Constant Input Attribute Based (and Predicate) Encryption from Evasive and Tensor LWE

Shweta Agrawal (IIT Madras)

Mélissa Rossi (ANSSI Paris)

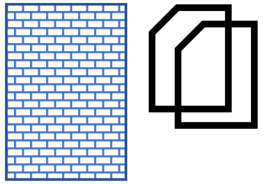
Anshu Yadav (IIT Madras)

Shota Yamada (AIST Tokyo)

Example

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma

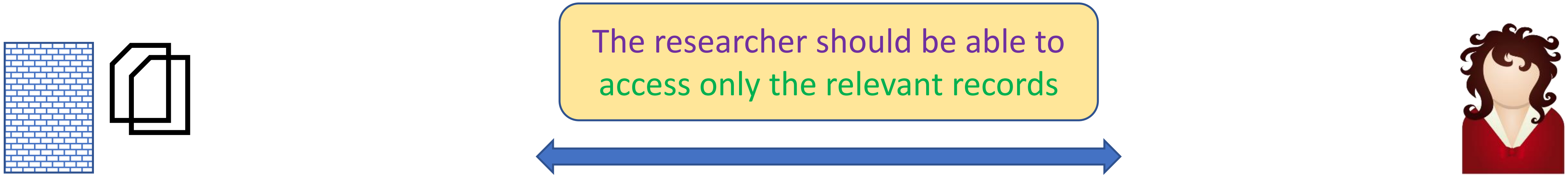
Example



The researcher should be able to access only the relevant records

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma

Example

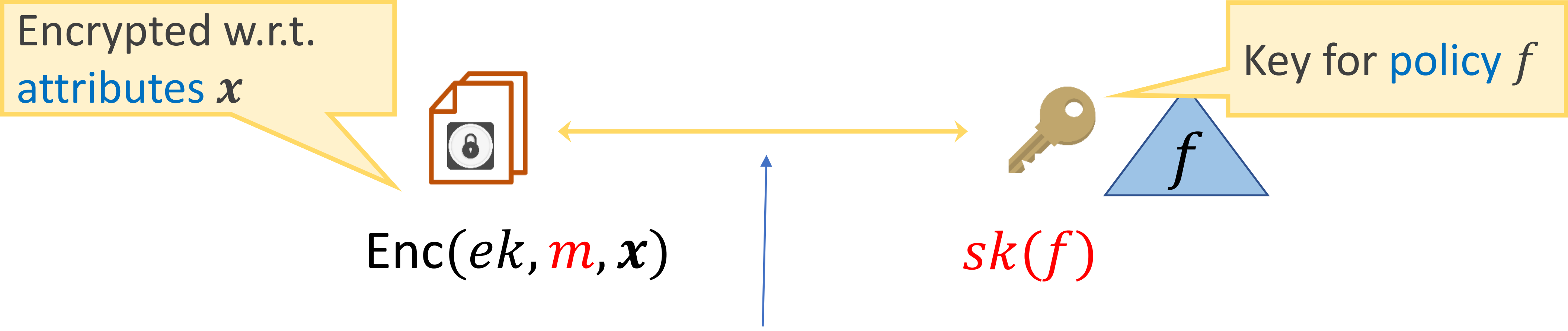


The researcher should be able to access only the relevant records

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma

Attribute Based Encryption ABE

Attribute Based Encryption (ABE)



Encrypted w.r.t. attributes $\boldsymbol{x}$

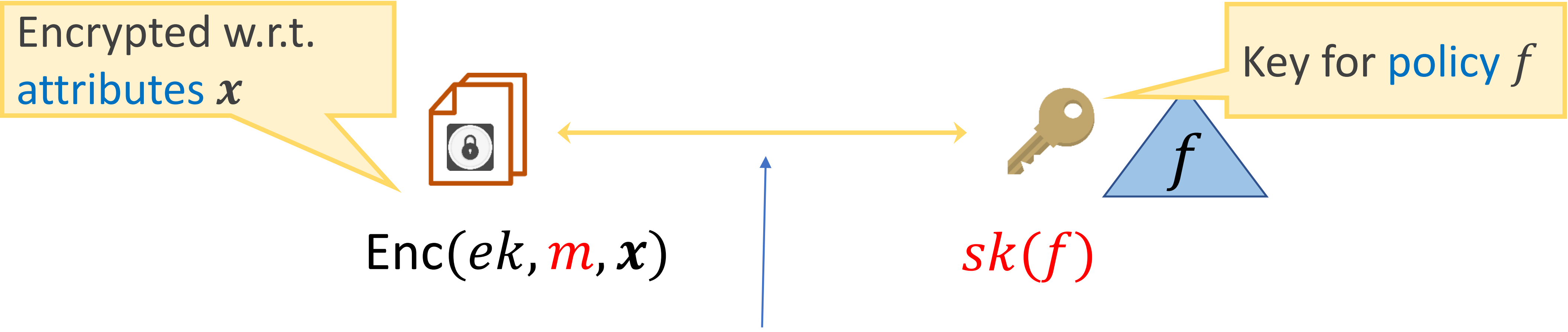
Key for policy f

$\text{Enc}(ek, m, \boldsymbol{x})$

$sk(f)$

$$\boxed{\text{Dec}\big(sk(f), CT(m, \boldsymbol{x})\big) = m \;\Leftrightarrow\; f(\boldsymbol{x}) = 1}$$

Predicate Encryption (PE)



Encrypted w.r.t. attributes $\boldsymbol{x}$

Key for policy f

$\text{Enc}(ek, m, \boldsymbol{x})$

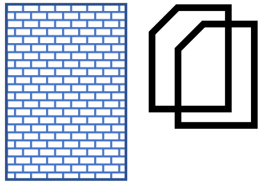
$sk(f)$

$$\text{Dec}\big(sk(f), CT(m, \boldsymbol{x})\big) = m \iff f(\boldsymbol{x}) = 1$$

Predicate Encryption: Ciphertext hides attributes as well

Example

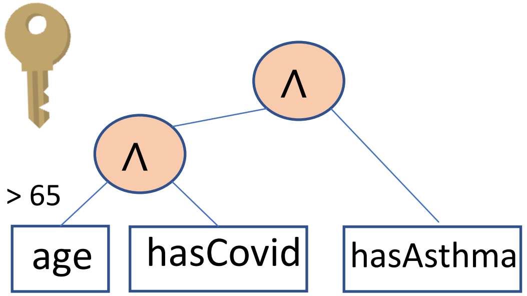
ABE-Enc(🗐, (age, hasCovid, has Asthma))



