Simple and General Counterexamples to Evasive LWE





Nico Döttling
CISPA

Abhishek Jain
JHU and NTT Research

Giulio Malavolta
Bocconi University

Surya Mathialagan
MIT → NTT Research

Vinod Vaikuntanathan
MIT

TLDR

TLDR

- Give a **simple** attack that rules out **all** variants of **private-coin** evasive LWE.

TLDR

- Give a **simple** attack that rules out **all** variants of **private-coin** evasive LWE.

    - Our attack is an example of a “zeroizing” attack.

TLDR

- Give a **simple** attack that rules out **all** variants of **private-coin** evasive LWE.
  - Our attack is an example of a “zeroizing” attack.
  - Questions the underlying philosophy of evasive LWE in the private-coin setting.

TLDR

- Give a **simple** attack that rules out **all** variants of **private-coin** evasive LWE.
    - Our attack is an example of a “zeroizing” attack.
    - Questions the underlying philosophy of evasive LWE in the private-coin setting.
- **Concurrent work:** [Hsieh-Jain-Lin 25], [Agrawal-Modi-Yadav-Yamada 25] also show attacks on evasive LWE. More on this later.

LWE [Regev '05]

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell \times n}, \mathbf{E} \leftarrow \chi^{\ell \times m}$, then:

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell \times n}, \mathbf{E} \leftarrow \chi^{\ell \times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathscr{U})$$

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell \times n}, \mathbf{E} \leftarrow \chi^{\ell \times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathscr{U})$$

In this talk, we will treat $\mathbf{S}$ as a matrix rather than a vector.

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell\times n}, \mathbf{E} \leftarrow \chi^{\ell\times m}$, then:

$$(\mathbf{B}, \mathbf{SB}+\mathbf{E}) \approx_c (\mathbf{B}, \mathcal{U})$$

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell \times n}, \mathbf{E} \leftarrow \chi^{\ell \times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathscr{U})$$

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell\times n}, \mathbf{E} \leftarrow \chi^{\ell\times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathscr{U})$$

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell \times n}, \mathbf{E} \leftarrow \chi^{\ell \times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathscr{U})$$

- LWE has proven to be **extremely fruitful**: e.g. Fully homomorphic encryption, attribute-based encryption, etc.

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell\times n}, \mathbf{E} \leftarrow \chi^{\ell\times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathcal{U})$$

- LWE has proven to be **extremely fruitful**: e.g. Fully homomorphic encryption, attribute-based encryption, etc.
- However, some applications have still evaded us.

LWE [Regev '05]

- Let $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{\ell \times n}, \mathbf{E} \leftarrow \chi^{\ell \times m}$, then:

$$(\mathbf{B}, \mathbf{SB} + \mathbf{E}) \approx_c (\mathbf{B}, \mathscr{U})$$

- LWE has proven to be **extremely fruitful**: e.g. Fully homomorphic encryption, attribute-based encryption, etc.
- However, some applications have still evaded us.
  - Some souped up "LWE++" seems sufficient. E.g. want to give out some "auxiliary" information **involving the trapdoor of $\mathbf{B}$…**

Example

Example

Want to be able to compute:

Example

Want to be able to compute:

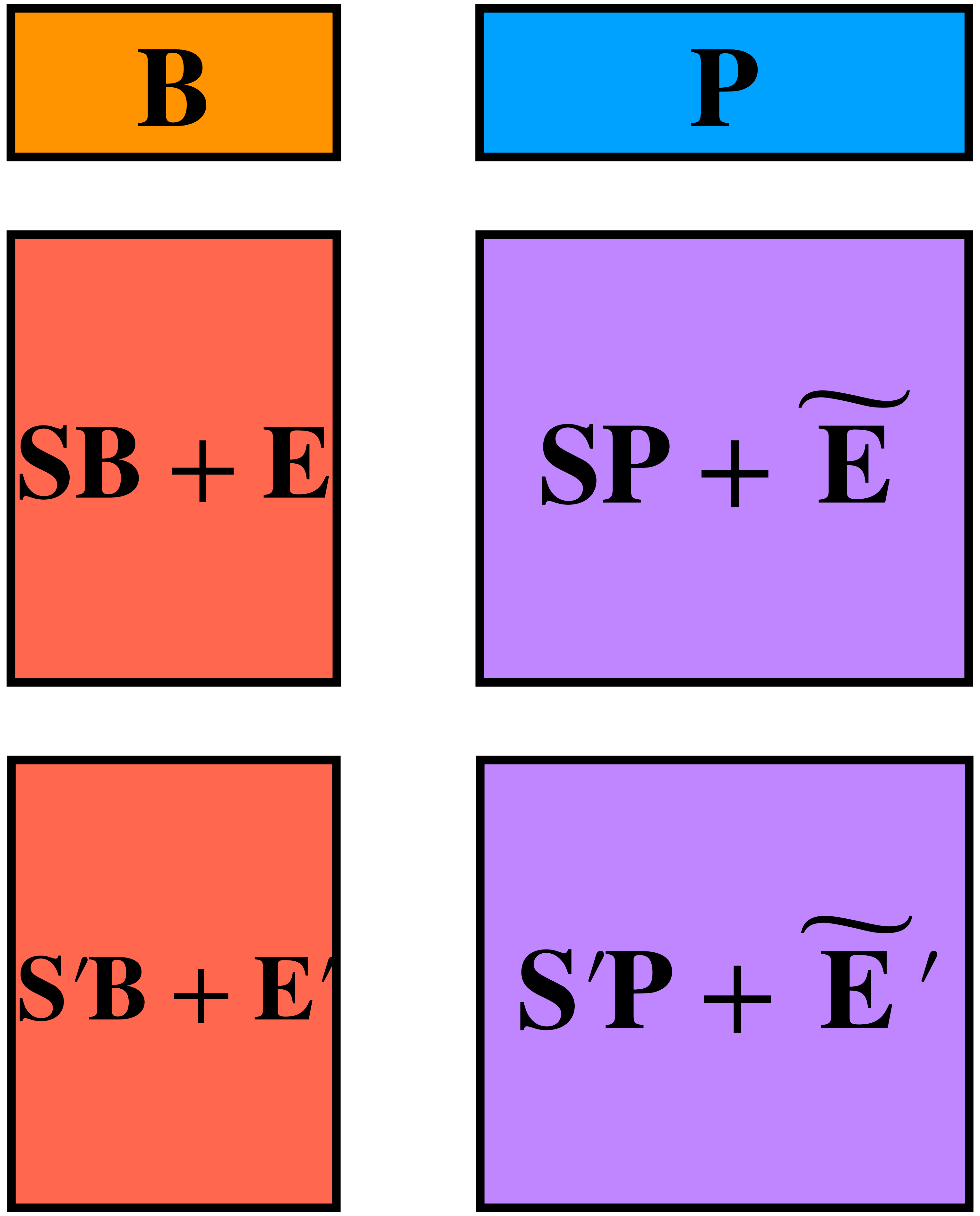
$\mathbf{B}$

$\mathbf{SB} + \mathbf{E}$

$\mathbf{S'B} + \mathbf{E'}$

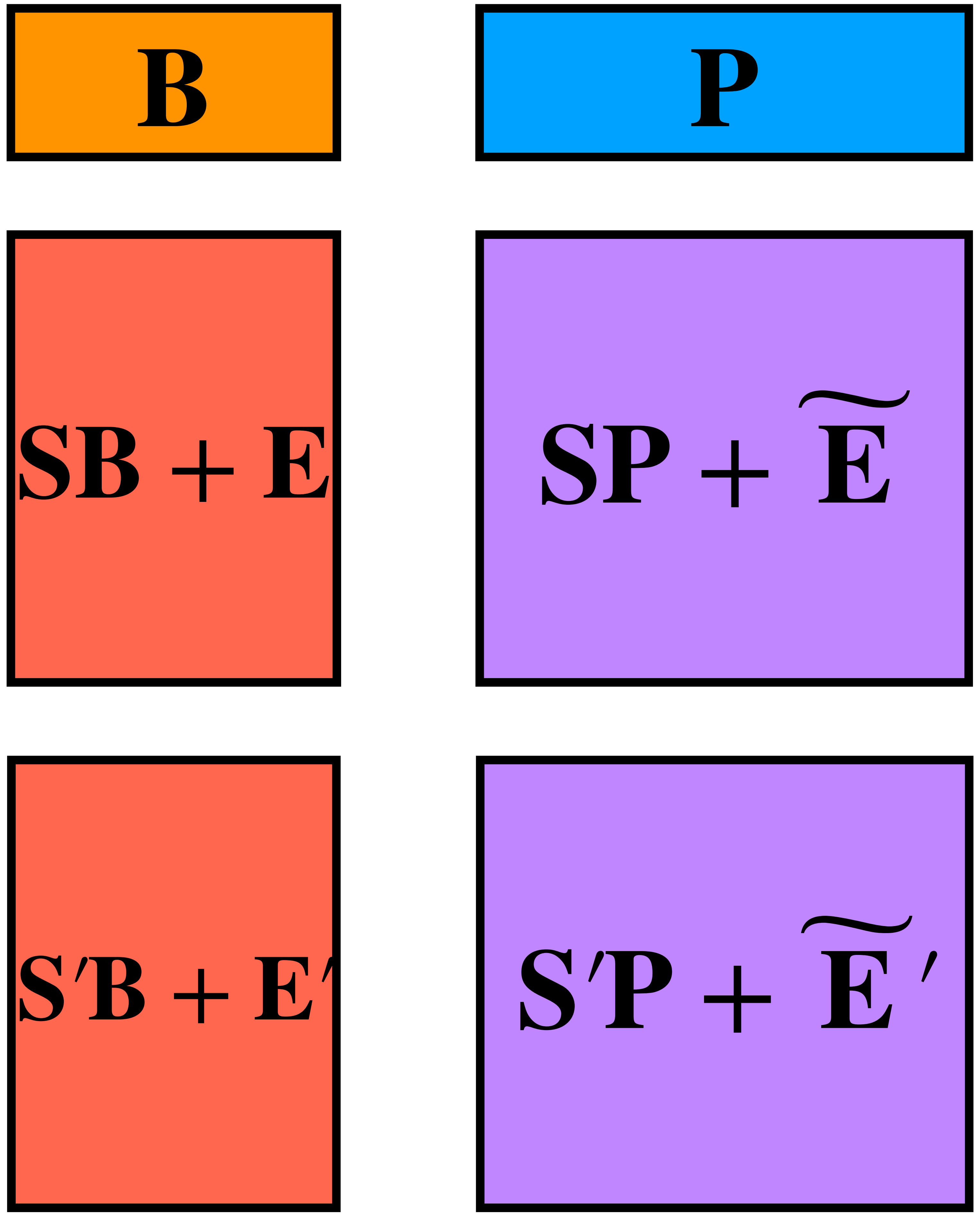
Example

Want to be able to compute:



Example

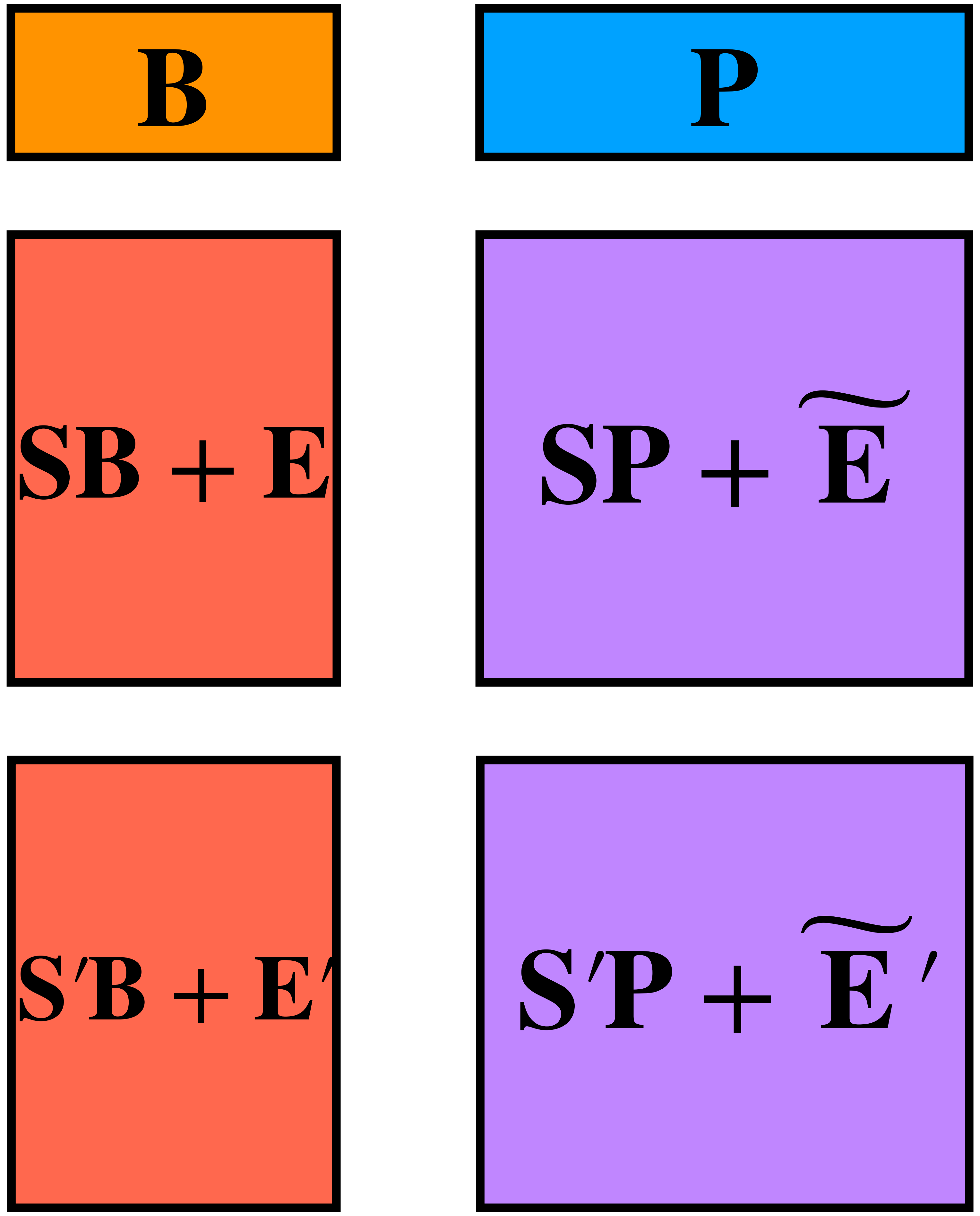
Want to be able to compute:



