \text{aux}, & {}_{\mathit{rand}}) \approx_c (\mathbf{B}, \ \mathbf{P}, \ \text{random}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \text{aux}, \ {}_{\mathit{rand}})
\end{array}
$$

A Closer Look at Evasive LWE(s)

2. [ARYY23] :

For random $\mathbf{B} \leftarrow\$\ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathrm{aux}) \leftarrow\$\ \mathrm{Samp}(_{rand})$ from randomness $_{rand}$,

$$\text{If} \quad (\mathbf{B}, \quad , \mathbf{SB}, \mathbf{SP}, \mathrm{aux}, \quad) \approx_c (\mathbf{B}, \quad , \text{random}, \text{random}, \mathrm{aux}, \quad)$$

$$\text{Then} \quad (\mathbf{B}, \quad , \mathbf{SB}, \mathbf{B}^{-1}(\mathbf{P}), \mathrm{aux}, \quad) \approx_c (\mathbf{B}, \quad , \text{random}, \mathbf{B}^{-1}(\mathbf{P}), \mathrm{aux}, \quad)$$

A Closer Look at Evasive LWE(s)

3. [VWW22]:

For random $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathrm{aux}) \leftarrow\$ \mathrm{Samp}(_{rand})$ from randomness $_{rand}$,

$$\text{If} \quad (\;,\; ,\; \mathbf{SB},\; \mathbf{SP},\; \mathrm{aux},\;) \approx_c (\;,\; ,\; \text{random},\; \text{random},\; \mathrm{aux},\;)$$

$$\text{Then} \quad (\;,\; ,\; \mathbf{SB},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathrm{aux},\;) \approx_c (\;,\; ,\; \text{random},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathrm{aux},\;)$$

A Closer Look at Evasive LWE(s)

4. [Tsa22] (with some reformulation):

For "random" $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow_\$ \mathsf{Samp}(\mathbf{B}, \mathsf{td}_{\mathbf{B}}, \$_{rand})$ from randomness $\$_{rand}$,

If $\quad (\;,\quad ,\; \utilde{\mathbf{SB}},\; \utilde{\mathbf{SP}},\; \mathsf{aux},\quad) \approx_c (\;,\quad ,\; \text{random},\; \text{random},\; \mathsf{aux},\quad)$

Then $\quad (\;,\quad ,\; \utilde{\mathbf{SB}},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathsf{aux},\quad) \approx_c (\;,\quad ,\; \text{random},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathsf{aux},\quad)$

A Closer Look at Evasive LWE(s)

4. [Tsa22] (with some reformulation):

For "random" $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow_{\$} \mathsf{Samp}(\mathbf{B}, \mathsf{td}_{\mathbf{B}}, {}_{rand})$ from randomness ${}_{rand}$,

$$\text{If} \quad (\;,\; ,\; \underset{\sim}{\mathbf{SB}},\; \underset{\sim}{\mathbf{SP}},\; \mathsf{aux},\;) \approx_c (\;,\; ,\; \text{random},\; \text{random},\; \mathsf{aux},\;)$$

$$\text{Then} \quad (\;,\; ,\; \underset{\sim}{\mathbf{SB}},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathsf{aux},\;) \approx_c (\;,\; ,\; \text{random},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathsf{aux},\;)$$

- We ask: Are they the same? Or how different are they?
- Results: Counterexamples against some variants + Framework to classify them + Implications

Some Counterexamples

Case 1 [ARYY23]:

For random $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow\$ \mathsf{Samp}({}_{rand})$,

$$\text{If} \quad (\mathbf{B}, \quad , \quad \mathbf{S}\mathbf{B}, \quad \mathbf{S}\mathbf{P}, \quad \mathsf{aux}, \quad) \approx_c (\mathbf{B}, \quad , \quad \mathsf{random}, \quad \mathsf{random}, \quad \mathsf{aux}, \quad)$$

$$\text{Then} \quad (\mathbf{B}, \quad , \quad \mathbf{S}\mathbf{B}, \quad \mathbf{B}^{-1}(\mathbf{P}), \quad \mathsf{aux}, \quad) \approx_c (\mathbf{B}, \quad , \quad \mathsf{random}, \quad \mathbf{B}^{-1}(\mathbf{P}), \quad \mathsf{aux}, \quad)$$

Some Counterexamples

Case 1 [ARYY23]:

For random $\mathbf{B} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow\!\!\$\ \mathsf{Samp}(_{rand})$,

$$\text{If} \quad (\mathbf{B}, \quad , \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \underset{\sim}{\mathbf{S}}\mathbf{P}, \ \mathsf{aux}, \qquad) \approx_c (\mathbf{B}, \quad , \ \mathsf{random}, \ \mathsf{random}, \ \mathsf{aux}, \qquad)$$

$$\text{Then} \quad (\mathbf{B}, \quad , \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \qquad) \approx_c (\mathbf{B}, \quad , \ \mathsf{random}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \qquad)$$

Want to show: “If” is true (under plausible assumption); but “Then” is false

Some Counterexamples

Case 1 [ARYY23]:

For random $\mathbf{B} \leftarrow_\$ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow_\$ \mathsf{Samp}({}_{rand})$,

$$\text{If} \quad (\mathbf{B}, \quad , \quad \mathbf{SB}, \quad \mathbf{SP}, \quad \mathsf{aux}, \quad) \approx_c (\mathbf{B}, \quad , \quad \text{random}, \quad \text{random}, \quad \mathsf{aux}, \quad)$$

$$\text{Then} \quad (\mathbf{B}, \quad , \quad \mathbf{SB}, \quad \mathbf{B}^{-1}(\mathbf{P}), \quad \mathsf{aux}, \quad) \approx_c (\mathbf{B}, \quad , \quad \text{random}, \quad \mathbf{B}^{-1}(\mathbf{P}), \quad \mathsf{aux}, \quad)$$

- Idea: Hide secret information in $\mathbf{P} = (\mathbf{P}_1, \mathbf{P}_2)$. Secret = short $\mathbf{x}$ satisfying $\mathbf{P}_1\mathbf{x} = \mathbf{0} \bmod q$

  Let $\mathbf{P}_2 = \begin{pmatrix} \mathbf{x}^\top \\ \text{random} \end{pmatrix} \implies \mathbf{s}^\top\mathbf{P}_2 = \text{random}$; By LWE $(\mathbf{s}^\top\mathbf{B}, \mathbf{s}^\top\mathbf{P}_1) \approx_c \text{random}$

Some Counterexamples

Case 1 [ARYY23]:

For random $\mathbf{B} \leftarrow\!\!\$\ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow\!\!\$\ \mathsf{Samp}(_{rand})$,

$$\text{If} \quad (\mathbf{B}, \quad , \quad \mathbf{S}\mathbf{B}, \quad \mathbf{S}\mathbf{P}, \quad \mathsf{aux}, \quad) \approx_c (\mathbf{B}, \quad , \quad \text{random}, \quad \text{random}, \quad \mathsf{aux}, \quad)$$

$$\text{Then} \quad (\mathbf{B}, \quad , \quad \mathbf{S}\mathbf{B}, \quad \mathbf{B}^{-1}(\mathbf{P}), \quad \mathsf{aux}, \quad) \approx_c (\mathbf{B}, \quad , \quad \text{random}, \quad \mathbf{B}^{-1}(\mathbf{P}), \quad \mathsf{aux}, \quad)$$

- Idea: Hide secret information in $\mathbf{P} = (\mathbf{P}_1, \mathbf{P}_2)$. Secret = short $\mathbf{x}$ satisfying $\mathbf{P}_1\mathbf{x} = \mathbf{0} \bmod q$

  Let $\mathbf{P}_2 = \begin{pmatrix} \mathbf{x}^\mathsf{T} \\ \text{random} \end{pmatrix} \implies \mathbf{s}^\mathsf{T}\mathbf{P}_2 = \text{random}$; By LWE $(\mathbf{s}^\mathsf{T}\mathbf{B}, \mathbf{s}^\mathsf{T}\mathbf{P}_1) \approx_c \text{random}$

- Distinguish "Then":

  Compute $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}_2) = \mathbf{P}_2$, therefore recover $\mathbf{x}$

  LHS: $\mathbf{s}^\mathsf{T}\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}_1) \cdot \mathbf{x} \approx \mathbf{s}^\mathsf{T}\mathbf{P}_1 \cdot \mathbf{x} \approx \mathbf{0}$ RHS: random $\cdot \mathbf{B}^{-1}(\mathbf{P}_1) \cdot \mathbf{x} \approx$ random

Some Counterexamples

Case 2 [VWW22]:

For random $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n \times m}$, and any $(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}(\ _{rand})$,

$$\text{If} \quad (\ ,\ ,\ \underset{\sim}{\mathbf{S}}\mathbf{B},\ \underset{\sim}{\mathbf{S}}\mathbf{P},\ \text{aux},\ ) \approx_c (\ ,\ ,\ \text{random},\ \text{random},\ \text{aux},\ )$$

$$\text{Then} \quad (\ ,\ ,\ \underset{\sim}{\mathbf{S}}\mathbf{B},\ \mathbf{B}^{-1}(\mathbf{P}),\ \text{aux},\ ) \approx_c (\ ,\ ,\ \text{random},\ \mathbf{B}^{-1}(\mathbf{P}),\ \text{aux},\ )$$

- Difference relative to Case 1: **B** not available

Some Counterexamples

Case 2 [VWW22]:

For random $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathrm{aux}) \leftarrow\$ \mathrm{Samp}(_{rand})$,

If $(\;,\; ,\; \mathbf{S}\mathbf{B},\; \mathbf{S}\mathbf{P},\; \mathrm{aux},\;) \approx_c (\;,\; ,\; \mathrm{random},\; \mathrm{random},\; \mathrm{aux},\;)$

Then $(\;,\; ,\; \mathbf{S}\mathbf{B},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathrm{aux},\;) \approx_c (\;,\; ,\; \mathrm{random},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathrm{aux},\;)$