The researcher should be able to access only the relevant records

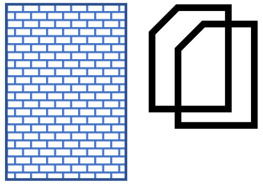
Attribute Based Encryption
ABE

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma



Example

ABE-Enc(🗐, (age, hasCovid, has Asthma))



The researcher should be able to access only the relevant records

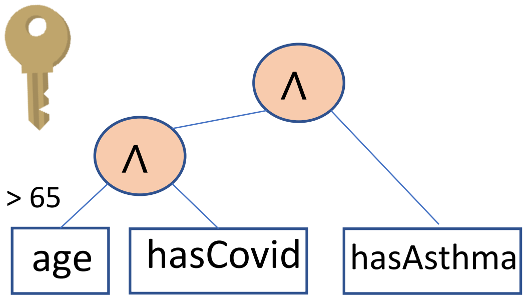
Att

Enc

ABE

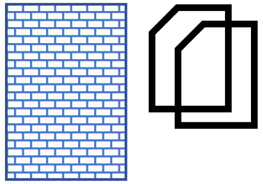
⚠ Records of a single patient is generally distributed across different departments or hospitals

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma

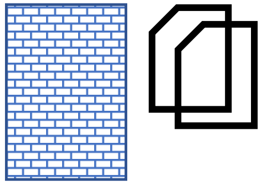


Example

ABE-Enc(🗐, (age, hasCovid, has Asthma))



Covid center



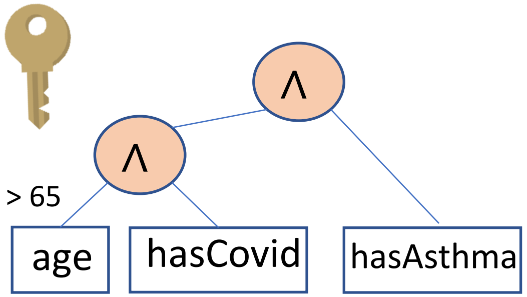
Pulmonary Department

The researcher should be able to access only the relevant records

Att
Enc
ABE

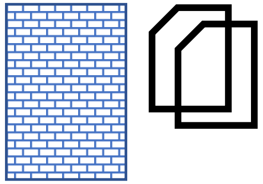
⚠ Records of a single patient is generally distributed across different departments or hospitals

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma

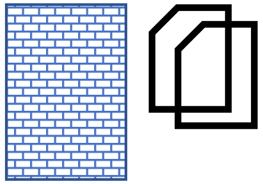


Example

ABE-Enc(🗐, (age, hasCovid, has Asthma))



Covid center



Pulmonary Department

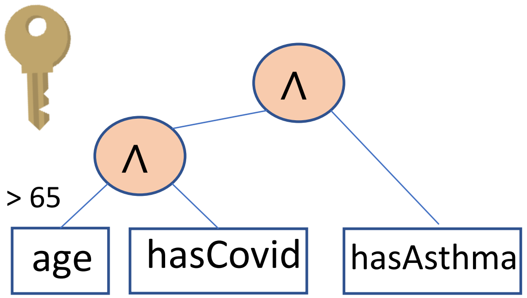
We need ABE/PE in distributed setup

The researcher should be able to access only the relevant records

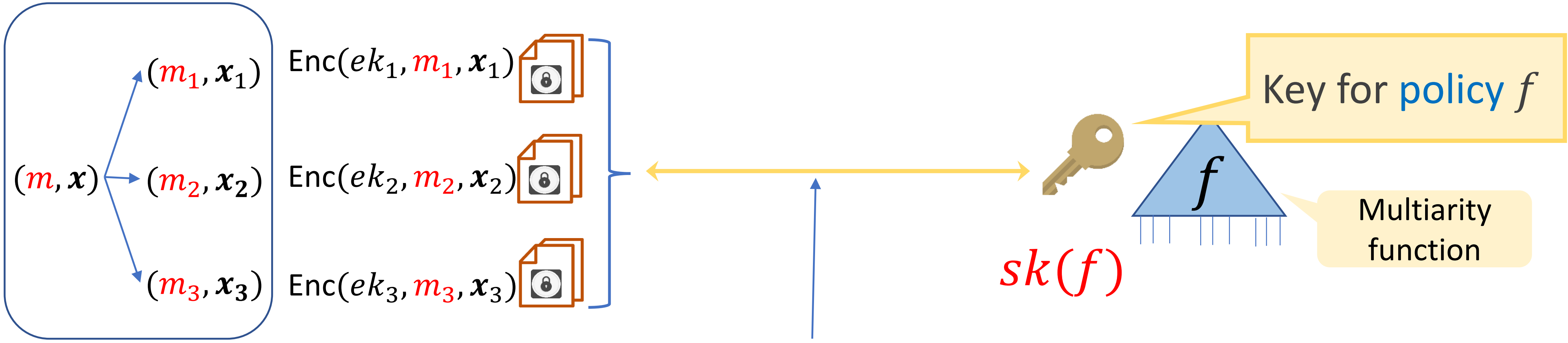
Att
Enc
ABE

⚠ Records of a single patient is generally distributed across different departments or hospitals

Wants to study the effectiveness of certain medicine on covid patients above 65 years with asthma



Multi-Input Attribute Based Encryption (miABE)