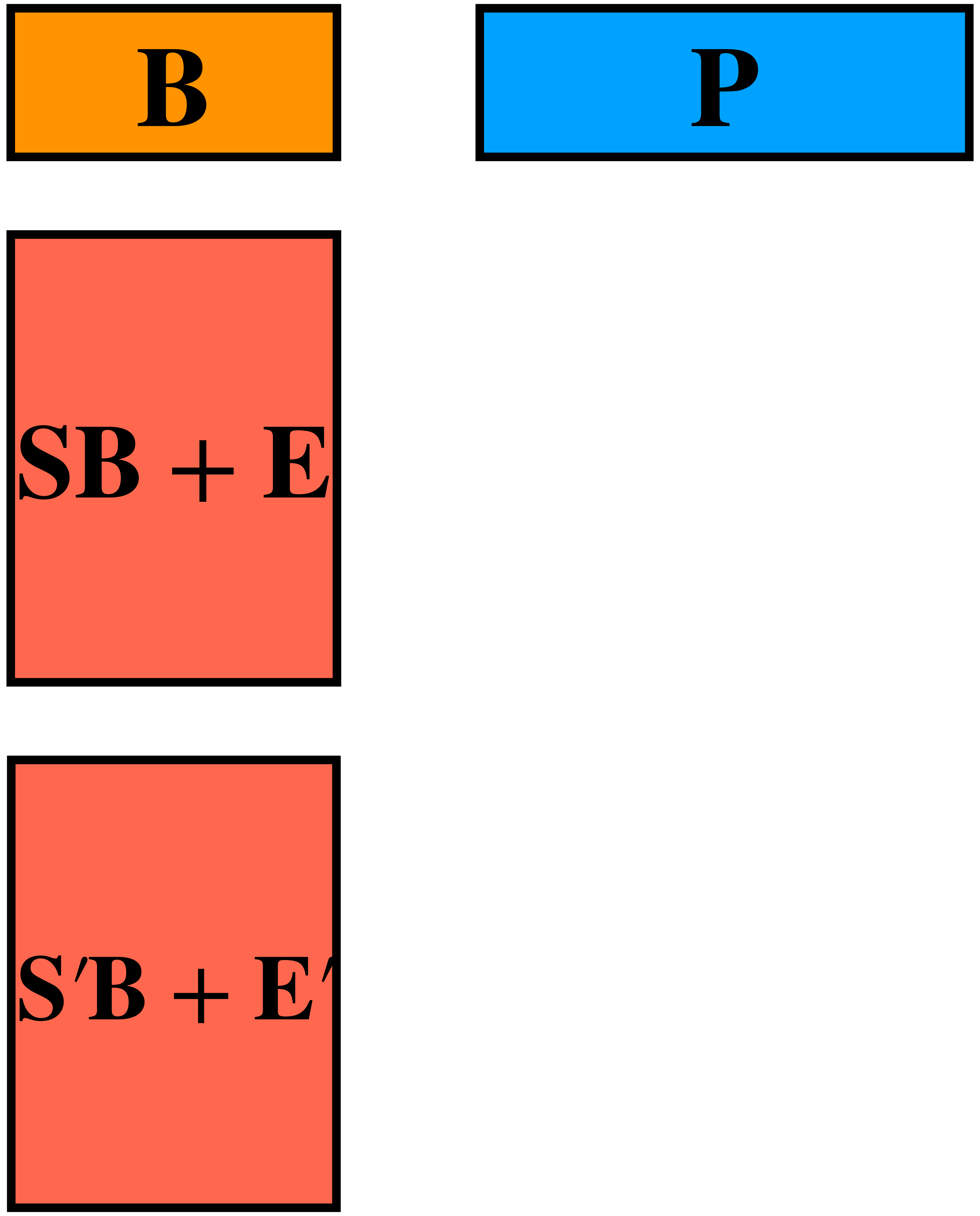
But want to give out:

Example

Want to be able to compute:

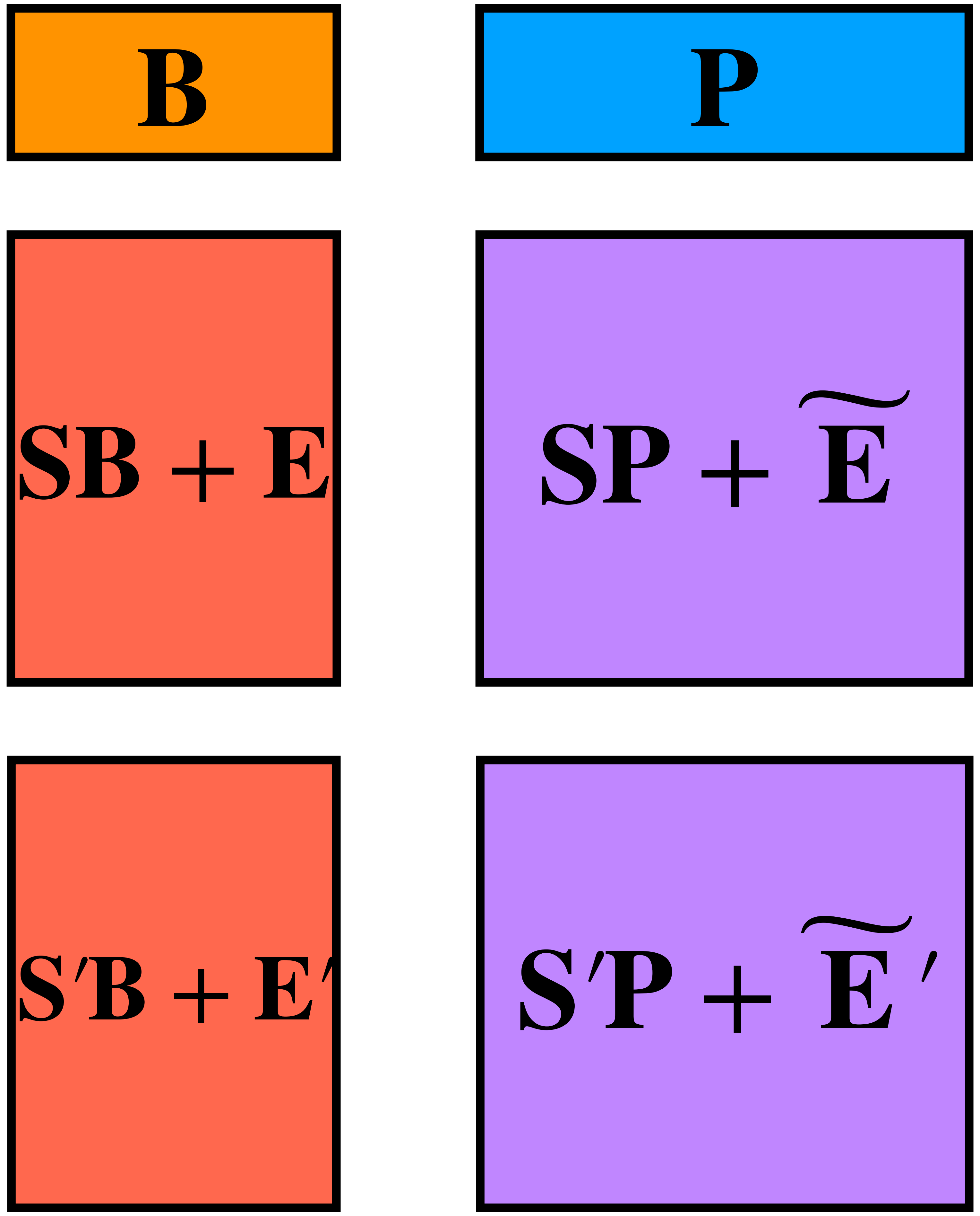


But want to give out:

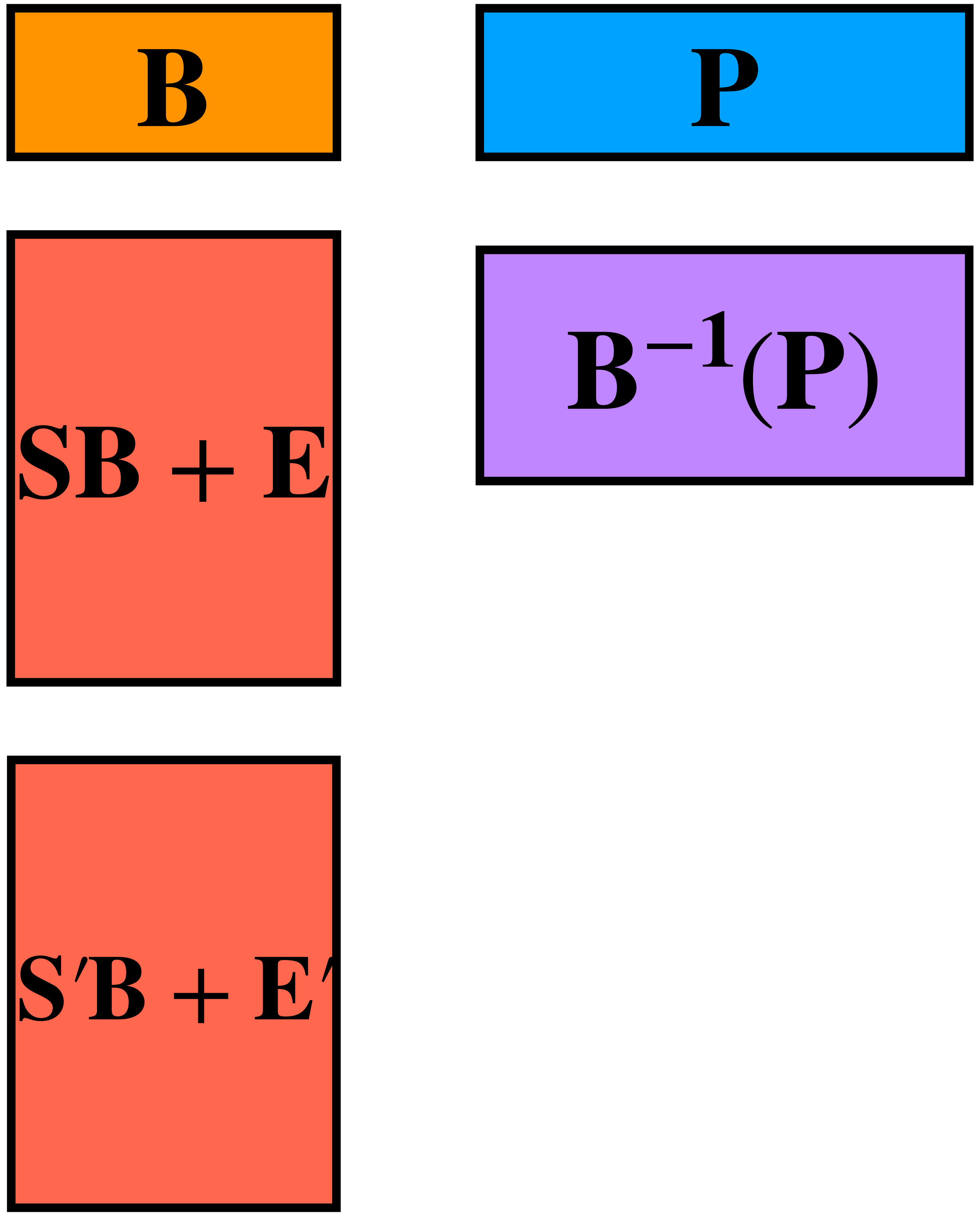


Example

Want to be able to compute:



But want to give out:



Example

$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

Want to be able to compute:

$\mathbf{B}$ $\mathbf{P}$

$\mathbf{SB} + \mathbf{E}$ $\mathbf{SP} + \widetilde{\mathbf{E}}$

$\mathbf{S'B} + \mathbf{E'}$ $\mathbf{S'P} + \widetilde{\mathbf{E}}'$

But want to give out:

$\mathbf{B}$ $\mathbf{P}$

$\mathbf{SB} + \mathbf{E}$ $\mathbf{B}^{-1}(\mathbf{P})$

$\mathbf{S'B} + \mathbf{E'}$

Example

$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

Want to be able to compute:

$\mathbf{B}$ $\mathbf{P}$

$\mathbf{SB} + \mathbf{E}$ $\mathbf{SP} + \widetilde{\mathbf{E}}$

$\mathbf{S'B} + \mathbf{E'}$ $\mathbf{S'P} + \widetilde{\mathbf{E}}'$

But want to give out:

$\mathbf{B}$ $\mathbf{P}$

$\mathbf{SB} + \mathbf{E}$ $\mathbf{B}^{-1}(\mathbf{P})$

$\mathbf{S'B} + \mathbf{E'}$

Let's you approximately compute $\mathbf{SP}$ and $\mathbf{S'P}$! Gives you *compression*

Example

$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

Want to be able to compute:

$\mathbf{B}$ $\mathbf{P}$

$\mathbf{SB} + \mathbf{E}$ $\mathbf{SP} + \widetilde{\mathbf{E}}$

$\mathbf{S'B} + \mathbf{E'}$ $\mathbf{S'P} + \widetilde{\mathbf{E}}'$

But want to give out:

$\mathbf{B}$ $\mathbf{P}$

$\mathbf{SB} + \mathbf{E}$ $\mathbf{B}^{-1}(\mathbf{P})$

$\mathbf{S'B} + \mathbf{E'}$

Let's you approximately compute $\mathbf{SP}$ and $\mathbf{S'P}$! Gives you *compression*

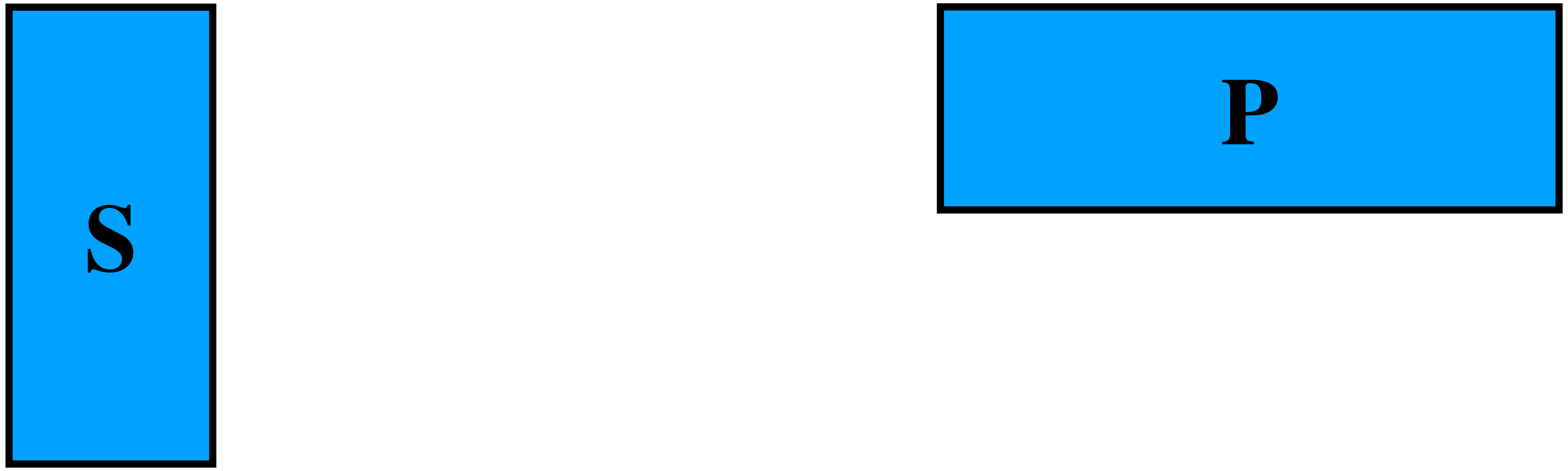
Evasive LWE:
When can give out $\mathbf{B}^{-1}(\mathbf{P})$?

Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

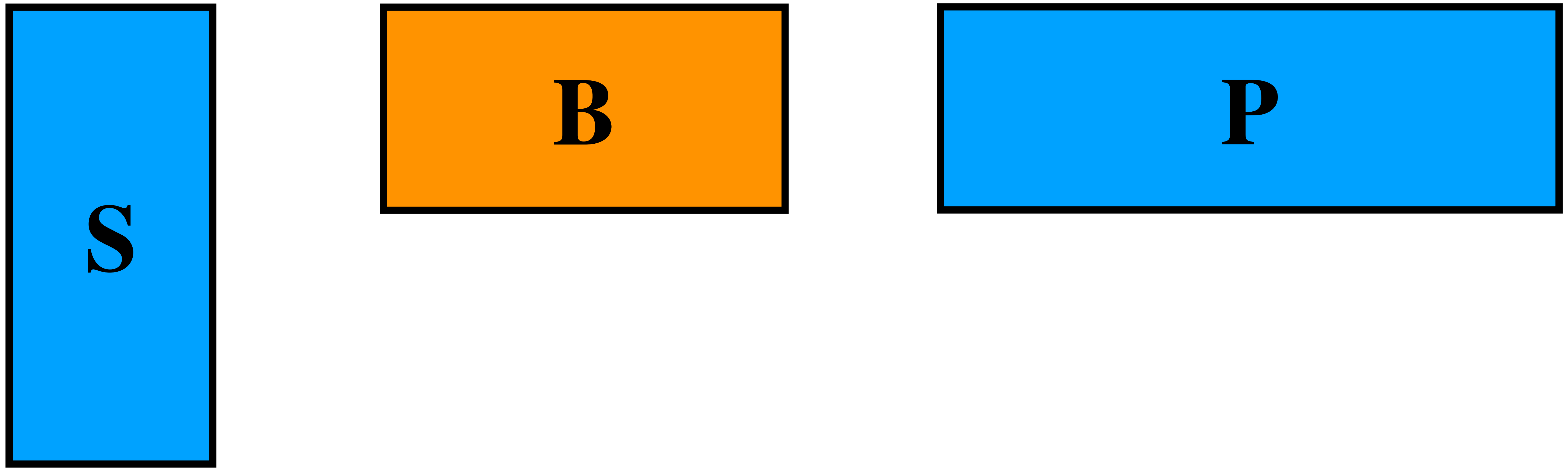
Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.



Evasive LWE [Wee '22, Tsabary '22]

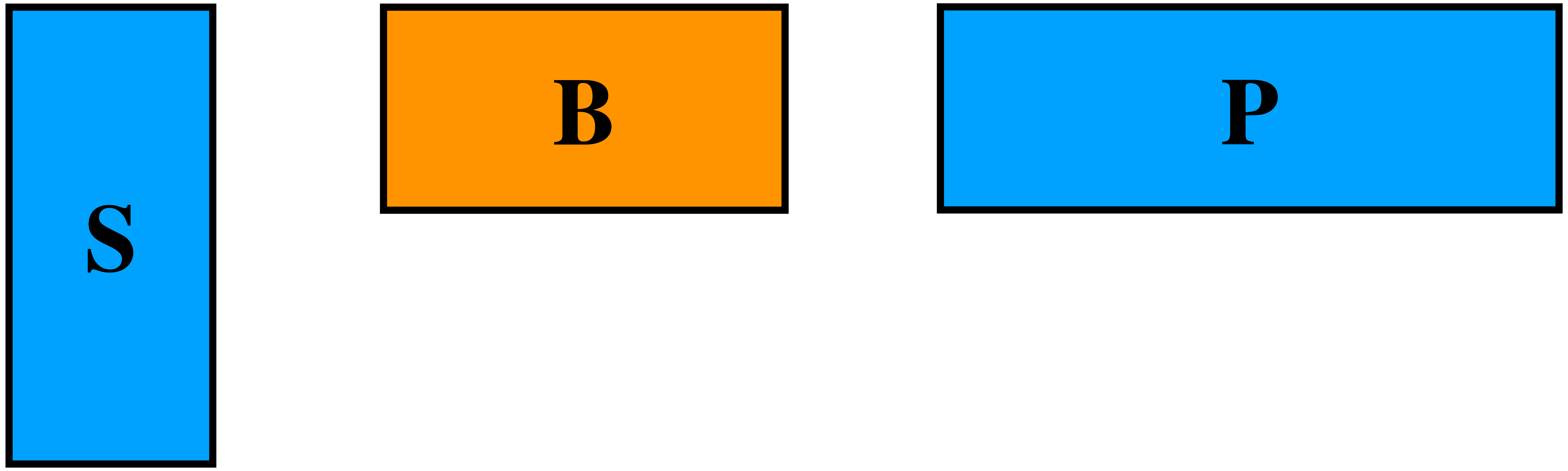
- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.



Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}$, aux $\leftarrow$ Samp(rand).

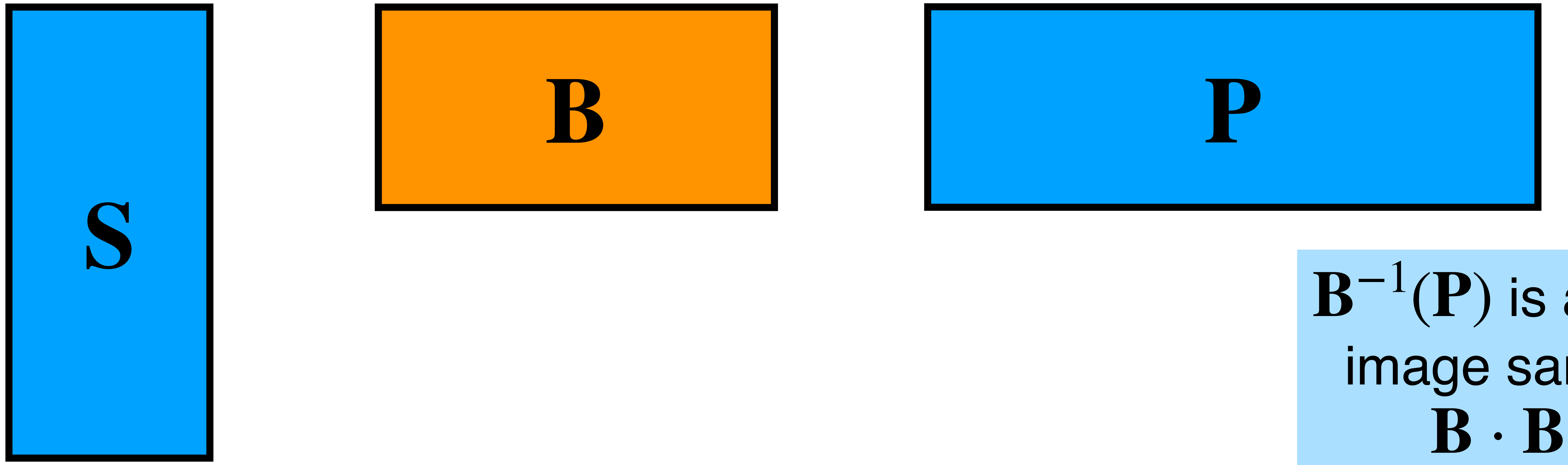
then $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$



Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

then $$(\mathbf{B}, \mathbf{P}, \mathbf{S}\mathbf{B} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$



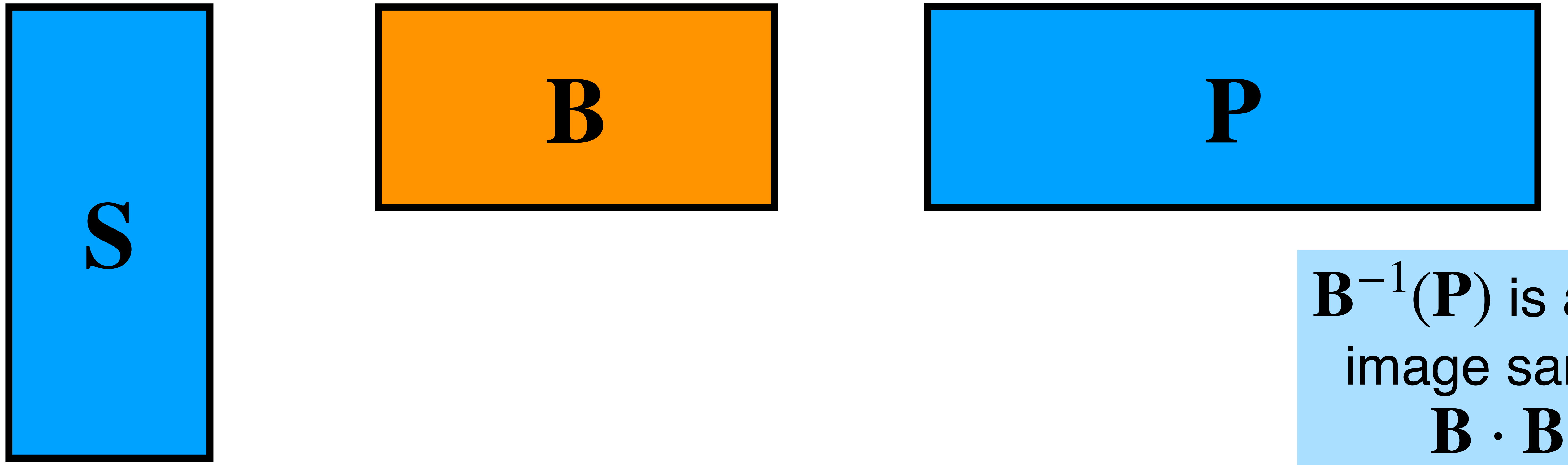
$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

if $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$



$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

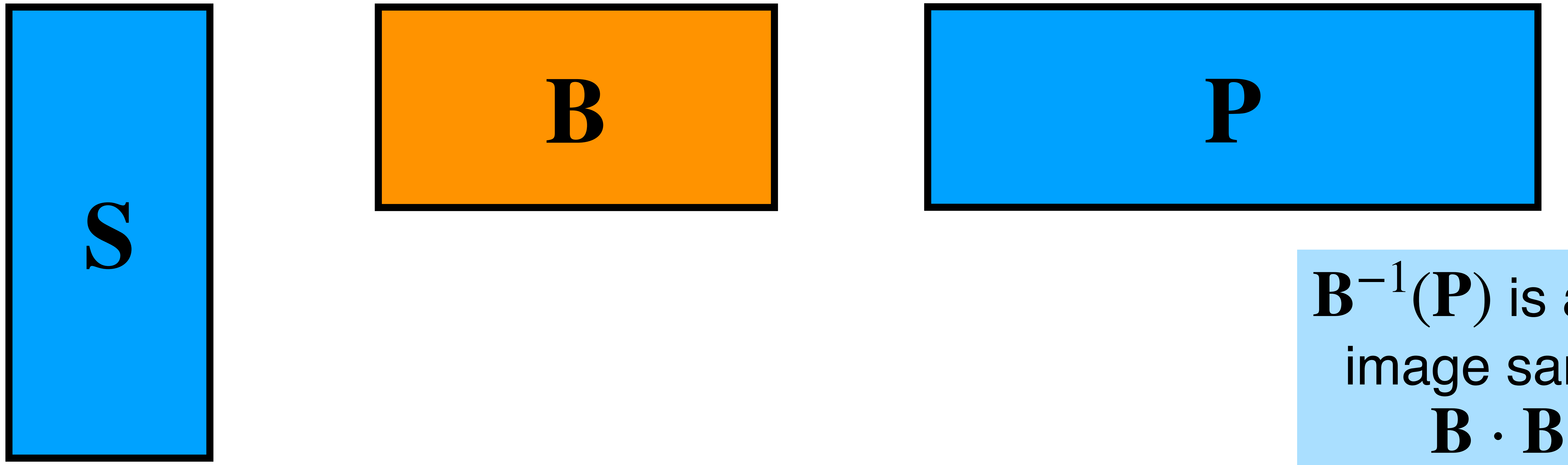
Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}, \text{aux} \leftarrow \text{Samp}(\text{rand})$.