- Difference relative to Case 1: $\mathbf{B}$ not available
- Idea: Extend to $\mathbf{P} = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3)$, put the random $\mathbf{P}_3$ inside aux to help recover $\mathbf{B}$
  We show: Given $\mathbf{B}^{-1}(\mathbf{P}_3)$ and $\mathbf{P}_3$, can recover $\mathbf{B}$ via linear system $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}_3) = \mathbf{P}_3 \bmod q$
  (Non-triviality: $\mathbf{B}^{-1}(\mathbf{P}_3)$ distributed as Gaussian)

Some Counterexamples

Case 2 [VWW22]:

For random $\mathbf{B} \leftarrow\$ \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathrm{aux}) \leftarrow\$ \mathrm{Samp}(\ {}_{rand})$,

$$\text{If} \quad (\ ,\quad ,\ \underset{\sim}{\mathbf{SB}},\ \underset{\sim}{\mathbf{SP}},\ \mathrm{aux},\qquad) \approx_c (\ ,\quad ,\ \mathrm{random},\ \mathrm{random},\ \mathrm{aux},\qquad)$$

$$\text{Then} \quad (\ ,\quad ,\ \underset{\sim}{\mathbf{SB}},\ \mathbf{B}^{-1}(\mathbf{P}),\ \mathrm{aux},\qquad) \approx_c (\ ,\quad ,\ \mathrm{random},\ \mathbf{B}^{-1}(\mathbf{P}),\ \mathrm{aux},\qquad)$$

- Difference relative to Case 1: $\mathbf{B}$ not available
- Idea: Extend to $\mathbf{P} = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3)$, put the random $\mathbf{P}_3$ inside aux to help recover $\mathbf{B}$

  We show: Given $\mathbf{B}^{-1}(\mathbf{P}_3)$ and $\mathbf{P}_3$, can recover $\mathbf{B}$ via linear system $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}_3) = \mathbf{P}_3 \bmod q$

  (Non-triviality: $\mathbf{B}^{-1}(\mathbf{P}_3)$ distributed as Gaussian)
- Distinguish “Then”:

  Recover $\mathbf{B}$ using $\mathbf{B}^{-1}(\mathbf{P}_3)$ and $\mathbf{P}_3$; Rest is identical to Case 1

Some Counterexamples

Case 3 [Tsa22] (with some reformulation) :

For "random" $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow\$ \text{Samp}(\mathbf{B}, \text{td}_{\mathbf{B}}, \$_{rand})$,

$$\text{If} \quad (\ ,\ \ ,\ \utilde{\mathbf{S}\mathbf{B}},\ \utilde{\mathbf{S}\mathbf{P}},\ \text{aux},\ \ ) \approx_c (\ ,\ \ ,\ \text{random},\ \text{random},\ \text{aux},\ \ )$$

$$\text{Then} \quad (\ ,\ \ ,\ \utilde{\mathbf{S}\mathbf{B}},\ \mathbf{B}^{-1}(\mathbf{P}),\ \text{aux},\ \ ) \approx_c (\ ,\ \ ,\ \text{random},\ \mathbf{B}^{-1}(\mathbf{P}),\ \text{aux},\ \ )$$

- Difference: Samp inputs **B**

Some Counterexamples

Case 3 [Tsa22] (with some reformulation) :

For “random” $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathrm{aux}) \leftarrow_\$ \mathrm{Samp}(\mathbf{B}, \mathrm{td}_{\mathbf{B}}, \text{🪙}_{rand})$,

$$\text{If} \quad (\;,\; \;,\; \mathbf{SB},\; \mathbf{SP},\; \mathrm{aux}, \quad) \approx_c (\;,\; \;,\; \mathrm{random},\; \mathrm{random},\; \mathrm{aux}, \quad)$$

$$\text{Then} \quad (\;,\; \;,\; \mathbf{SB},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathrm{aux}, \quad) \approx_c (\;,\; \;,\; \mathrm{random},\; \mathbf{B}^{-1}(\mathbf{P}),\; \mathrm{aux}, \quad)$$

- Difference: Samp inputs $\mathbf{B}$
- Idea: Generate PKE key-pair from $\mathbf{B}$, s.t. $\mathbf{B}^{-1}(\mathbf{P}_2)$ is decryption key

  Encrypt some secret vector, e.g. short $\mathbf{x}$ s.t. $\mathbf{P}_1 \cdot \mathbf{x} = \mathbf{0}$ as before, put ctxt into aux

Some Counterexamples

Case 3 [Tsa22] (with some reformulation) :

For “random” $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, and any $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow_\$ \mathsf{Samp}(\mathbf{B}, \mathsf{td}_{\mathbf{B}}, \$_{rand})$,

If $(\ ,\ ,\ \utilde{\mathbf{S}}\mathbf{B},\ \utilde{\mathbf{S}}\mathbf{P},\ \mathsf{aux},\ ) \approx_c (\ ,\ ,\ \text{random},\ \text{random},\ \mathsf{aux},\ )$

Then $(\ ,\ ,\ \utilde{\mathbf{S}}\mathbf{B},\ \mathbf{B}^{-1}(\mathbf{P}),\ \mathsf{aux},\ ) \approx_c (\ ,\ ,\ \text{random},\ \mathbf{B}^{-1}(\mathbf{P}),\ \mathsf{aux},\ )$