$(m, \boldsymbol{x})$

$(m_1, \boldsymbol{x}_1)$

$(m_2, \boldsymbol{x}_2)$

$(m_3, \boldsymbol{x}_3)$

Enc$(ek_1, m_1, \boldsymbol{x}_1)$

Enc$(ek_2, m_2, \boldsymbol{x}_2)$

Enc$(ek_3, m_3, \boldsymbol{x}_3)$

Key for policy f

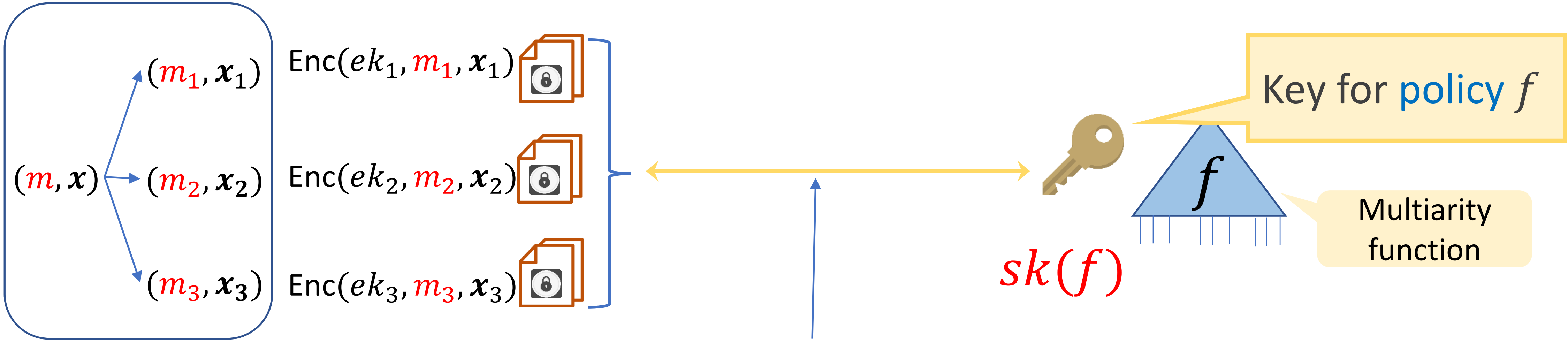
f

$sk(f)$

Multiarity function

$$\text{Dec}\big(sk(f), \text{Enc}(m_1, \boldsymbol{x}_1), \text{Enc}(m_2, \boldsymbol{x}_2), \text{Enc}(m_3, \boldsymbol{x}_3)\big) = (m_1, m_2, m_3) \;\Leftrightarrow\; f(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3) = 1$$

Multi-Input Attribute Based Encryption (miABE)


$(m, \boldsymbol{x})$
$(m_1, \boldsymbol{x}_1)$
$(m_2, \boldsymbol{x}_2)$
$(m_3, \boldsymbol{x}_3)$
$\mathrm{Enc}(ek_1, m_1, \boldsymbol{x}_1)$
$\mathrm{Enc}(ek_2, m_2, \boldsymbol{x}_2)$
$\mathrm{Enc}(ek_3, m_3, \boldsymbol{x}_3)$
Key for policy f
f
$sk(f)$
Multiarity function

$$\mathrm{Dec}\Big(sk(f), \underbrace{\mathrm{Enc}(m_1, \boldsymbol{x}_1), \mathrm{Enc}(m_2, \boldsymbol{x}_2), \mathrm{Enc}(m_3, \boldsymbol{x}_3)}_{\mathrm{Enc}(m, \boldsymbol{x})}\Big) = (\underbrace{m_1, m_2, m_3}_{m}) \Leftrightarrow f(\underbrace{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3}_{\boldsymbol{x}}) = 1$$

Related Work

Reference	Function Class	Arity	Assumption
[AYY22]	NC1	2	LWE+pairings
[AYY22]	P	2	Heuristic

Related Work

Reference	Function Class	Arity	Assumption
[AYY22]	NC1	2	LWE+pairings
[AYY22]	P	2	Heuristic
[ATY23]	Conjunctions in NC1	Poly	MDDH

Related Work

Reference	Function Class	Arity	Assumption
[AYY22]	NC1	2	LWE+pairings
[AYY22]	P	2	Heuristic
[ATY23]	Conjunctions in NC1	Poly	MDDH
Ours	NC1	Constant	Evasive LWE

Related Work

Reference	Function Class	Arity	Assumption
[AYY22]	NC1	2	LWE+pairings
[AYY22]	P	2	Heuristic
[ATY23]	Conjunctions in NC1	Poly	MDDH
Ours	NC1	Constant	Evasive LWE
Ours	P	Constant	Evasive+Gen. Tensor LWE
Ours	P	2	Evasive + Tensor LWE

Related Work

Reference	Function Class	Arity	Assumption
[AYY22]	NC1	2	LWE+pairings
[AYY22]	P	2	Heuristic
[ATY23]	Conjunctions in NC1	Poly	MDDH
Ours	NC1	Constant	Evasive LWE
Ours	P	Constant	Evasive+Gen. Tensor LWE
Ours	P	2	Evasive + Tensor LWE

Collusion Resistant

Related Work

Reference	Function Class	Arity	Assumption
[AYY22]	NC1	2	LWE+pairings
[AYY22]	P	2	Heuristic
[ATY23]	Conjunctions in NC1	Poly	MDDH
Ours	NC1	Constant	Evasive LWE
Ours	P	Constant	Evasive+Gen. Tensor LWE
Ours	P	2	Evasive + Tensor LWE

Collusion Resistant

[FFMV23] supports conjunctions without collusion resistance from LWE

Our Results

miABE for constant arity

Arity	**Function Class**	**Assumption**
Constant	NC1	evasive LWE
2	P	Evasive and tensor LWE
Constant	P	Evasive and Generalized tensor LWE

Our Results

miABE for constant arity

Arity	Function Class	Assumption
Constant	NC1	evasive LWE
2	P	Evasive and tensor LWE
Constant	P	Evasive and Generalized tensor LWE

By using [AYY22] compiler, we get Multi Input Predicate Encryption for same settings

Our Results

miABE for constant arity

Arity	**Function Class**	**Assumption**
Constant	NC1	evasive LWE
2	P	Evasive and tensor LWE
Constant	P	Evasive and Generalized tensor LWE

By using [AYY22] compiler, we get Multi Input Predicate Encryption for same settings

Studying tensor LWE: We show that tensor LWE can be reduced to standard LWE in a special case

Fundamental Challenge in Constructing miABE

Two opposite requirements

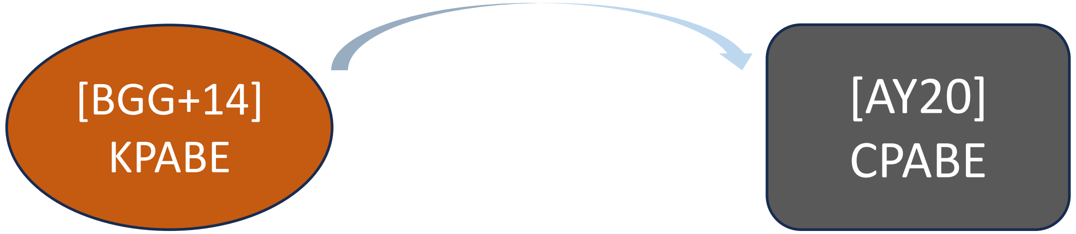
Multiple encryptors generate the ciphertext components independently