A heuristic to justify the post-condition

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$



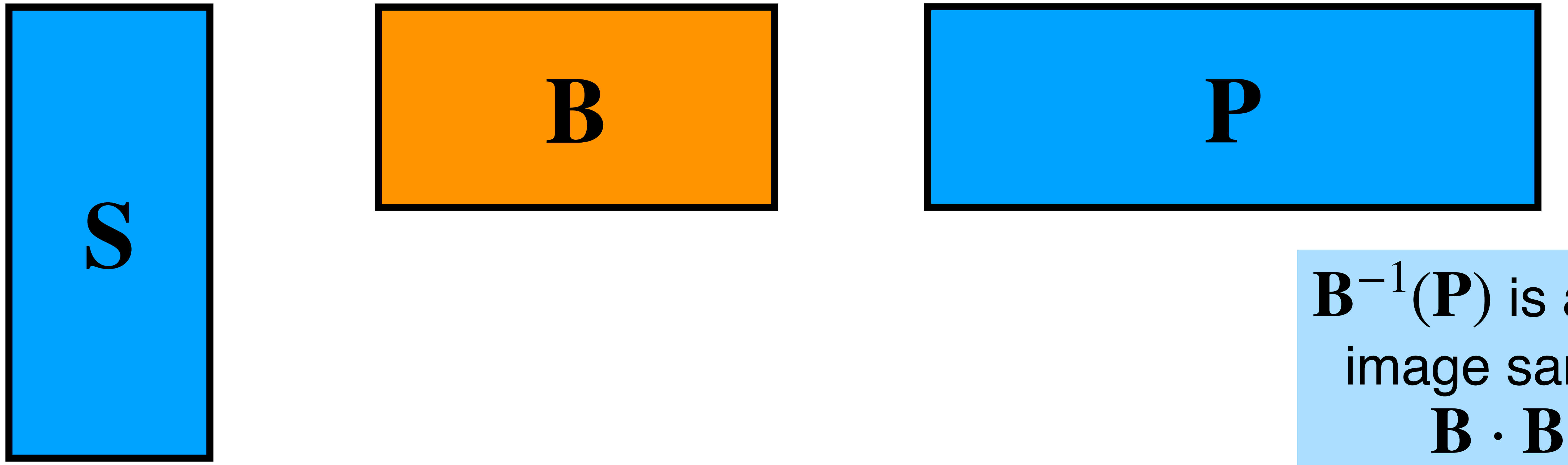
$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B}\cdot\mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

if $$(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

then $$(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$



$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

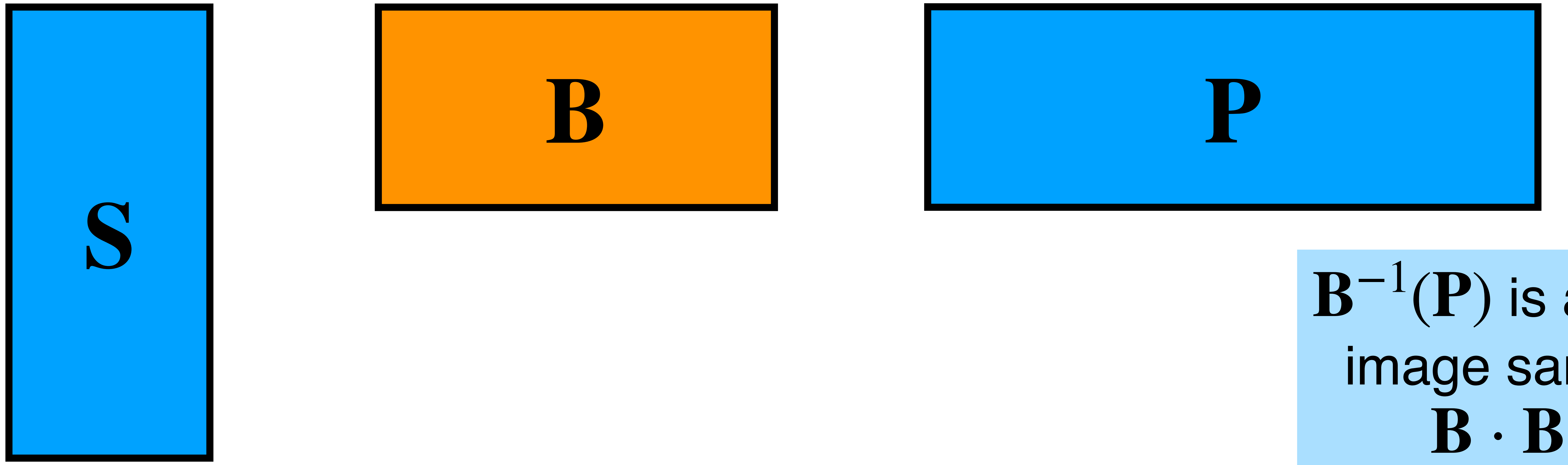
Evasive LWE [Wee '22, Tsabary '22]

- Let $\mathbf{S}, \mathbf{P}$, aux $\leftarrow$ Samp(rand).

Will omit aux for the next few slides.

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$



$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

Toy Examples

[Inspired by Hoeteck's talks]

if $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

then $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$

Toy Examples

[Inspired by Hoeteck's talks]

if $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

then $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB} + \mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$

$\mathbf{B}^{-1}(\mathbf{P})$ is a Gaussian pre-image sample such that $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{P}$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB} + \mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB} + \mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB}+\mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB} + \mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

If $\mathbf{SP} = 0$, then both pre and post-condition **do not hold**!

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB} + \mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

If $\mathbf{SP} = 0$, then both pre and post-condition **do not hold**!

$$(\mathbf{SB} + \mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{EB}^{-1}(\mathbf{P})$$

Toy Examples

[Inspired by Hoeteck's talks]

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$

If $\mathbf{P} = \mathscr{U}$, then both pre and post-conditions **hold**! [GPV08]

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_s (\mathbf{B}, \mathbf{BD}, \mathbf{SB}+\mathbf{E}, \mathbf{D}) \approx_c (\mathbf{B}, \mathbf{BD}, \mathscr{U}, \mathbf{D})$$

If $\mathbf{SP} = 0$, then both pre and post-condition **do not hold**!

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) = \mathbf{EB}^{-1}(\mathbf{P})$$

Both $\mathbf{E}$ and $\mathbf{B}^{-1}(\mathbf{P})$ have low norm! We now have an equation over **integers,** AKA **"zeroizing"**

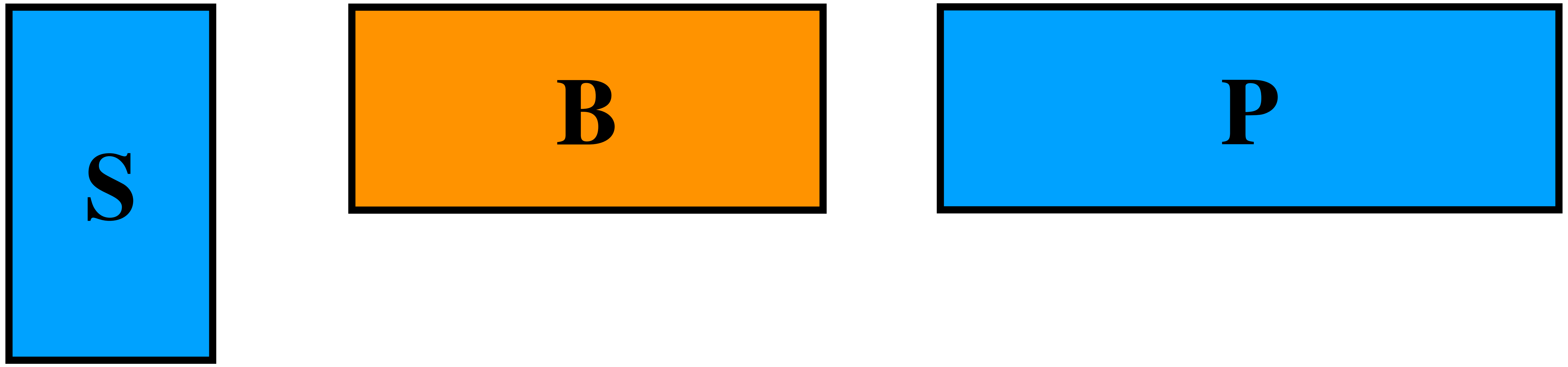
Evasive LWE: Design Philosophy

[Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

if $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}') \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U})$$

then $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}))$$



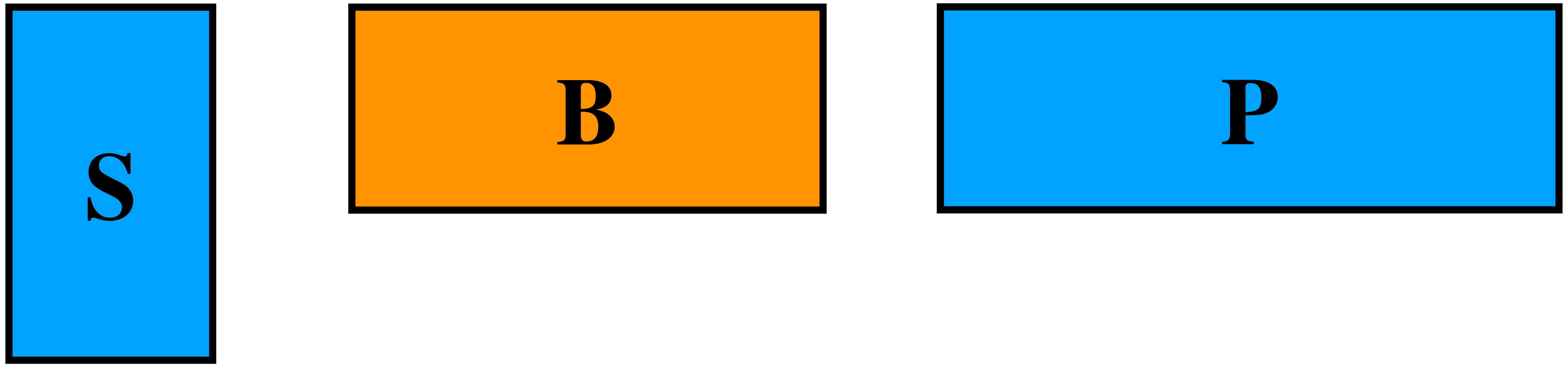
Evasive LWE: Design Philosophy

[Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

if $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}') \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U})$$

then $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}))$$



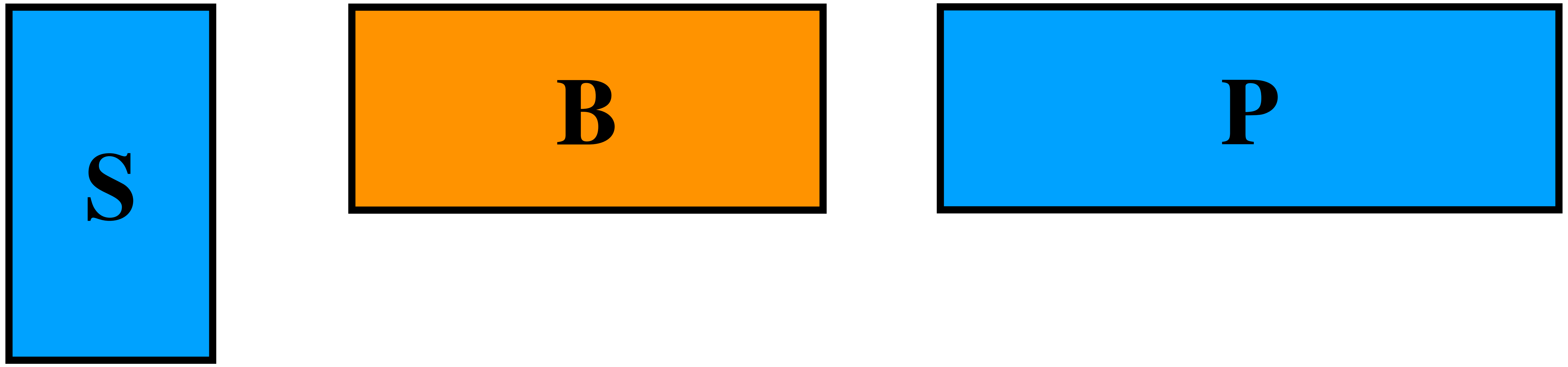
Evasive LWE: Design Philosophy

[Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow$ Samp(rand).

if $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}') \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U})$

then $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}))$



Evasive LWE: Design Philosophy

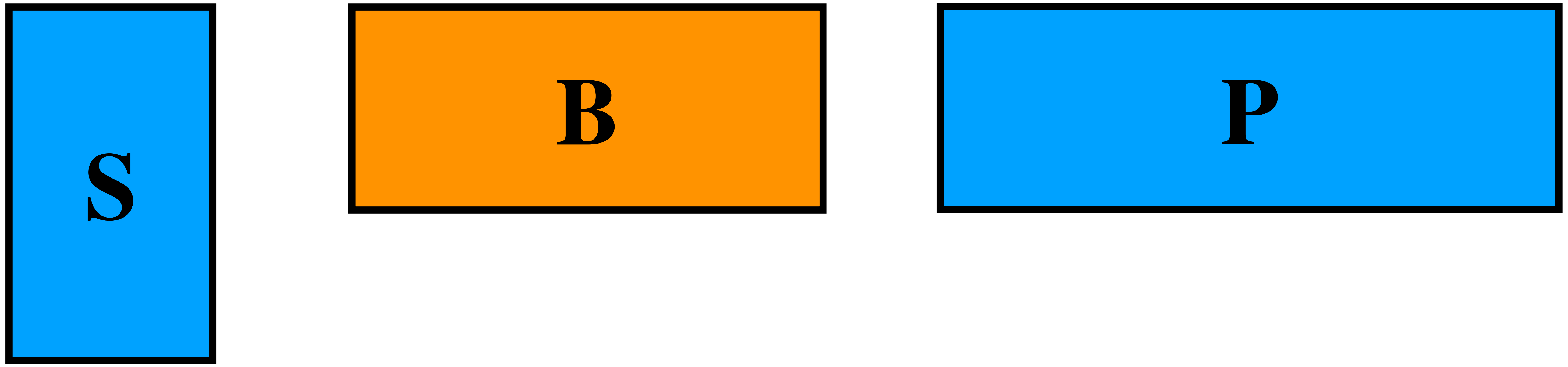
[Wee '22]

Hope: Hard to collect equations over integers if $\mathbf{SP}+\mathbf{E}' \approx_c \mathscr{U}$