- Difference: Samp inputs $\mathbf{B}$
- Idea: Generate PKE key-pair from $\mathbf{B}$, s.t. $\mathbf{B}^{-1}(\mathbf{P}_2)$ is decryption key

  Encrypt some secret vector, e.g. short $\mathbf{x}$ s.t. $\mathbf{P}_1 \cdot \mathbf{x} = \mathbf{0}$ as before, put ctxt into aux
- Dual-Regev PKE: public key $= (\mathbf{B}, \mathbf{P}_2)$, secret key = $\mathbf{B}^{-1}(\mathbf{P}_2)$

  ctxt $= (\mathbf{c}_1^\mathsf{T}, \mathbf{c}_2^\mathsf{T}) = (\utilde{\mathbf{s}^\mathsf{T}}\mathbf{B},\ \utilde{\mathbf{s}^\mathsf{T}}\mathbf{P}_2 + \mathbf{x}^\mathsf{T})$, decryption: $\mathbf{c}_2^\mathsf{T} - \mathbf{c}_1^\mathsf{T} \cdot \mathbf{B}^{-1}(\mathbf{P}_2) \approx \mathbf{x}^\mathsf{T}$

  Rest is identical to Case 1

Three Families of Plausible Evasive LWEs

Any variants might we still believe in?

Three Families of Plausible Evasive LWEs

Any variants might we still believe in?

Observations:

- Randomness 🪙$_{rand}$ is crucial:

  Distinguisher can rerun Samp given 🪙$_{rand}$ $\implies$ Cannot "hide" secrets into problem instance

  $\implies$ When given 🪙$_{rand}$, none of the counterexamples works

Three Families of Plausible Evasive LWEs

Any variants might we still believe in?

Observations:

- Randomness $\faCoins_{rand}$ is crucial:
  Distinguisher can rerun Samp given $\faCoins_{rand}$ $\implies$ Cannot "hide" secrets into problem instance
  $\implies$ When given $\faCoins_{rand}$, none of the counterexamples works
- Cases 1 and 2: Exploit linear system $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P} \bmod q$, distinguish "Then" by
  - using $\mathbf{B}$ and $\mathbf{B}^{-1}(\mathbf{P})$ to recover $\mathbf{P}$, and/or
  - using $\mathbf{P}$ and $\mathbf{B}^{-1}(\mathbf{P})$ to recover $\mathbf{B}$

  $\implies$ A plausible assumption should prohibit these

Three Families of Plausible Evasive LWEs

Any variants might we still believe in?

Observations:

- Randomness 🪙$_{rand}$ is crucial:

  Distinguisher can rerun Samp given 🪙$_{rand}$ $\implies$ Cannot "hide" secrets into problem instance

  $\implies$ When given 🪙$_{rand}$, none of the counterexamples works

- Cases 1 and 2: Exploit linear system $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P} \bmod q$, distinguish "Then" by
  - using $\mathbf{B}$ and $\mathbf{B}^{-1}(\mathbf{P})$ to recover $\mathbf{P}$, and/or
  - using $\mathbf{P}$ and $\mathbf{B}^{-1}(\mathbf{P})$ to recover $\mathbf{B}$

  $\implies$ A plausible assumption should prohibit these

- Case 3: Samp should not input $\mathbf{B}$

Three Families of Plausible Evasive LWEs

1. Public-coin: $\mathbf{P} \leftarrow_{\$} \mathrm{Samp}({}_{rand})$

If $(\mathbf{B}, \mathbf{P}, \mathbf{SB}, \utilde{\mathbf{SP}}, \text{aux}, {}_{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \text{random}, \text{aux}, {}_{rand})$

Then $(\mathbf{B}, \mathbf{P}, \utilde{\mathbf{SB}}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}, {}_{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}, {}_{rand})$

Three Families of Plausible Evasive LWEs

1. Public-coin: $\mathbf{P} \leftarrow_{\$} \mathrm{Samp}({}_{rand})$

$$\text{If} \quad (\mathbf{B}, \mathbf{P}, \mathbf{S}\underset{\sim}{\mathbf{B}}, \underset{\sim}{\mathbf{SP}}, \text{aux}, {}_{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \text{random}, \text{aux}, {}_{rand})$$

$$\text{Then} \quad (\mathbf{B}, \mathbf{P}, \underset{\sim}{\mathbf{SB}}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}, {}_{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}, {}_{rand})$$

2. (Private-coin) Binding: $(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow_{\$} \mathrm{Samp}({}_{rand})$

$$\text{If} \quad (\mathbf{B}, \mathbf{P}, \underset{\sim}{\mathbf{SB}}, \underset{\sim}{\mathbf{SP}}, \text{aux}, \quad) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \text{random}, \text{aux}, \quad)$$

$$\text{Then} \quad (\mathbf{B}, \mathbf{P}, \underset{\sim}{\mathbf{SB}}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}, \quad) \approx_c (\mathbf{B}, \mathbf{P}, \text{random}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}, \quad)$$