The ciphertext components are independent

Independently generated components must be joined in a meaningful way

Need correlated ciphertext components for decryption

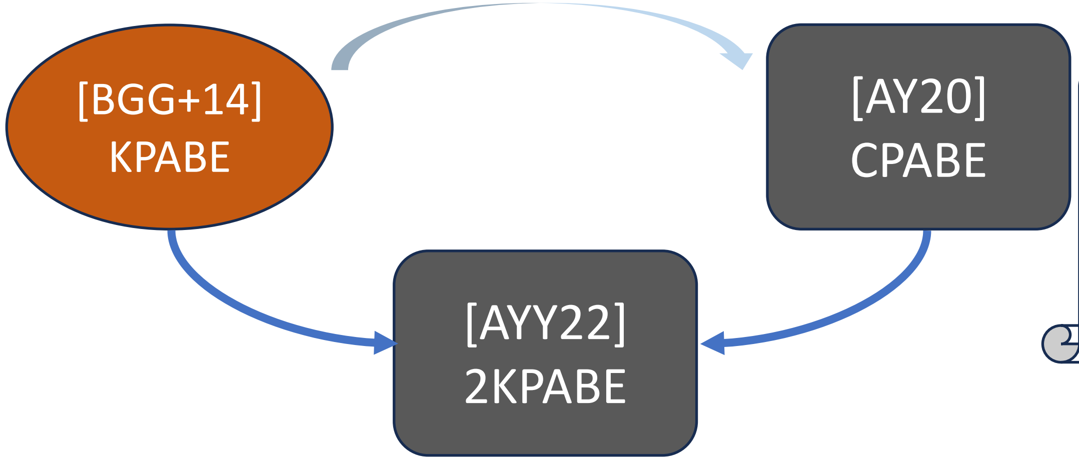
Pathway


[BGG+14]
KPABE

[AY20]
CPABE

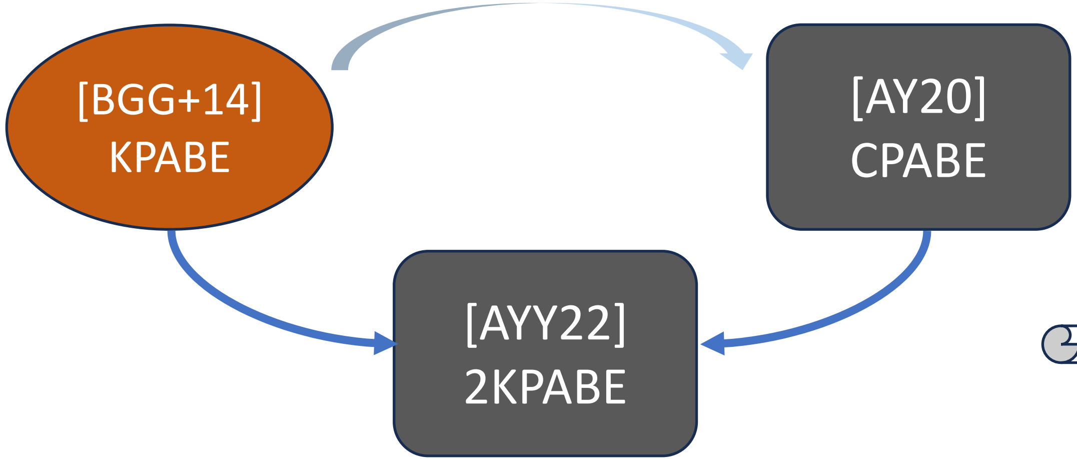
Uses pairings to hide BGG+ components in the exponent