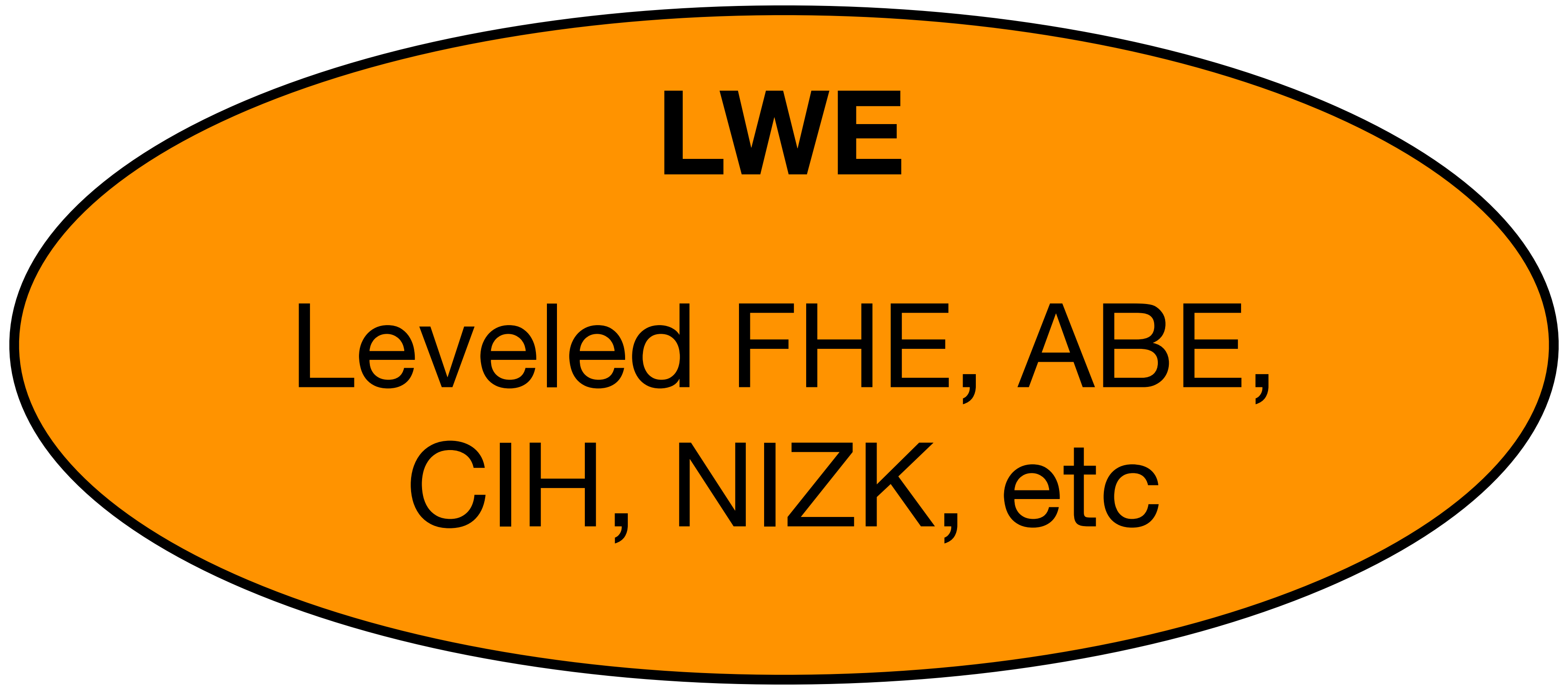
- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

if $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}') \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U})$

then $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P})) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}))$



LWE Zoo



LWE Zoo

LWE

Leveled FHE, ABE, CIH, NIZK, etc

Optimal broadcast

Multi-Authority ABE

Succinct CP-ABE

Unleveled FHE

iO for circuits

Witness encryption

LWE Zoo

LWE

Leveled FHE, ABE, CIH, NIZK, etc

Optimal broadcast

Multi-Authority ABE

*Succinct witness encryption**

Succinct CP-ABE

Unleveled FHE

iO for circuits

Witness encryption

*not even known from iO

Evasive LWE Zoo

LWE

Leveled FHE, ABE,
CIH, NIZK, etc

Optimal broadcast

Multi-Authority ABE

*Succinct witness encryption**

Succinct CP-ABE

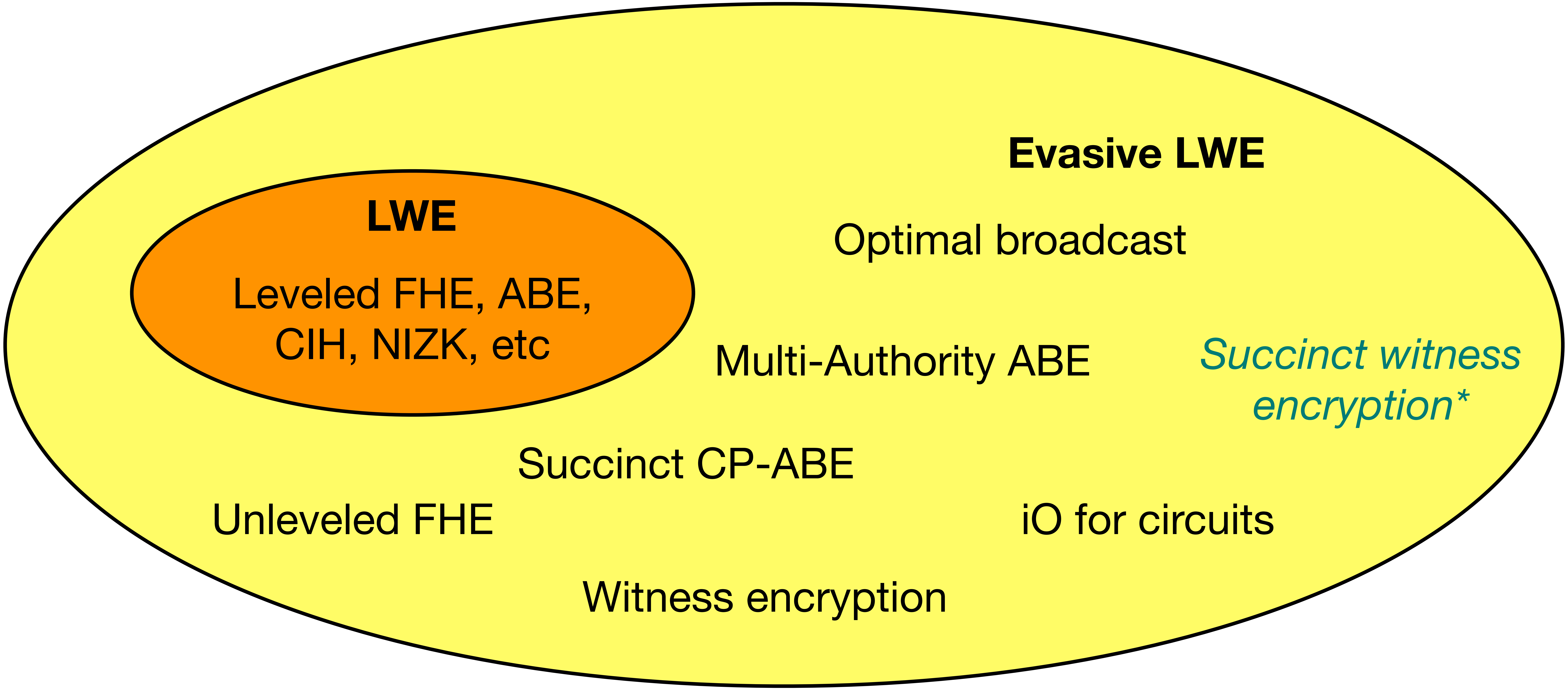
Unleveled FHE

iO for circuits

Witness encryption

*not even known from iO

Evasive LWE Zoo



*not even known from iO

What can we do with Evasive LWE?

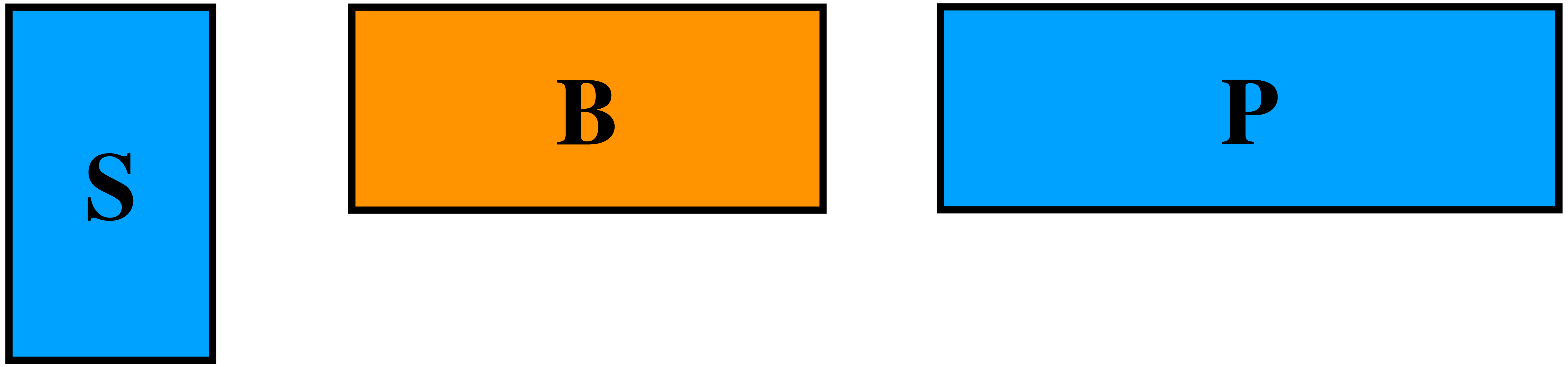
- Optimal Broadcast Encryption [Wee22]
- Multi-Authority ABE [WWW22]
- Unbounded depth ABE [HLL23]
- Witness Encryption [CVW18, VWW22]
- SNARKs for UP [**M**PV24]
- SNARGs for NP [JKL**M**24]
- ABE for TMs [AKY24]
- Pseudorandom Obfuscation (FHE, succinct WE) [DJM**M**PV25]
- Pseudorandom functional encryption [AKY24]
- Succinct iO for Turing Machines [JJ**M**P25]

<u>Public-Coin</u> Evasive LWE [Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

if $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}=\mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \mathsf{aux}=\mathsf{rand})$

then $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}=\mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}=\mathsf{rand})$

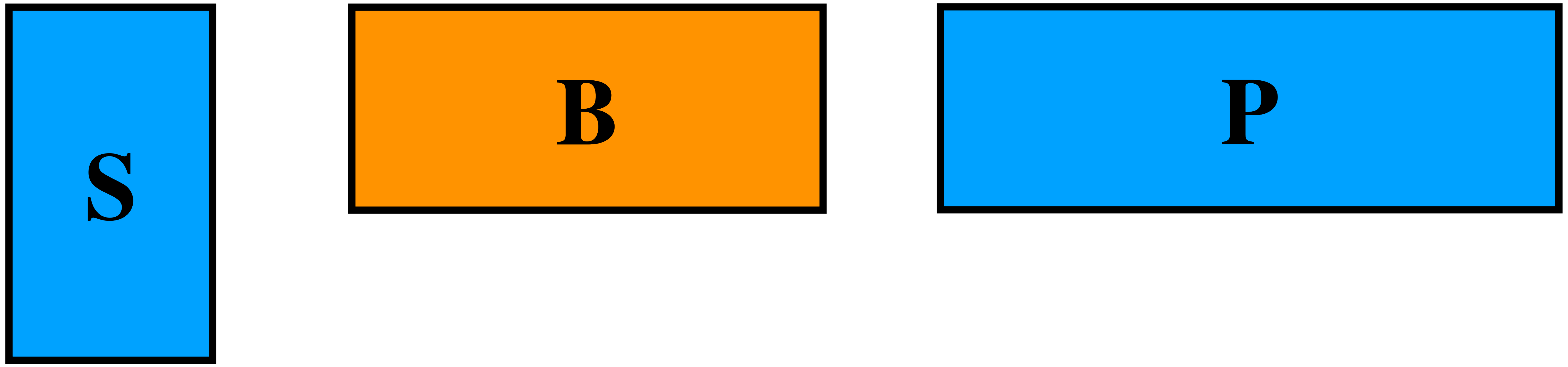


<u>Public-Coin</u> Evasive LWE [Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

$$\text{if} \quad (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux} = \mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux} = \mathsf{rand})$$

$$\text{then} \quad (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux} = \mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux} = \mathsf{rand})$$



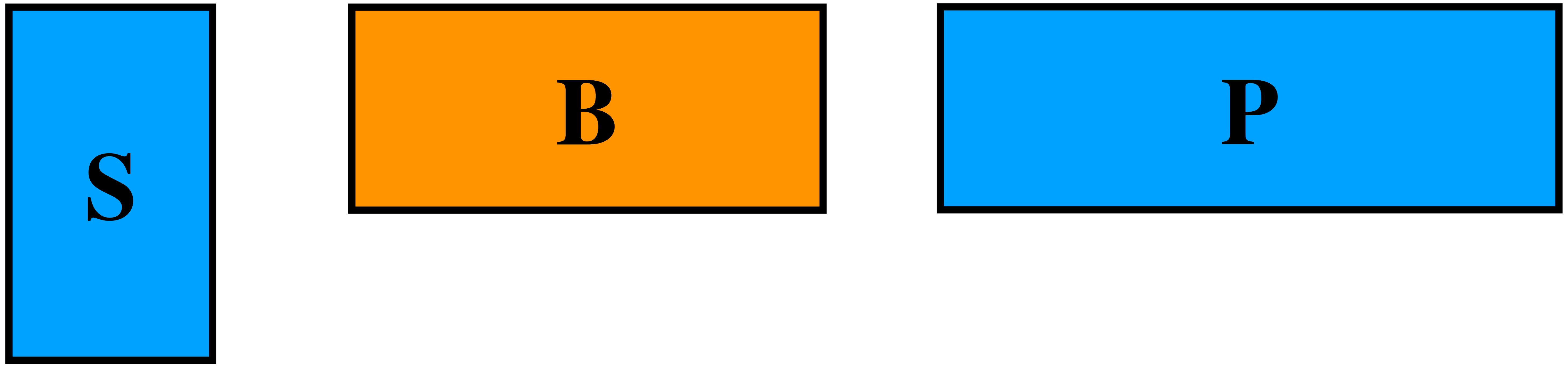
Public-Coin Evasive LWE [Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

Randomness used to sample $\mathbf{S}, \mathbf{P}$ is public

if $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}=\mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux}=\mathsf{rand})$

then $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}=\mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}=\mathsf{rand})$



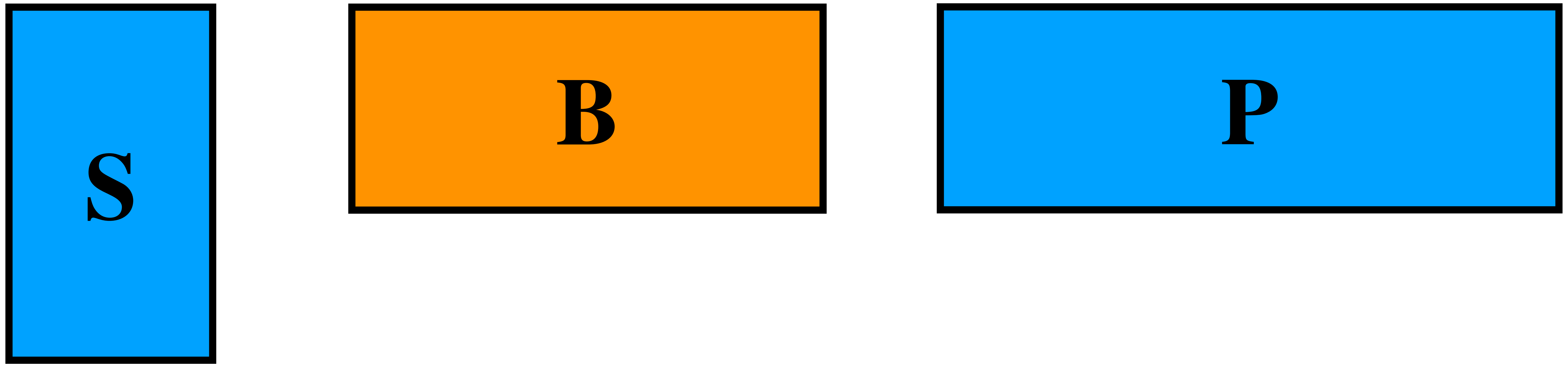
Public-Coin Evasive LWE [Wee '22]