Three Families of Plausible Evasive LWEs

1. Public-coin: $\mathbf{P} \leftarrow\!\!\$ \ \mathsf{Samp}(\mathsf{coins}_{rand})$

$$\begin{array}{lllllll}
\text{If} & (\mathbf{B}, \ \mathbf{P}, \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \underset{\sim}{\mathbf{S}}\mathbf{P}, \ \mathsf{aux}, \ \mathsf{coins}_{rand}) & \approx_c & (\mathbf{B}, \ \mathbf{P}, \ \mathsf{random}, \ \mathsf{random}, \ \mathsf{aux}, \ \mathsf{coins}_{rand}) \\
\text{Then} & (\mathbf{B}, \ \mathbf{P}, \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \ \mathsf{coins}_{rand}) & \approx_c & (\mathbf{B}, \ \mathbf{P}, \ \mathsf{random}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \ \mathsf{coins}_{rand})
\end{array}$$

2. (Private-coin) Binding: $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow\!\!\$ \ \mathsf{Samp}(\mathsf{coins}_{rand})$

$$\begin{array}{lllllll}
\text{If} & (\mathbf{B}, \ \mathbf{P}, \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \underset{\sim}{\mathbf{S}}\mathbf{P}, \ \mathsf{aux}, \ \ ) & \approx_c & (\mathbf{B}, \ \mathbf{P}, \ \mathsf{random}, \ \mathsf{random}, \ \mathsf{aux}, \ \ ) \\
\text{Then} & (\mathbf{B}, \ \mathbf{P}, \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \ \ ) & \approx_c & (\mathbf{B}, \ \mathbf{P}, \ \mathsf{random}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \ \ )
\end{array}$$

3. (Private-coin) Hiding: $(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow\!\!\$ \ \mathsf{Samp}(\mathsf{coins}_{rand})$

$$\begin{array}{lllllll}
\text{If} & (\ , \ \ , \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \underset{\sim}{\mathbf{S}}\mathbf{P}, \ \mathsf{aux}, \ \ ) & \approx_c & (\ , \ \ , \ \mathsf{random}, \ \mathsf{random}, \ \mathsf{aux}, \ \ )
\end{array}$$

and **P** provably "sufficiently hidden given aux"

$$\begin{array}{lllllll}
\text{Then} & (\ , \ \ , \ \underset{\sim}{\mathbf{S}}\mathbf{B}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \ \ ) & \approx_c & (\ , \ \ , \ \mathsf{random}, \ \mathbf{B}^{-1}(\mathbf{P}), \ \mathsf{aux}, \ \ )
\end{array}$$

Hiding Evasive LWE: What does "**P** sufficiently hidden" mean

- Our proposal: Hiding Evasive LWE parametrised by $\ell \in \{1, 2 \ldots, q\}$.
  Define "**P** hidden given aux":

For $(\mathbf{S}, \mathbf{P}, \mathrm{aux}) \leftarrow \mathrm{Samp}(\text{🪙}_{rand})$,

$$(\mathbf{P}, \quad \mathrm{aux}) \quad \approx_c \quad (\mathbf{P} + \mathbf{R}, \quad \mathrm{aux})$$

where each entry of **R** uniform over $\{0, 1, \ldots, \ell\}$.

- Interpretation: **R** some noise; **P** cannot be approximated given aux

Hiding Evasive LWE: What does "**P** sufficiently hidden" mean

- Our proposal: Hiding Evasive LWE parametrised by $\ell \in \{1, 2 \ldots, q\}$.
  Define "**P** hidden given aux":

For $(\mathbf{S}, \mathbf{P}, \text{aux}) \leftarrow \text{Samp}(🪙_{rand})$,

$$(\mathbf{P}, \quad \text{aux}) \qquad \approx_c \qquad (\mathbf{P} + \mathbf{R}, \quad \text{aux})$$

where each entry of **R** uniform over $\{0, 1, \ldots, \ell\}$.

- Interpretation: **R** some noise; **P** cannot be approximated given aux
- Increase $\ell \iff$ **P** "more hidden" $\iff$ weaker Hiding Evasive LWE assumption
  E.g. $\ell = q$: **P** is pseudorandom conditioned on aux
  (Prior works: $\ell = 0$, false by our counterexample)
- We cannot find counterexample even when $\ell = 1$

(We thank an anonymous reviewer for sharing with us a counterexample against a prior proposal of Hiding Evasive LWE!)

Implications on Related Prior Works

- [ARYY23; AKY24]:
  - Security proofs do not directly use the stated variant, but another one: $\mathsf{aux} = (\mathsf{aux}_1, \mathsf{aux}_2)$, where $\mathbf{P}$ efficiently computable from aux_2
  - Special case of Private-coin Binding Evasive LWE

Implications on Related Prior Works

- [ARYY23; AKY24]:
  - Security proofs do not directly use the stated variant, but another one: $\mathsf{aux} = (\mathsf{aux}_1, \mathsf{aux}_2)$, where $\mathbf{P}$ efficiently computable from aux_2
  - Special case of Private-coin Binding Evasive LWE
- [Tsa22]:
  - Assumption lets Samp input $\mathbf{B}$ (and its trapdoor), morally false by our result
  - Instance in security proof does not exploit this; Output $\mathbf{P}$ independent of $\mathbf{B}$
  - Our speculation: Scheme may be reproved via the proposed private-coin evasive LWEs