Pathway



Uses pairings to hide BGG+ components in the exponent

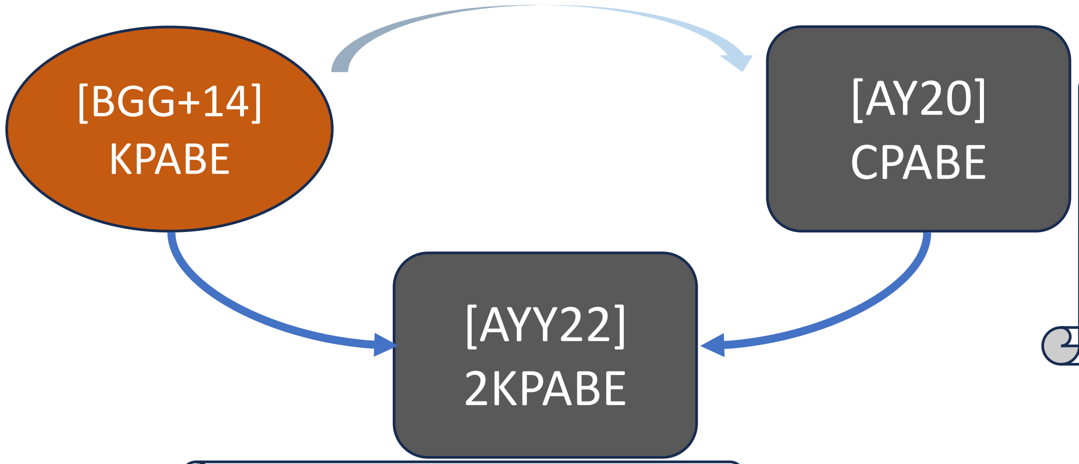
Pathway



Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

Pathway

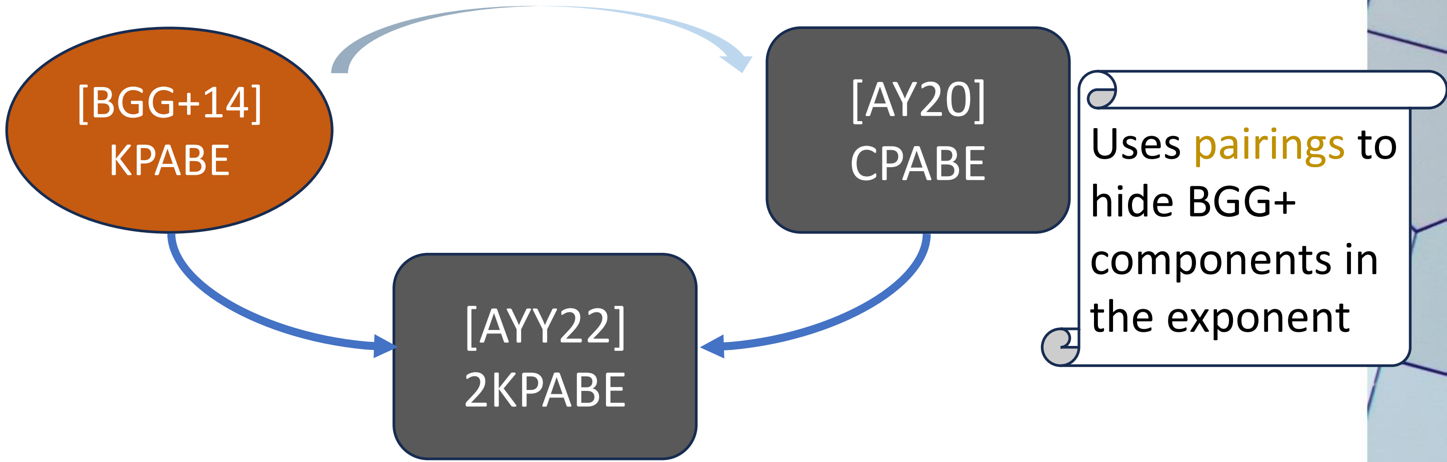


Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$

Pathway

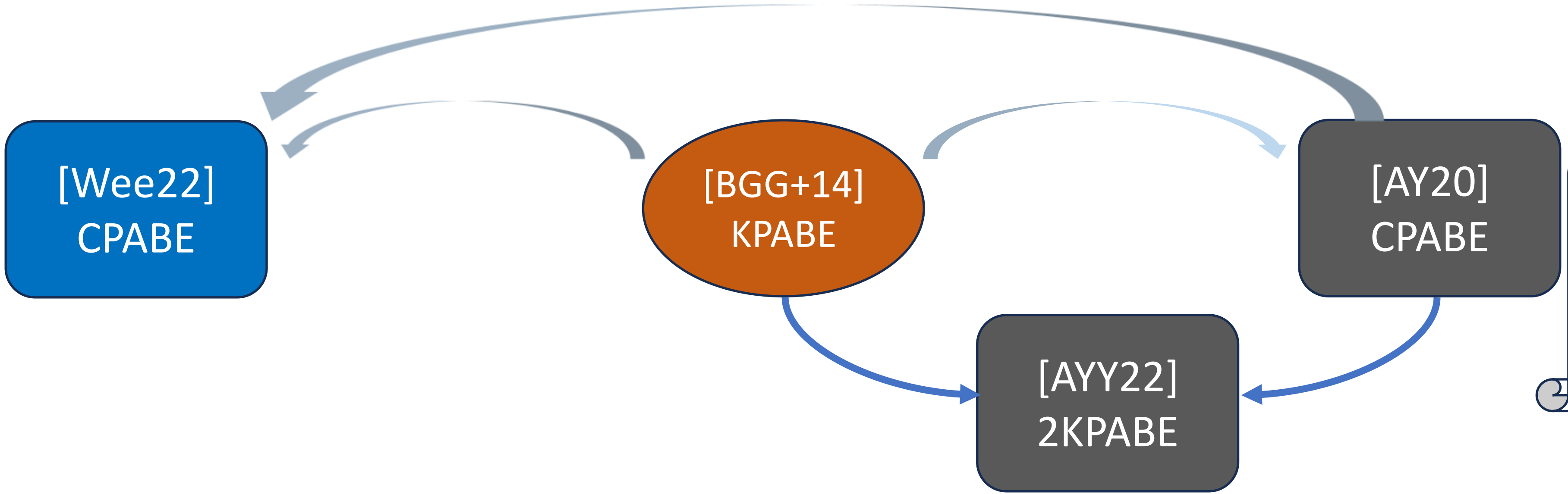


Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$
Decryptor	$[r_1r_2\psi_{\boldsymbol{x}}]_T$	$[r_1r_2\psi_{\boldsymbol{y}}]_T$

Pathway

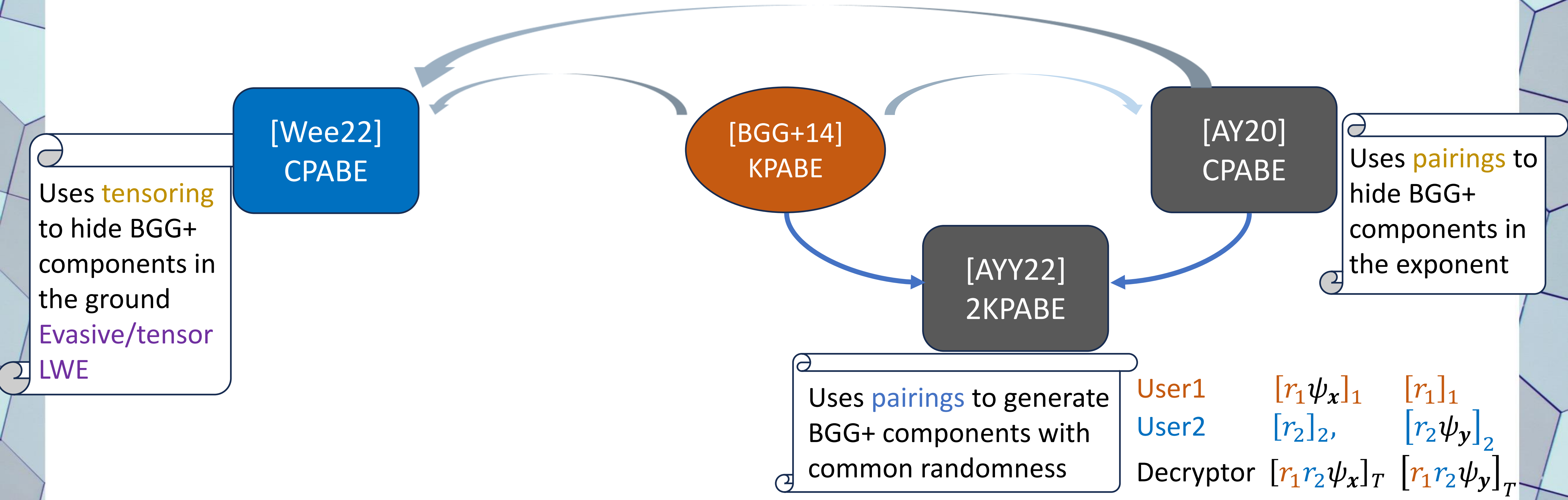


Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$
Decryptor	$[r_1r_2\psi_{\boldsymbol{x}}]_T$	$[r_1r_2\psi_{\boldsymbol{y}}]_T$