- Let $\mathbf{S}, \mathbf{P} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

Randomness used to sample $\mathbf{S}, \mathbf{P}$ is public

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux} = \mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux} = \mathsf{rand})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux} = \mathsf{rand}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux} = \mathsf{rand})$



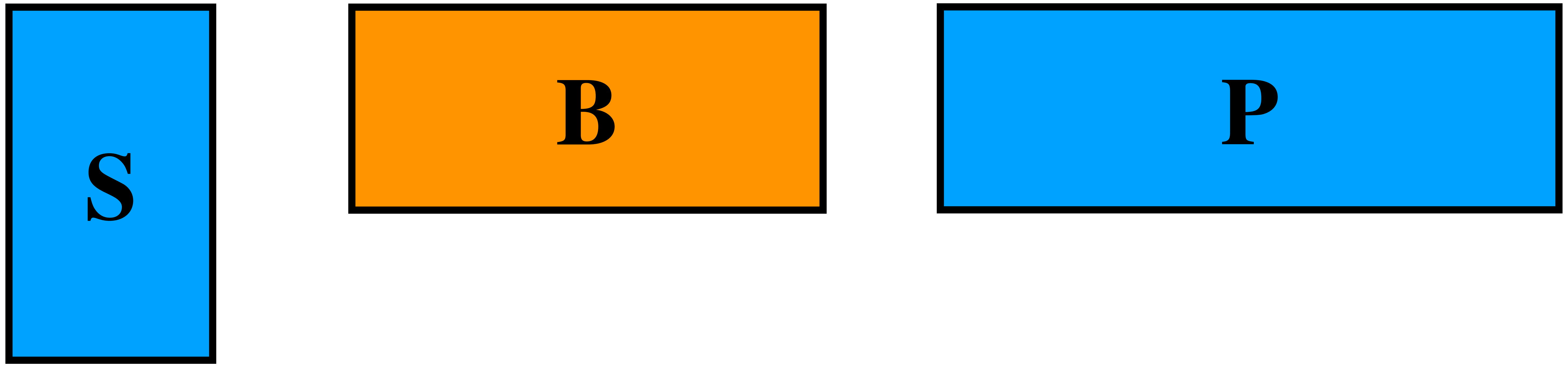
Private-Coin Evasive LWE

[VWW22, Tsabary 22]

- Let $\mathbf{S}, \mathbf{P}, \text{aux} \leftarrow \text{Samp(rand)}$.

$$\text{if} \quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$$

$$\text{then} \quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$$



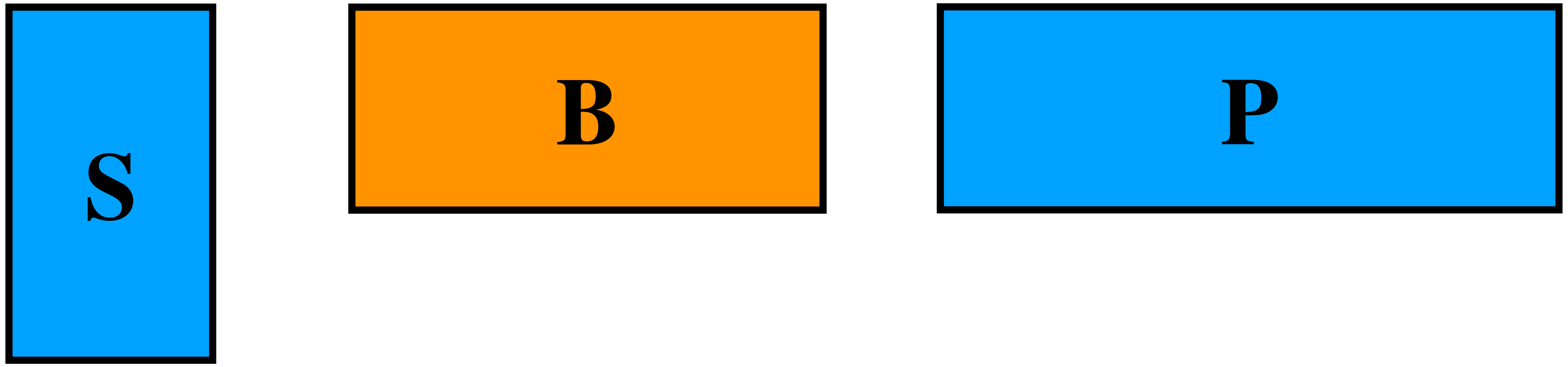
Private-Coin Evasive LWE

[VWW22, Tsabary 22]

- Let $\mathbf{S}, \mathbf{P}$, aux $\leftarrow$ Samp(rand).

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$



<u>Private-Coin</u> Evasive LWE

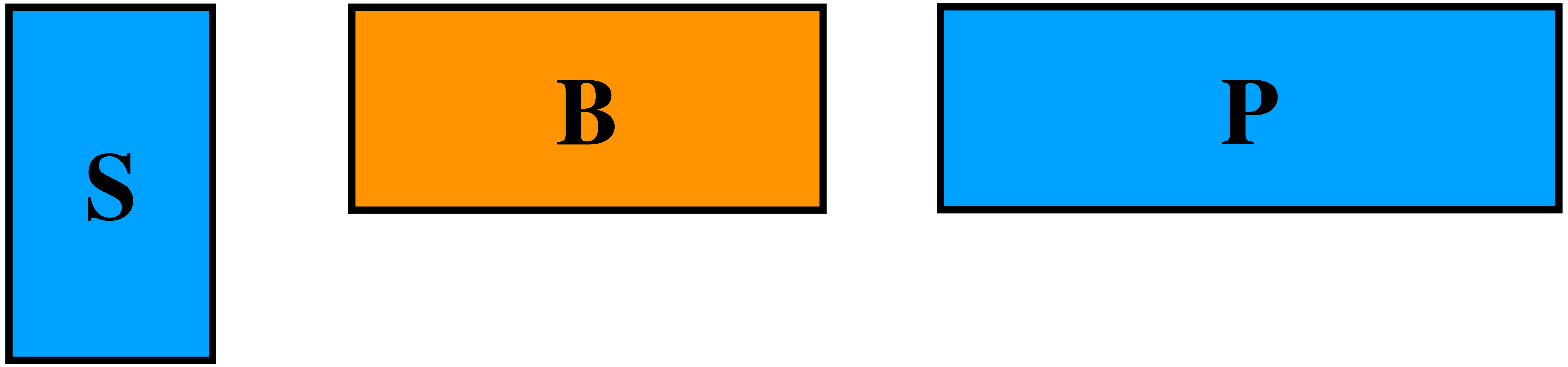
[VWW22, Tsabary 22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

Randomness used to sample $\mathbf{S}, \mathbf{P}$, aux is **<u>private</u>**

if $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $\quad (\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$



Private-Coin Evasive LWE

[VWW22, Tsabary 22]

- Let $\mathbf{S}, \mathbf{P}, \mathsf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$.

Randomness used to sample $\mathbf{S}, \mathbf{P}$, aux is **private**

if $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

then $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$

$\mathbf{S}$

Many variants! E.g. Fully available $\mathbf{B}, \mathbf{P}$, Hidden $\mathbf{B}, \mathbf{P}$, etc.