Implications on Related Prior Works

- [ARYY23; AKY24]:
  - Security proofs do not directly use the stated variant, but another one: $\mathsf{aux} = (\mathsf{aux}_1, \mathsf{aux}_2)$, where $\mathbf{P}$ efficiently computable from aux_2
  - Special case of Private-coin Binding Evasive LWE
- [Tsa22]:
  - Assumption lets Samp input $\mathbf{B}$ (and its trapdoor), morally false by our result
  - Instance in security proof does not exploit this; Output $\mathbf{P}$ independent of $\mathbf{B}$
  - Our speculation: Scheme may be reproved via the proposed private-coin evasive LWEs
- [VWW22]:
  - Assumption does not require $\mathbf{P}$ sufficiently hidden, false by our result
  - We show: For the instance in security proof [VWW22, Lemma 5.2], $\mathbf{P}$ can be proven sufficiently hidden $\implies$ Remains secure assuming Private-coin Hiding Evasive LWE

[VWW22]: Proving **P** hidden

- Outputs of Samp:
  - $\mathbf{S} := \left\{\hat{\mathbf{S}}_{i,b}\right\}_{i\in[h],b\in\{0,1\}}, \quad \mathbf{P} := \left(\hat{\mathbf{S}}_{j,0}\mathbf{A}_j + \mathbf{E}_{j,0},\ \hat{\mathbf{S}}_{j,1}\mathbf{A}_j + \mathbf{E}_{j,1}\right)$ where $\mathbf{A}_j$ uniform
  - $\mathrm{aux} := \left\{\mathbf{A}_{i-1}^{-1}(\hat{\mathbf{S}}_{i,b}\mathbf{A}_i + \mathbf{E}_{i,b})\right\}_{i\geq j+1,b\in\{0,1\}}, \quad \left\{\hat{\mathbf{S}}_{i,b}\right\}_{i\in[h],b\in\{0,1\}}$

[VWW22]: Proving **P** hidden

- Outputs of Samp:
  - $\mathbf{S} := \left\{\hat{\mathbf{S}}_{i,b}\right\}_{i\in[h],b\in\{0,1\}}, \quad \mathbf{P} := \left(\hat{\mathbf{S}}_{j,0}\mathbf{A}_j + \mathbf{E}_{j,0},\ \hat{\mathbf{S}}_{j,1}\mathbf{A}_j + \mathbf{E}_{j,1}\right)$ where $\mathbf{A}_j$ uniform
  - $\text{aux} := \left\{\mathbf{A}_{i-1}^{-1}(\hat{\mathbf{S}}_{i,b}\mathbf{A}_i + \mathbf{E}_{i,b})\right\}_{i\geq j+1,b\in\{0,1\}}, \quad \left\{\hat{\mathbf{S}}_{i,b}\right\}_{i\in[h],b\in\{0,1\}}$
- [VWW22] showed

$$(\ ,\quad ,\quad \mathbf{SB},\quad \mathbf{SP},\quad \text{aux},\qquad)\quad \approx_c\quad (\ ,\qquad ,\quad \text{random},\quad \text{random},\quad \text{aux},\qquad)$$

Invoke Hiding Evasive LWE, remains to show $\mathbf{P} \approx_c \mathbf{P} + \mathbf{R}$ where $\mathbf{R}$ uniform over $\{0, 1, \ldots, \ell\}$

- Observation: $\mathbf{E}_{j,b}$ in $\mathbf{P}$ independent of aux

[VWW22]: Proving **P** hidden

- Outputs of Samp:
  - $\mathbf{S} := \left\{\hat{\mathbf{S}}_{i,b}\right\}_{i\in[h],b\in\{0,1\}}, \quad \mathbf{P} := \left(\hat{\mathbf{S}}_{j,0}\mathbf{A}_j + \mathbf{E}_{j,0},\ \hat{\mathbf{S}}_{j,1}\mathbf{A}_j + \mathbf{E}_{j,1}\right)$ where $\mathbf{A}_j$ uniform
  - $\text{aux} := \left\{\mathbf{A}_{i-1}^{-1}(\hat{\mathbf{S}}_{i,b}\mathbf{A}_i + \mathbf{E}_{i,b})\right\}_{i\geq j+1,b\in\{0,1\}}, \quad \left\{\hat{\mathbf{S}}_{i,b}\right\}_{i\in[h],b\in\{0,1\}}$
- [VWW22] showed

$$(\ , \quad , \ \utilde{\mathbf{S}\mathbf{B}}, \ \utilde{\mathbf{S}\mathbf{P}}, \ \text{aux}, \qquad) \approx_c (\ , \qquad , \ \text{random}, \ \text{random}, \ \text{aux}, \qquad)$$

Invoke Hiding Evasive LWE, remains to show $\mathbf{P} \approx_c \mathbf{P} + \mathbf{R}$ where $\mathbf{R}$ uniform over $\{0, 1, \ldots, \ell\}$