Pathway



[Wee22]
CPABE

[BGG+14]
KPABE

[AY20]
CPABE

[AYY22]
2KPABE

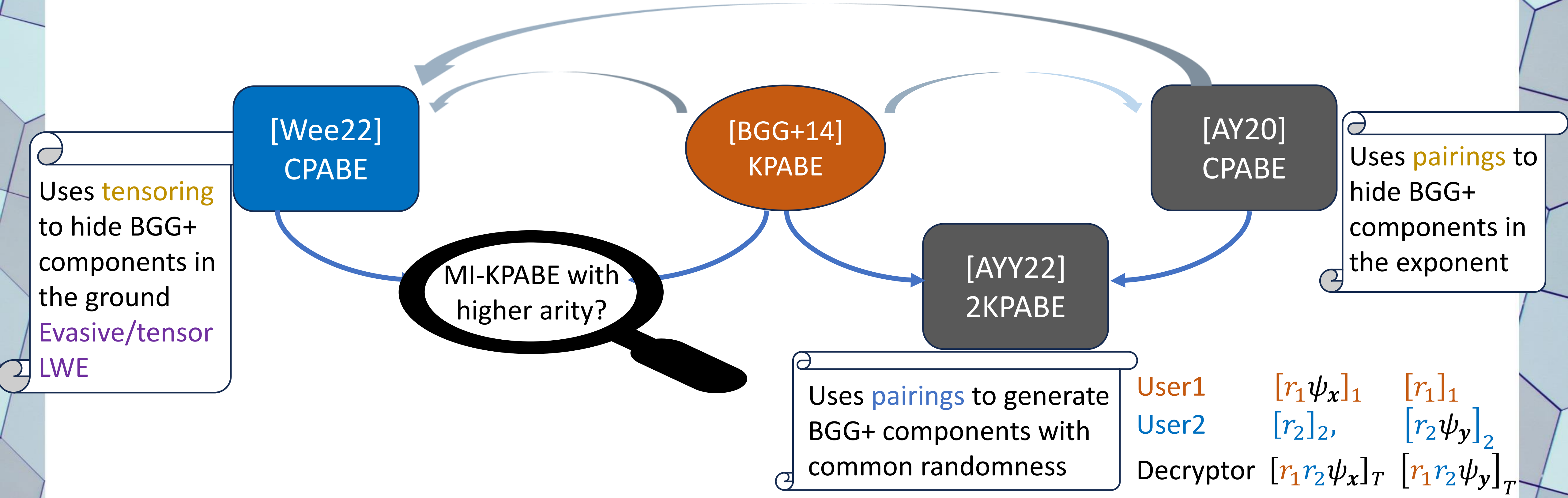
Uses tensoring to hide BGG+ components in the ground
Evasive/tensor LWE

Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$
Decryptor	$[r_1r_2\psi_{\boldsymbol{x}}]_T$	$[r_1r_2\psi_{\boldsymbol{y}}]_T$

Pathway



[Wee22]
CPABE

[BGG+14]
KPABE

[AY20]
CPABE

[AYY22]
2KPABE

MI-KPABE with higher arity?

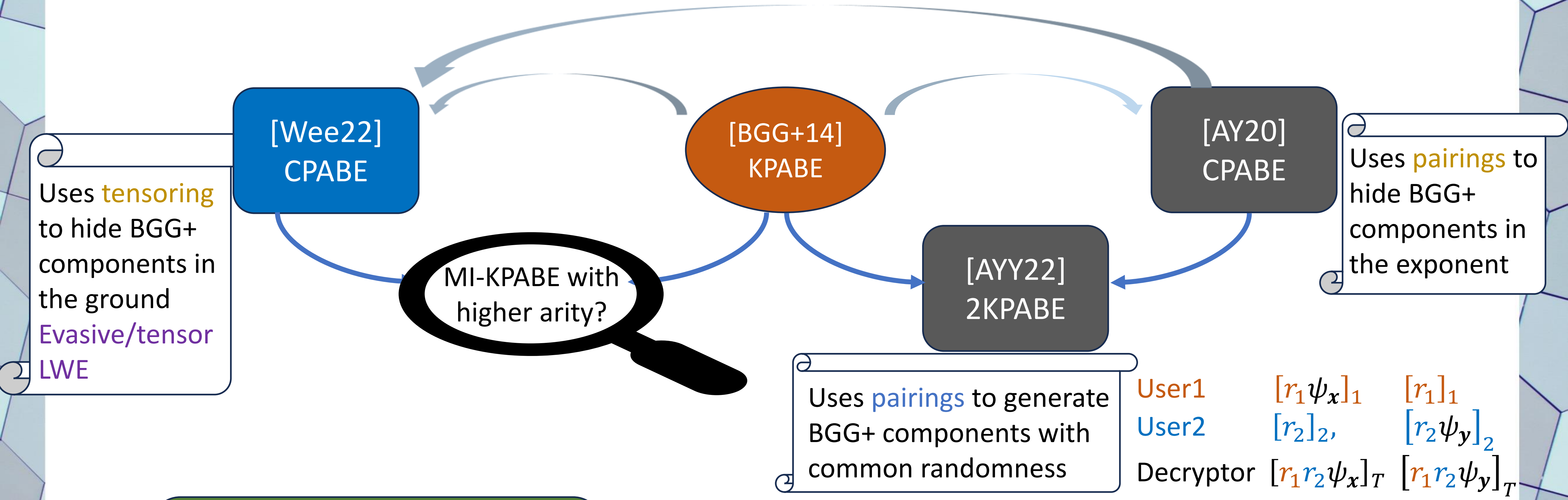
Uses tensoring to hide BGG+ components in the ground
Evasive/tensor LWE

Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$
Decryptor	$[r_1r_2\psi_{\boldsymbol{x}}]_T$	$[r_1r_2\psi_{\boldsymbol{y}}]_T$

Pathway



[Wee22] CPABE

[BGG+14] KPABE

[AY20] CPABE

[AYY22] 2KPABE

MI-KPABE with higher arity?