Evasive LWE Zoo

LWE

Leveled FHE, ABE, CIH, NIZK, etc

Optimal broadcast

Multi-Authority ABE

*Succinct witness encryption**

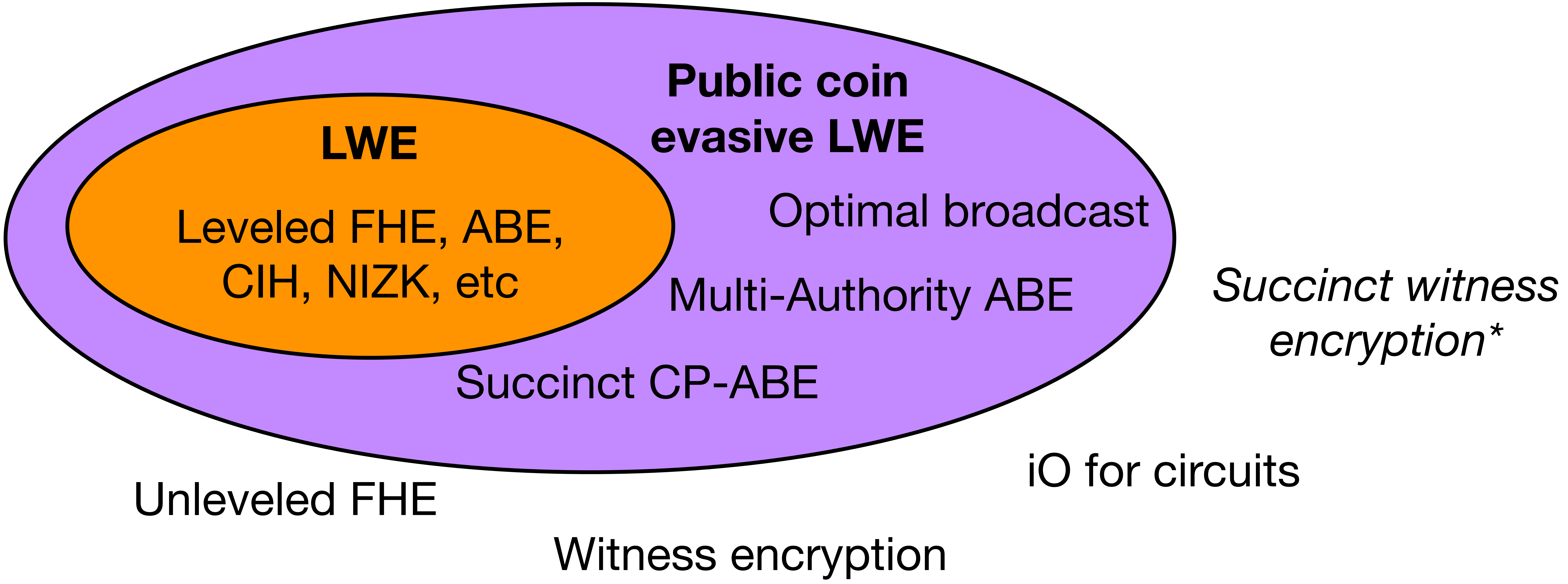
Succinct CP-ABE

iO for circuits

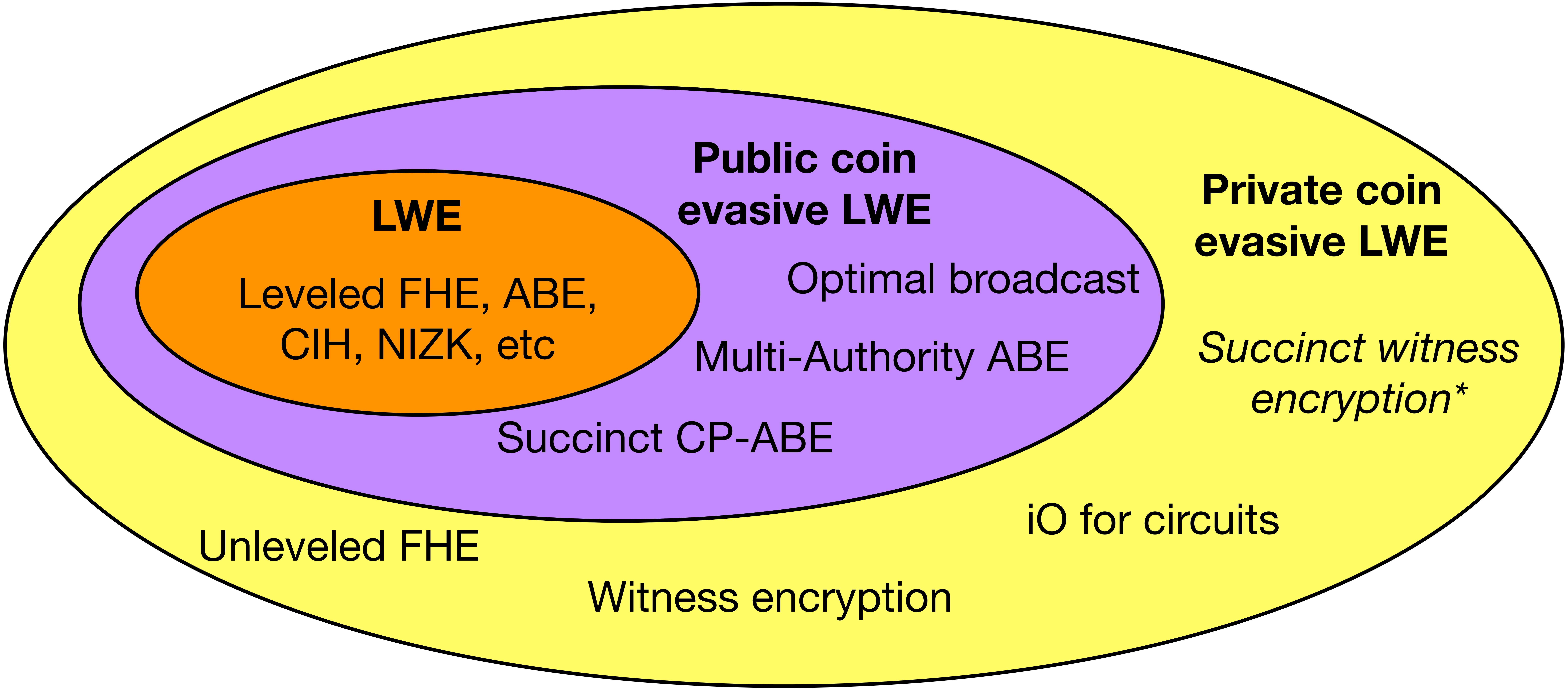
Unleveled FHE

Witness encryption

Evasive LWE Zoo



Evasive LWE Zoo

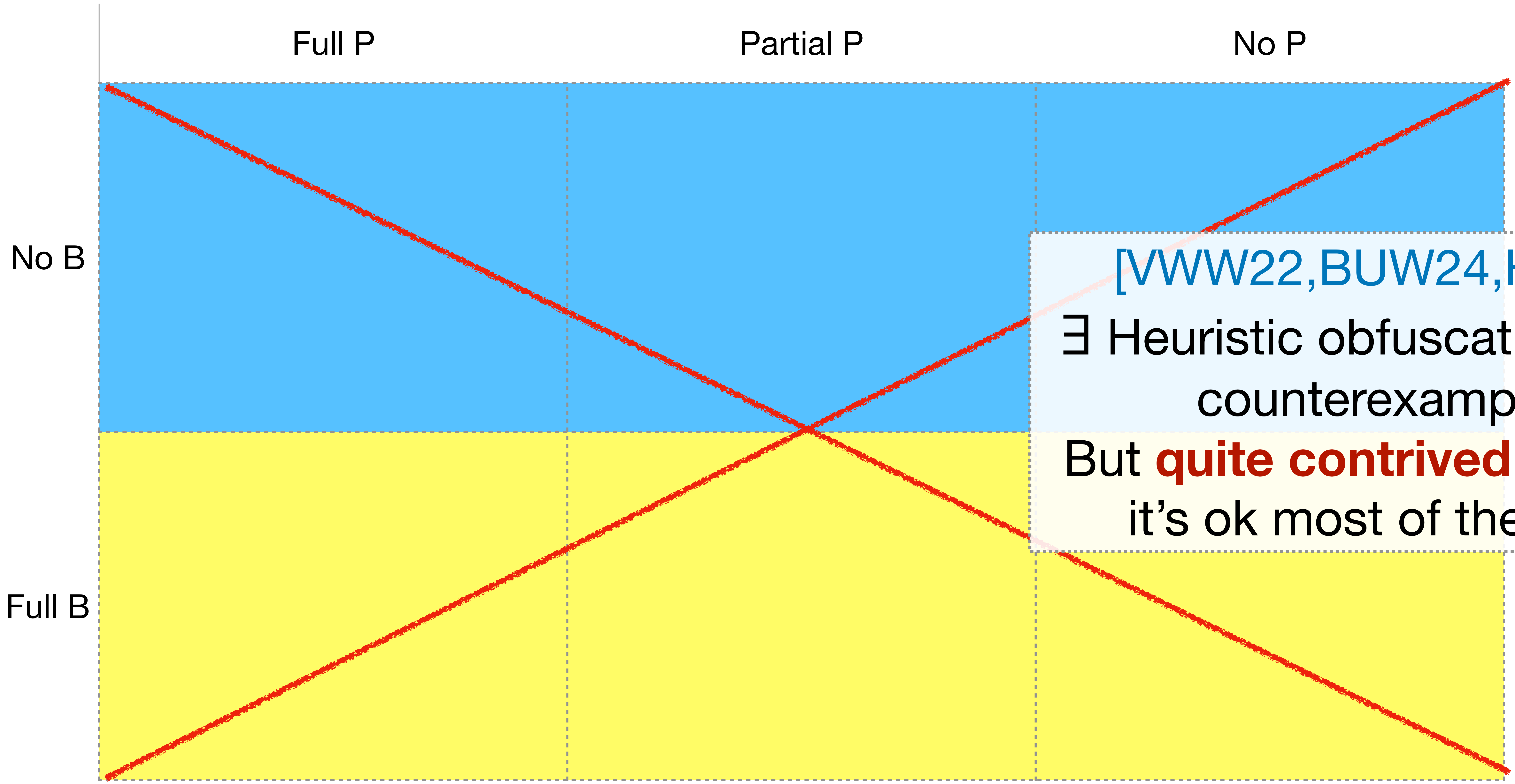


*not even known from iO

Private-Coin Evasive Attacks

	Full P	Partial P	No P
No B			
Full B			

Private-Coin Evasive Attacks

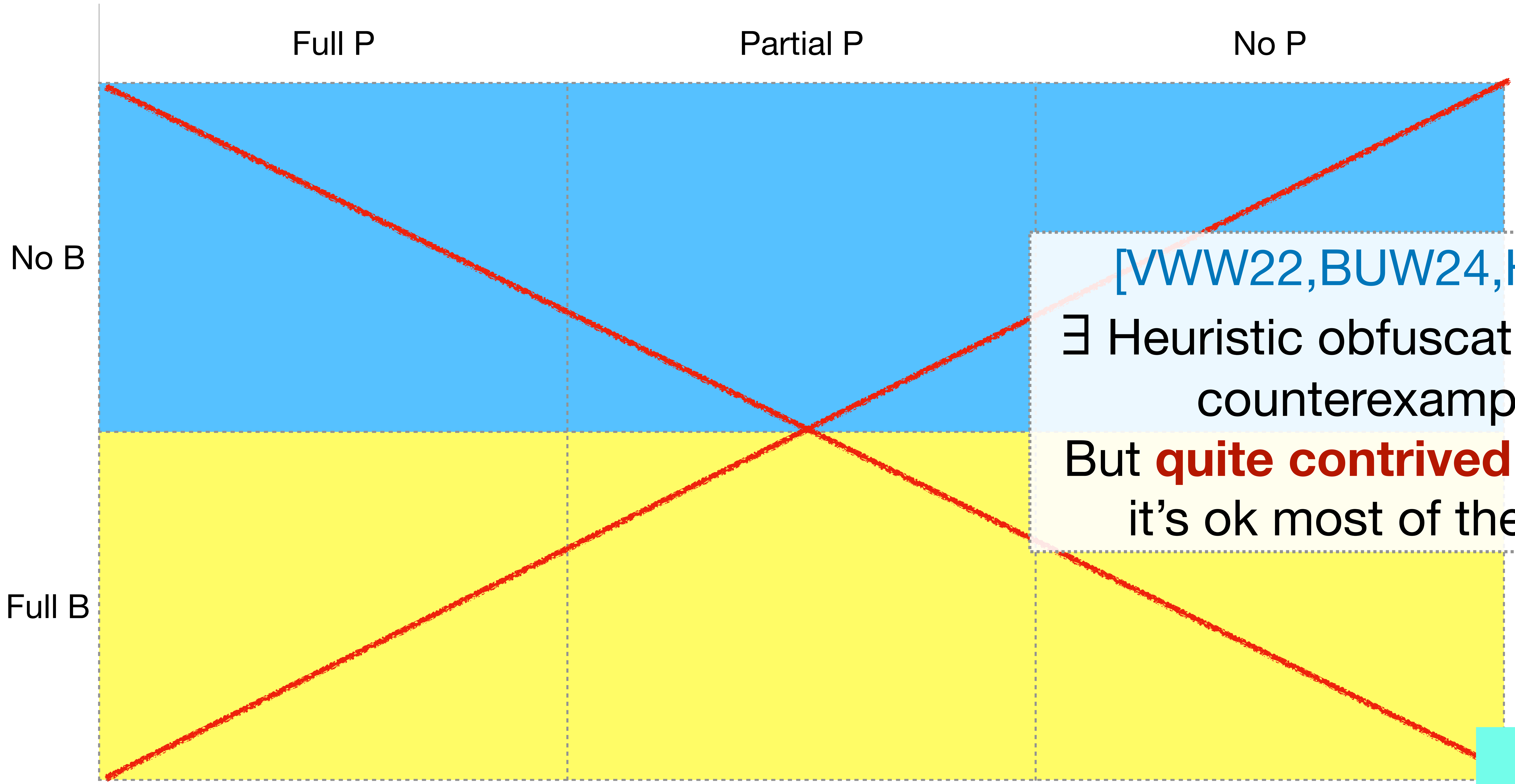


[VWW22,BUW24,HHY25]

∃ Heuristic obfuscation based counterexample!!!

But **quite contrived**… Maybe it’s ok most of the time?

Private-Coin Evasive Attacks



[VWW22,BUW24,HHY25]

∃ Heuristic obfuscation based counterexample!!!

But **quite contrived**... Maybe it's ok most of the time?

Bonus slide with attack. Ask later!

Private-Coin Evasive Attacks

[Brzuska-Unal-Woo '25]

	Full P	Partial P	No P
No B			
Full B			

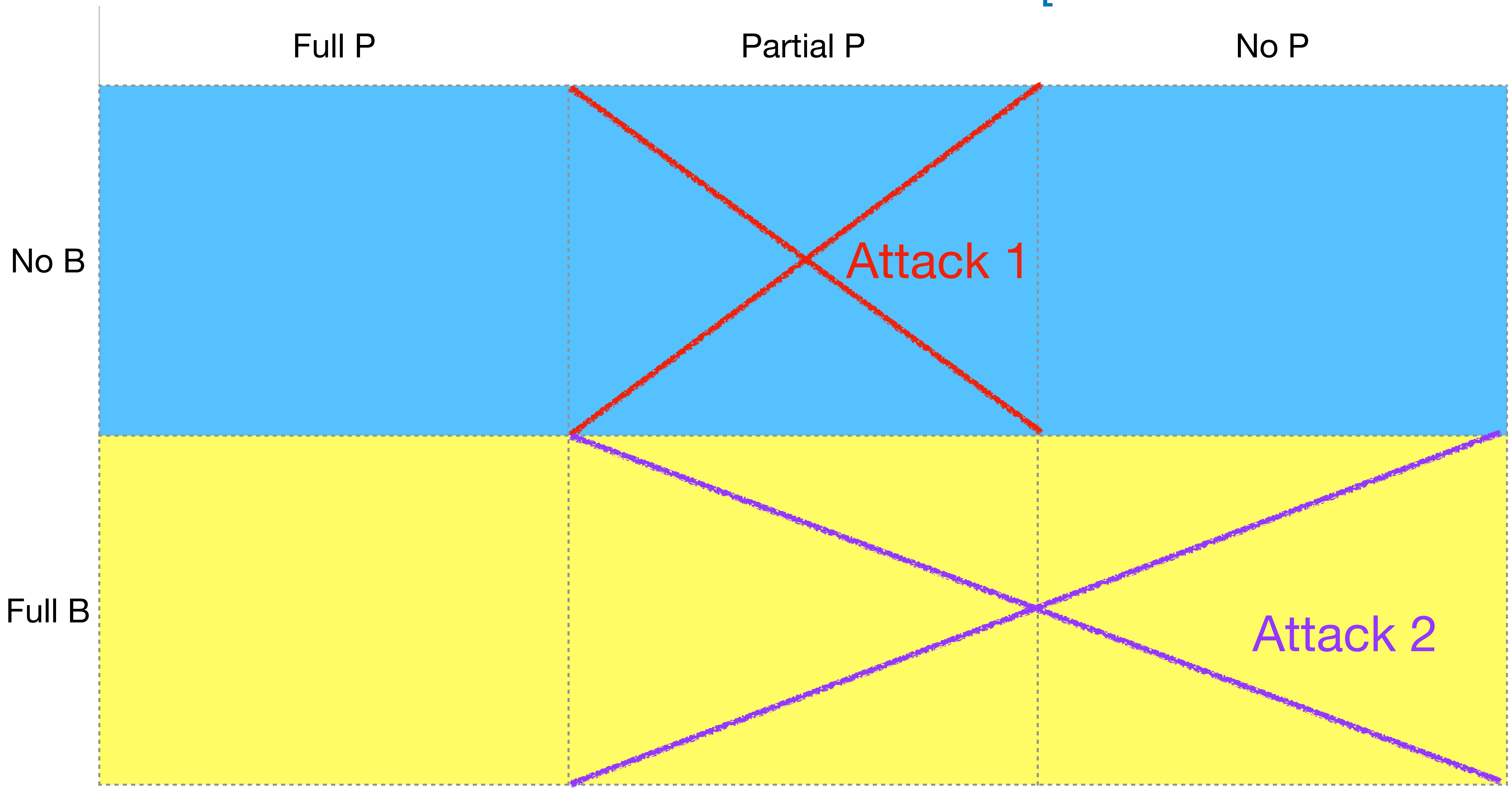
Private-Coin Evasive Attacks

[Brzuska-Unal-Woo ’25]

	Full P	Partial P	No P
No B		Attack 1	
Full B			

Private-Coin Evasive Attacks

[Brzuska-Unal-Woo ’25]



Private-Coin Evasive Attacks

[Brzuska-Unal-Woo ’25]

	Full P	Partial P	No P
No B			Private-coin hiding evasive LWE*
Full B	Private-coin binding evasive LWE		

*pre-condition needs to satisfy additional conditions, but we will gloss over this for this talk

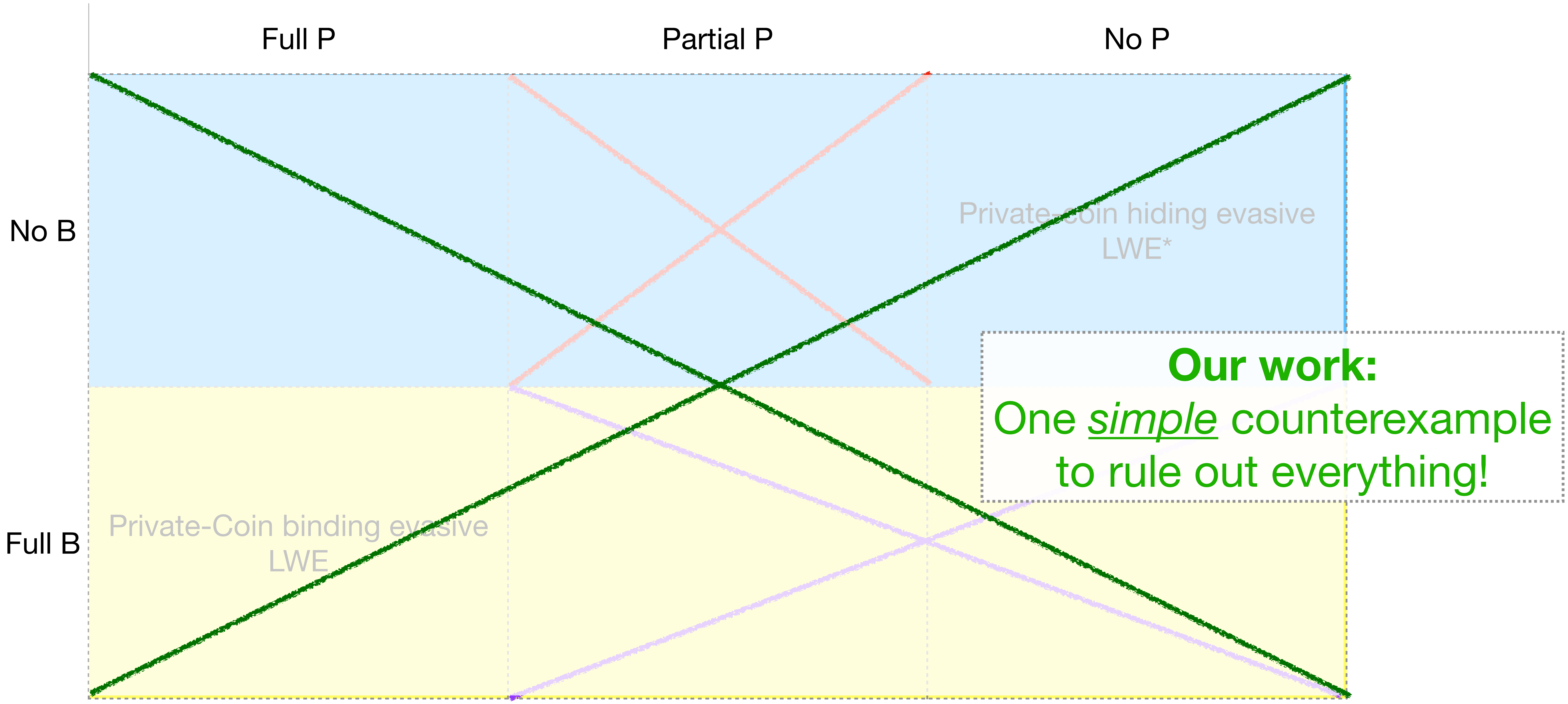
Private-Coin Evasive Attacks

	Full P	Partial P	No P
No B			Private-coin hiding evasive LWE*
Full B	Private-Coin binding evasive LWE		

Our work:
One *simple* counterexample to rule out everything!