- Observation: $\mathbf{E}_{j,b}$ in $\mathbf{P}$ independent of aux

$$\mathbf{P} = \left(\hat{\mathbf{S}}_{j,0}\mathbf{A}_j + \mathbf{E}_{j,0},\ \hat{\mathbf{S}}_{j,1}\mathbf{A}_j + \mathbf{E}_{j,1}\right) \approx_s \left(\hat{\mathbf{S}}_{j,0}\mathbf{A}_j + \mathbf{E}_{j,0} + \mathbf{R}_0,\ \hat{\mathbf{S}}_{j,1}\mathbf{A}_j + \mathbf{E}_{j,1} + \mathbf{R}_1\right) = \mathbf{P} + \mathbf{R}$$

by noise-flooding, for $\mathbf{R} = (\mathbf{R}_0, \mathbf{R}_1) \ll (\mathbf{E}_{j,0}, \mathbf{E}_{j,1})$, e.g. $\ell = \lambda^{O(1)}$ for parameters in [VWW22]

Extras: Obfuscation-based Counterexample (appearing in Eprint)

- Borrowing ideas from [VWW22], we prove an obfuscation-based counterexample
- Applies to all private-coin variants (priors ones + our proposed ones)
- Evidence of difference between public- vs. private-coin

Extras: Obfuscation-based Counterexample (appearing in Eprint)

- Borrowing ideas from [VWW22], we prove an obfuscation-based counterexample
- Applies to all private-coin variants (priors ones + our proposed ones)
- Evidence of difference between public- vs. private-coin
- Idea: Let Obf be null-iO scheme, let aux contain obfuscation $\tilde{C} = \mathsf{Obf}(C)$ of a circuit C:
  - With $\mathbf{SP} + \mathbf{E}'$ hardwired ($\mathbf{E}'$ sampled by Samp)
  - Input matrices: tall $\mathbf{M}_1 \in \mathbb{Z}_q^{m \times n}$ and wide $\mathbf{M}_2 \in \mathbb{Z}_q^{n \times m}$
  - Output 1 if $(\mathbf{SP} + \mathbf{E}') - \mathbf{M}_1\mathbf{M}_2$ is low-norm, else output 0

Extras: Obfuscation-based Counterexample (appearing in Eprint)

- Borrowing ideas from [VWW22], we prove an obfuscation-based counterexample
- Applies to all private-coin variants (priors ones + our proposed ones)
- Evidence of difference between public- vs. private-coin
- Idea: Let Obf be null-iO scheme, let aux contain obfuscation $\tilde{C} = \mathrm{Obf}(C)$ of a circuit C:
  - With $\mathbf{SP} + \mathbf{E}'$ hardwired ($\mathbf{E}'$ sampled by Samp)
  - Input matrices: tall $\mathbf{M}_1 \in \mathbb{Z}_q^{m \times n}$ and wide $\mathbf{M}_2 \in \mathbb{Z}_q^{n \times m}$
  - Output 1 if $(\mathbf{SP} + \mathbf{E}') - \mathbf{M}_1\mathbf{M}_2$ is low-norm, else output 0
- Distinguishing "Then":
  - $\tilde{C}(\underset{\sim}{\mathbf{SB}}, \mathbf{B}^{-1}(\mathbf{P})) = 1$ w.h.p., since $\underset{\sim}{\mathbf{SB}} \cdot \mathbf{B}^{-1}(\mathbf{P}) \approx \mathbf{SP} + \mathbf{E}'$
  - $\tilde{C}(\mathrm{random}, \mathbf{B}^{-1}(\mathbf{P})) = 0$ w.h.p., since $\mathrm{random} \cdot \mathbf{B}^{-1}(\mathbf{P}) \not\approx \mathbf{SP} + \mathbf{E}'$
- Note: $\mathbf{B}, \mathbf{P}$ not needed for distinguishing. Applies to both Binding + Hiding Evasive LWE

Extras: Obfuscation-based Counterexample (appearing in Eprint)

- We prove: For uniform $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{m\times m}$,

$$\Pr\left[\exists \mathbf{M}_1 \in \mathbb{Z}_q^{m\times n}, \mathbf{M}_2 \in \mathbb{Z}_q^{n\times m} : \mathbf{A} - \mathbf{M}_1\mathbf{M}_2 \text{ is short}\right] \le \mathrm{negl}(\lambda) \tag{1}$$

- Proving "If" by noise-flooding + LWE + null-iO security:

$$\begin{aligned}
& (\mathbf{B}, \quad \mathbf{P}, \quad \underset{\sim}{\mathbf{SB}}, \quad \underset{\sim}{\mathbf{SP}}, \quad \tilde{C}_{\mathbf{SP}+\mathbf{E}'}) \\
\approx_s\ & (\mathbf{B}, \quad \mathbf{P}, \quad \underset{\sim}{\mathbf{SB}}, \quad \underset{\sim}{\mathbf{SP}}, \quad \tilde{C}_{\underset{\sim}{\mathbf{SP}}+\mathbf{E}'}) && \text{/ noise-flooding, } \mathbf{E}' \text{ large} \\
\approx_c\ & (\mathbf{B}, \quad \mathbf{P}, \quad \mathrm{random}_1, \quad \mathrm{random}_2, \quad \tilde{C}_{\mathrm{random}_2+\mathbf{E}'}) && \text{/ LWE} \\
\approx_c\ & (\mathbf{B}, \quad \mathbf{P}, \quad \mathrm{random}_1, \quad \mathrm{random}_2, \quad \tilde{C}_{\mathrm{random}_3}) && \text{/ claim (1) + null-iO} \\
\approx_c\ & (\mathbf{B}, \quad \mathbf{P}, \quad \mathrm{random}_1, \quad \mathrm{random}_2, \quad \tilde{C}_{\mathbf{SP}+\mathbf{E}'}) && \text{/ LWE}
\end{aligned}$$