Uses tensoring to hide BGG+ components in the ground Evasive/tensor LWE

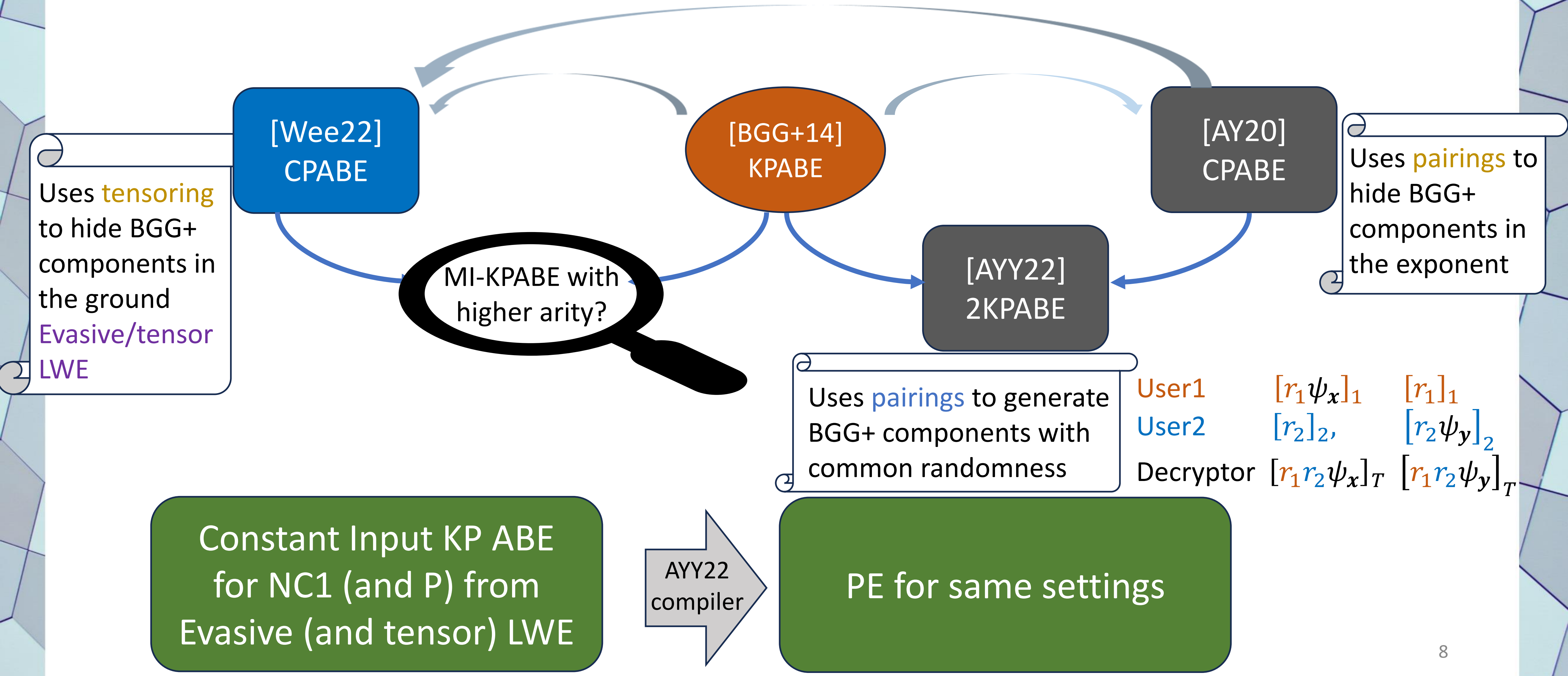
Uses pairings to hide BGG+ components in the exponent

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$
Decryptor	$[r_1r_2\psi_{\boldsymbol{x}}]_T$	$[r_1r_2\psi_{\boldsymbol{y}}]_T$

Constant Input KP ABE for NC1 (and P) from Evasive (and tensor) LWE

Pathway



[Wee22]
CPABE

Uses tensoring to hide BGG+ components in the ground
Evasive/tensor LWE

[BGG+14]
KPABE

[AY20]
CPABE

Uses pairings to hide BGG+ components in the exponent

MI-KPABE with higher arity?

[AYY22]
2KPABE

Uses pairings to generate BGG+ components with common randomness

User1	$[r_1\psi_{\boldsymbol{x}}]_1$	$[r_1]_1$
User2	$[r_2]_2,$	$[r_2\psi_{\boldsymbol{y}}]_2$
Decryptor	$[r_1r_2\psi_{\boldsymbol{x}}]_T$	$[r_1r_2\psi_{\boldsymbol{y}}]_T$

Constant Input KP ABE for NC1 (and P) from Evasive (and tensor) LWE

AYY22 compiler

PE for same settings

Tensor Product

Tensoring

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad \boldsymbol{B} \qquad \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} \end{pmatrix}$$

Tensor Product

Tensoring

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \qquad \boldsymbol{B} \qquad\qquad \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} \end{pmatrix}$$

$$(\boldsymbol{A} \otimes \boldsymbol{B})(\boldsymbol{C} \otimes \boldsymbol{D}) = \boldsymbol{AC} \otimes \boldsymbol{BD}$$

Tensor Product

Tensoring

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \qquad \boldsymbol{B} \qquad\qquad \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} \end{pmatrix}$$

$$(\boldsymbol{A} \otimes \boldsymbol{B})(\boldsymbol{C} \otimes \boldsymbol{D}) = \boldsymbol{AC} \otimes \boldsymbol{BD}$$

$$\Downarrow$$

$$(\boldsymbol{A} \otimes \boldsymbol{I})(\boldsymbol{I} \otimes \boldsymbol{r}^T) = \boldsymbol{A} \otimes \boldsymbol{r}^T$$

$$(\boldsymbol{A} \otimes \boldsymbol{r}^T)\boldsymbol{B} = \boldsymbol{AB} \otimes \boldsymbol{r}^T$$