*pre-condition needs to satisfy additional conditions, but we will gloss over this for this talk

Private-Coin Evasive Attacks



*pre-condition needs to satisfy additional conditions, but we will gloss over this for this talk

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$ such that:

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow$ Samp(rand) such that:

Satisfies strongest pre-condition

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow \text{Samp(rand)}$ such that:

Satisfies strongest pre-condition

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$$

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$ such that:

Satisfies strongest pre-condition

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Does not satisfy weakest post-condition

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow \mathsf{Samp}(\mathsf{rand})$ such that:

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow$ Samp(rand) such that:

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

- $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow$ Samp(rand) such that:

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

- $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform** $\mathbb{Z}_q$ entries, where q is **odd.**

Our attack: Evasive LWE

- We give $\mathbf{S}, \mathbf{P}, \mathbf{aux} \leftarrow$ Samp(rand) such that:

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \not\approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$$

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$ entries**, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Attack on post-condition

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - \mathbf{2T}$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$ where $\text{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \text{aux} \pmod q$$

$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E}\cdot\mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E}\cdot\mathbf{B}^{-1}(\mathbf{P}) + 2\mathbf{T} \pmod q$$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + 2\mathbf{T} \pmod q$$

Because $\mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})$ is *small*, whp. does not wrap around $\bmod q$!

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + 2\mathbf{T} \pmod q$$
$$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod 2$$

Because $\mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})$ is *small*, whp. does not wrap around $\bmod q$!

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$ where $\text{aux} = \mathbf{SP} - \mathbf{2T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \text{aux} \pmod{q}$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod{q}$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + \mathbf{2T} \pmod{q}$$
$$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod{2}$$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - \mathbf{2T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + \mathbf{2T} \pmod q$$
$$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod 2$$

In the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$!

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:	RHS:
$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$	
$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$	
$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + 2\mathbf{T} \pmod q$	
$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod 2$	
In the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$!	

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathcal{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - \mathbf{2T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + \mathbf{2T} \pmod q$$
$$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod 2$$

In the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$!

RHS:

$$\mathcal{U} \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \approx_s \mathcal{U} \pmod 2$$

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + 2\mathbf{T} \pmod q$$
$$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod 2$$

In the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$!

RHS:

$$\mathscr{U} \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \approx_s \mathscr{U} \pmod 2$$

Leftover hash lemma!

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \text{aux})$ where $\text{aux} = \mathbf{SP} - \mathbf{2T}$

LHS:

$$(\mathbf{SB}+\mathbf{E})\cdot\mathbf{B}^{-1}(\mathbf{P}) - \text{aux} \pmod q$$
$$= (\mathbf{SP}+\mathbf{E}\cdot\mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E}\cdot\mathbf{B}^{-1}(\mathbf{P}) + \mathbf{2T} \pmod q$$
$$\equiv \mathbf{E}\cdot\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$$

In the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$!

RHS:

$$\mathscr{U}\cdot\mathbf{B}^{-1}(\mathbf{P}) - \text{aux} \approx_s \mathscr{U} \pmod 2$$

Leftover hash lemma!

NOT in the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$ with high probability!
Recall $\mathbf{B}^{-1}(\mathbf{P})$ is wide.

Attack on post-condition

Goal: $(\mathbf{SB}+\mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \not\approx_c (\mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$ where $\mathsf{aux} = \mathbf{SP} - 2\mathbf{T}$

LHS:

$$(\mathbf{SB}+\mathbf{E}) \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \pmod q$$
$$= (\mathbf{SP} + \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P})) - (\mathbf{SP} - 2\mathbf{T}) \pmod q$$
$$= \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) + 2\mathbf{T} \pmod q$$
$$\equiv \mathbf{E} \cdot \mathbf{B}^{-1}(\mathbf{P}) \pmod 2$$

In the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$!

RHS:

$$\mathscr{U} \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathsf{aux} \approx_s \mathscr{U} \pmod 2$$

Leftover hash lemma!

NOT in the row span of $\mathbf{B}^{-1}(\mathbf{P}) \pmod 2$ with high probability!
Recall $\mathbf{B}^{-1}(\mathbf{P})$ is wide.

Zeroizing Attack!!

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform** $\mathbb{Z}_q$ entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal:

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform** $\mathbb{Z}_q$ entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \mathsf{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow \text{Samp}$, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

By noise-flooding and picking $\mathbf{E}'' \ll \mathbf{E}', \mathbf{T}$.
(Pick q to be super polynomial.)

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform** $\mathbb{Z}_q$ entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0, 1, \ldots, \lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform** $\mathbb{Z}_q$ entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow \text{Samp}$, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \text{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

$$\approx_c (\mathscr{U} + \mathbf{E}', \mathscr{U} - 2\mathbf{T})$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow \mathsf{Samp}$, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$ entries**, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

$$\approx_c (\mathscr{U} + \mathbf{E}', \mathscr{U} - 2\mathbf{T})$$

LWE with ***even*** error (because q is odd)

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \text{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow$ Samp, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

$$\approx_c (\mathcal{U} + \mathbf{E}', \mathcal{U} - 2\mathbf{T})$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow \mathsf{Samp}$, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

$$\approx_c (\mathscr{U} + \mathbf{E}', \mathscr{U} - 2\mathbf{T})$$

$$\approx_s (\mathscr{U}, \mathscr{U}')$$

Analyzing the Pre-Condition

- $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = \mathbf{SP} - 2\mathbf{T}) \leftarrow \mathsf{Samp}$, where:
  - $\mathbf{S}, \mathbf{P}$ have **uniform $\mathbb{Z}_q$** entries, where q is **odd.**
  - $\mathbf{T} \leftarrow [0,1,\ldots,\lfloor q/2 \rfloor]$, (i.e. $2\mathbf{T} \approx$ random matrix with even entries mod q).

Goal: $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

$$(\mathbf{SP} + \mathbf{E}', \mathbf{SP} - 2\mathbf{T}) \approx_s (\mathbf{SP} + 2\mathbf{E}'' + \mathbf{E}', \mathbf{SP} + 2\mathbf{E}'' - 2\mathbf{T})$$

$$\approx_c (\mathscr{U} + \mathbf{E}', \mathscr{U} - 2\mathbf{T})$$

$$\approx_s (\mathscr{U}, \mathscr{U}')$$

$2\mathbf{T} + \mathbf{E}' \approx_s \mathscr{U}$

Concurrent attacks

Concurrent attacks

- [Hsieh-Jain-Lin/Agrawal-Modi-Yadav-Yamada 25]

Concurrent attacks

- [Hsieh-Jain-Lin/Agrawal-Modi-Yadav-Yamada 25]
    - Shows the exact version of evasive LWE used in the works of [Agrawal-Kumari-Yadav24] and [BDJ+25] are insecure.

Concurrent attacks

- [Hsieh-Jain-Lin/Agrawal-Modi-Yadav-Yamada 25]
  - Shows the exact version of evasive LWE used in the works of [Agrawal-Kumari-Yadav24] and [BDJ+25] are insecure.
- [AMYY25]

Concurrent attacks

- [Hsieh-Jain-Lin/Agrawal-Modi-Yadav-Yamada 25]
  - Shows the exact version of evasive LWE used in the works of [Agrawal-Kumari-Yadav24] and [BDJ+25] are insecure.
- [AMYY25]
  - Also shows a counterexample to the circular private-coin evasive LWE (used in [Hsieh-Lin-Luo 22])

Concurrent attacks

- [Hsieh-Jain-Lin/Agrawal-Modi-Yadav-Yamada 25]
  - Shows the exact version of evasive LWE used in the works of [Agrawal-Kumari-Yadav24] and [BDJ+25] are insecure.
- [AMYY25]
  - Also shows a counterexample to the circular private-coin evasive LWE (used in [Hsieh-Lin-Luo 22])
- Our work: Simple attack on evasive LWE itself

Concurrent attacks

- [Hsieh-Jain-Lin/Agrawal-Modi-Yadav-Yamada 25]
  - Shows the exact version of evasive LWE used in the works of [Agrawal-Kumari-Yadav24] and [BDJ+25] are insecure.
- [AMYY25]
  - Also shows a counterexample to the circular private-coin evasive LWE (used in [Hsieh-Lin-Luo 22])
- Our work: Simple attack on evasive LWE itself
- All zeroizing attacks!

Reflections

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.
  - See [VWW22] and Hoeteck's talk from Simons for specific versions.

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.
    - See [VWW22] and Hoeteck's talk from Simons for specific versions.
- **One view:** Evasive LWE as a lens to LWE-based security.

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.
  - See [VWW22] and Hoeteck's talk from Simons for specific versions.
- **One view:** Evasive LWE as a lens to LWE-based security.
  - Never meant to be an end goal, meant to be a *stepping stone*.

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.
    - See [VWW22] and Hoeteck's talk from Simons for specific versions.
- **One view:** Evasive LWE as a lens to LWE-based security.
    - Never meant to be an end goal, meant to be a *stepping stone*.
        - E.g. Rate-1 laconic function evaluation: first constructed from evasive LWE/ ℓ-succinct LWE [Wee24]; later shown from standard LWE [AMR25]

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.
  - See [VWW22] and Hoeteck's talk from Simons for specific versions.
- **One view:** Evasive LWE as a lens to LWE-based security.
  - Never meant to be an end goal, meant to be a *stepping stone*.
    - E.g. Rate-1 laconic function evaluation: first constructed from evasive LWE/ ℓ-succinct LWE [Wee24]; later shown from standard LWE [AMR25]
    - E.g. Almost all implications from **public coin evasive LWE** have now been shown from **falsifiable lattice assumptions** (ℓ-succinct LWE) [Personal communication with Hoeteck]

Reflections

- **Aftermath:** Private-coin evasive LWE in its full generality is broken, but many constructions are **still unbroken**.
    - See [VWW22] and Hoeteck's talk from Simons for specific versions.
- **One view:** Evasive LWE as a lens to LWE-based security.
    - Never meant to be an end goal, meant to be a *stepping stone*.
        - E.g. Rate-1 laconic function evaluation: first constructed from evasive LWE/ ℓ-succinct LWE [Wee24]; later shown from standard LWE [AMR25]
        - E.g. Almost all implications from **public coin evasive LWE** have now been shown from **falsifiable lattice assumptions** (ℓ-succinct LWE) [Personal communication with Hoeteck]
- **Open:** Can we achieve a similar story in the private-coin setting?

Thank you for your attention!

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

Return to
main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a “contrived” obfuscation-based attack.

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a "contrived" obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a "contrived" obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp},$
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a “contrived” obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M_1}, \mathbf{M_2}$ such that $\mathbf{W} \approx \mathbf{M_1 M_2}$.

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a “contrived” obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M_1}, \mathbf{M_2}$ such that $\mathbf{W} \approx \mathbf{M_1 M_2}$.

By LWE, $\mathbf{W} \approx_c \mathscr{U}$ in pre-condition, so $O_{\mathbf{W}} = \mathbf{Zero}$.

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a "contrived" obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M_1}, \mathbf{M_2}$ such that $\mathbf{W} \approx \mathbf{M_1}\mathbf{M_2}$.

By LWE, $\mathbf{W} \approx_c \mathscr{U}$ in pre-condition, so $O_{\mathbf{W}} = \mathbf{Zero}$.

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a "contrived" obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \text{aux} = O_{\mathbf{W}} \leftarrow \text{Samp},$
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M}_1, \mathbf{M}_2$ such that $\mathbf{W} \approx \mathbf{M}_1\mathbf{M}_2$.

By LWE, $\mathbf{W} \approx_c \mathcal{U}$ in pre-condition, so $O_{\mathbf{W}} = \mathbf{Zero}$.

Pre ✓ $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \text{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathcal{U}, \mathcal{U}, \text{aux})$

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a “contrived” obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M_1}, \mathbf{M_2}$ such that $\mathbf{W} \approx \mathbf{M_1 M_2}$.

By LWE, $\mathbf{W} \approx_c \mathscr{U}$ in pre-condition, so $O_{\mathbf{W}} = \mathbf{Zero}$.

Pre ✓ $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

$$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a "contrived" obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M_1}, \mathbf{M_2}$ such that $\mathbf{W} \approx \mathbf{M_1 M_2}$.

By LWE, $\mathbf{W} \approx_c \mathscr{U}$ in pre-condition, so $O_{\mathbf{W}} = \mathbf{Zero}$.

Pre ✓ $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$$

Post ✗ $$(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$$

Return to main body

Heuristic Obfuscation-based Attack

[VWW22, BUW24, HHY25]

- Private-coin evasive LWE has a "contrived" obfuscation-based attack.
- $\mathbf{S}, \mathbf{P}, \mathsf{aux} = O_{\mathbf{W}} \leftarrow \mathsf{Samp}$,
  - $\mathbf{S}, \mathbf{P}$ are sampled uniformly,
  - $\mathbf{W} = \mathbf{SP} + \widetilde{\mathbf{E}}$ and O_W accepts low-rank $\mathbf{M_1}, \mathbf{M_2}$ such that $\mathbf{W} \approx \mathbf{M_1 M_2}$.

By LWE, $\mathbf{W} \approx_c \mathscr{U}$ in pre-condition, so $O_{\mathbf{W}} = \mathbf{Zero}$.

Pre ✓ $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathscr{U}, \mathsf{aux})$

Post ✗ $(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux}) \approx_c (\mathbf{B}, \mathbf{P}, \mathscr{U}, \mathbf{B}^{-1}(\mathbf{P}), \mathsf{aux})$

Clearly broken in post-condition!

Return to main body