Extras: Issue on Distribution of $\mathbf{B}$ (appearing in Eprint)

- In proceedings version, we further generalise evasive LWEs in multiple directions:
  1. Public-coin variant: Allow secret $\mathbf{S}$ with arbitrary public distribution + "public-coin" leakage
  2. All variants: Also cover ring settings
  3. All variants: Allow $\mathbf{B}$ with arbitrary distribution

Extras: Issue on Distribution of $\mathbf{B}$ (appearing in Eprint)

- In proceedings version, we further generalise evasive LWEs in multiple directions:
  1. Public-coin variant: Allow secret $\mathbf{S}$ with arbitrary public distribution + “public-coin” leakage
  2. All variants: Also cover ring settings
  3. All variants: Allow $\mathbf{B}$ with arbitrary distribution
- Subsequently we realise simple counterexample against (3)

Extras: Issue on Distribution of $\mathbf{B}$ (appearing in Eprint)

- In proceedings version, we further generalise evasive LWEs in multiple directions:
  1. Public-coin variant: Allow secret $\mathbf{S}$ with arbitrary public distribution + "public-coin" leakage
  2. All variants: Also cover ring settings
  3. All variants: Allow $\mathbf{B}$ with arbitrary distribution
- Subsequently we realise simple counterexample against (3)
- Let $\mathbf{B}, \mathbf{P}$ be both block diagonal

$$\underbrace{\begin{pmatrix} \mathbf{B}_1 & \\ & \mathbf{B}_2 \end{pmatrix}}_{\mathbf{B}} \underbrace{\begin{pmatrix} \mathbf{U}_{11} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{pmatrix}}_{\mathbf{U}} = \underbrace{\begin{pmatrix} \mathbf{P}_1 & \\ & \mathbf{P}_2 \end{pmatrix}}_{\mathbf{P}}$$

$\implies \mathbf{B}_1\mathbf{U}_{12} = \mathbf{B}_2\mathbf{U}_{21} = \mathbf{0}$, i.e. obtain Ajtai trapdoors of $\mathbf{B}_1, \mathbf{B}_2$

- Interesting open question: What is the boundary on distributions of $\mathbf{B}$?
- Our opinion for now: Stay with uniform $\mathbf{B}$ as in prior works

Summary

- Background, Evasive LWEs in prior works
- Counterexamples against 3 existing private-coin variants (assuming LWE)
- Proposed plausible classes: Public-coin, Private-coin Binding, Private-coin Hiding
- Implications to prior works + Re-prove [VWW22]
- Appearing in Eprint:
  - Provable obfuscation-based counterexample against all private-coin variants (assuming null-iO + LWE)
  - On arbitrary distribution of **B**

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

Thank You!

References I

[AKY24] Shweta Agrawal, Simran Kumari, and Shota Yamada. "Attribute Based Encryption for Turing Machines from Lattices". In: *CRYPTO 2024, Part III*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14922. LNCS. Springer, Cham, Aug. 2024, pp. 352–386. DOI: 10.1007/978-3-031-68382-4_11.

[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.

[BDJM+24] Pedro Branco, Nico Döttling, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, Spencer Peters, and Vinod Vaikuntanathan. *Pseudorandom Obfuscation and Applications*. Cryptology ePrint Archive, Paper 2024/1742. https://eprint.iacr.org/2024/1742. 2024.

[CLW24] Valerio Cini, Russell W. F. Lai, and Ivy K. Y. Woo. "Lattice-based Multi-Authority/Client Attribute-based Encryption for Circuits". In: 4 (2024). To appear in CiC 2024 (4).

References II

[HLL23] Yao-Ching Hsieh, Huijia Lin, and Ji Luo. "Attribute-based encryption for circuits of unbounded depth from lattices". In: *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2023, pp. 415–434.

[MPV24] Surya Mathialagan, Spencer Peters, and Vinod Vaikuntanathan. "Adaptively Sound Zero-Knowledge SNARKs for UP". In: *CRYPTO 2024, Part X*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14929. LNCS. Springer, Cham, Aug. 2024, pp. 38–71. DOI: 10.1007/978-3-031-68403-6_2.

[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.

References III

[Wee22] Hoeteck Wee. "Optimal broadcast encryption and CP-ABE from evasive lattice assumptions". In: *Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part II*. Springer. 2022, pp. 217–241.

[WWW22] Brent Waters, Hoeteck Wee, and David J Wu. "Multi-authority ABE from lattices without random oracles". In: *Theory of Cryptography Conference*. Springer. 2022, pp. 651–679.