BGG+14 KPABE Overview

Given $\boldsymbol{A}, \boldsymbol{x}, f$ $\exists$ efficiently computable short matrix $\boldsymbol{H}$ such that

$$(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})\boldsymbol{H} = \boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}$$

BGG+14 KPABE Overview

Given $\boldsymbol{A}, \boldsymbol{x}, f$ $\exists$ efficiently computable short matrix $\boldsymbol{H}$ such that

$$(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})\boldsymbol{H} = \boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}$$

Fresh secret

Part of mpk

Encryption$(\boldsymbol{x},\ \text{msg})$ $\underline{\boldsymbol{s}(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})}$ + other terms to embed msg

BGG+14 KPABE Overview

Given $\boldsymbol{A}, \boldsymbol{x}, f$ ∃ efficiently computable short matrix $\boldsymbol{H}$ such that

$$(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})\boldsymbol{H} = \boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}$$

Fresh secret

Part of mpk

Encryption$(\boldsymbol{x},$ msg$)$ $\underline{\boldsymbol{s}(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})}$ + other terms to embed msg

Right multiplication with $\boldsymbol{H}$ gives $\underline{\boldsymbol{s}\boldsymbol{A}_f}$ if $f(\boldsymbol{x}) = 0$

BGG+14 KPABE Overview

Given $\boldsymbol{A}, \boldsymbol{x}, f$ $\exists$ efficiently computable short matrix $\boldsymbol{H}$ such that

$$(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})\boldsymbol{H} = \boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}$$

Fresh secret

Part of mpk

Encryption$(\boldsymbol{x},\ \text{msg})$ $\underline{\boldsymbol{s}(\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G})}$ + other terms to embed msg

Right multiplication with $\boldsymbol{H}$ gives $\underline{\boldsymbol{s}\boldsymbol{A}_f}$ if $f(\boldsymbol{x}) = 0$

KeyGen(f) A short preimage of a public vector $\boldsymbol{u}$ wrt $\boldsymbol{A}_f$ to enable recovering the masking term $\underline{\boldsymbol{s}\boldsymbol{A}_f}$ when $f(\boldsymbol{x}) = 0$

Evasive and Tensor LWE

Evasive LWE

$(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}) \approx (\boldsymbol{B}, random)$ LWE

Evasive and Tensor LWE

Evasive LWE

😈

$(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}) \approx (\boldsymbol{B}, random)$ LWE

Given $\boldsymbol{B}^{-1}(\boldsymbol{P})$, can compute

$$\boxed{(\boldsymbol{sB} + \boldsymbol{e})\boldsymbol{B}^{-1}(\boldsymbol{P}) = \boldsymbol{sP} + \boldsymbol{e}'}$$

Evasive and Tensor LWE

Evasive LWE

😈

$(\boldsymbol{B}, \boldsymbol{sB}+\boldsymbol{e}) \approx (\boldsymbol{B}, random)$ LWE

Given $\boldsymbol{B}^{-1}(\boldsymbol{P})$, can compute

$$\boxed{(\boldsymbol{sB}+\boldsymbol{e})\boldsymbol{B}^{-1}(\boldsymbol{P}) = \boldsymbol{sP}+\boldsymbol{e}'}$$

Evasive LWE assumes that this is the only way of using $\boldsymbol{B}^{-1}(\boldsymbol{P})$

Evasive and Tensor LWE

Evasive LWE

$(\boldsymbol{B}, \boldsymbol{sB}+\boldsymbol{e}) \approx (\boldsymbol{B}, random)$ LWE

Given $\boldsymbol{B}^{-1}(\boldsymbol{P})$, can compute

$$\boxed{(\boldsymbol{sB}+\boldsymbol{e})\boldsymbol{B}^{-1}(\boldsymbol{P}) = \boldsymbol{sP}+\boldsymbol{e}'}$$

Evasive LWE assumes that this is the only way of using $\boldsymbol{B}^{-1}(\boldsymbol{P})$

⇒

If $(\boldsymbol{B}, \boldsymbol{sB}+\boldsymbol{e}, \boldsymbol{sP}+\boldsymbol{e}') \approx (\boldsymbol{B}, rand, rand)$

Then $\left(\boldsymbol{B}, \boldsymbol{sB}+\boldsymbol{e}, \boldsymbol{B}^{-1}(\boldsymbol{P})\right) \approx (\boldsymbol{B}, rand, \boldsymbol{B}^{-1}(\boldsymbol{P}))$

Evasive and Tensor LWE

Evasive LWE

$(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}) \approx (\boldsymbol{B}, random)$ LWE

Given $\boldsymbol{B}^{-1}(\boldsymbol{P})$, can compute

$$\boxed{(\boldsymbol{sB} + \boldsymbol{e})\boldsymbol{B}^{-1}(\boldsymbol{P}) = \boldsymbol{sP} + \boldsymbol{e}'}$$

Evasive LWE assumes that this is the only way of using $\boldsymbol{B}^{-1}(\boldsymbol{P})$

⇒

If $(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}, \boldsymbol{sP} + \boldsymbol{e}') \approx (\boldsymbol{B}, rand, rand)$

Then $\big(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}, \boldsymbol{B}^{-1}(\boldsymbol{P})\big) \approx (\boldsymbol{B}, rand, \boldsymbol{B}^{-1}(\boldsymbol{P}))$

Tensor LWE

Correlated BGG+ samples tensored with different random vectors remain pseudorandom

Evasive and Tensor LWE

Evasive LWE

$(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}) \approx (\boldsymbol{B}, random)$ LWE

Given $\boldsymbol{B}^{-1}(\boldsymbol{P})$, can compute

$$(\boldsymbol{sB} + \boldsymbol{e})\boldsymbol{B}^{-1}(\boldsymbol{P}) = \boldsymbol{sP} + \boldsymbol{e}'$$

Evasive LWE assumes that this is the only way of using $\boldsymbol{B}^{-1}(\boldsymbol{P})$

If $(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}, \boldsymbol{sP} + \boldsymbol{e}') \approx (\boldsymbol{B}, rand, rand)$

Then $\left(\boldsymbol{B}, \boldsymbol{sB} + \boldsymbol{e}, \boldsymbol{B}^{-1}(\boldsymbol{P})\right) \approx (\boldsymbol{B}, rand, \boldsymbol{B}^{-1}(\boldsymbol{P}))$

Tensor LWE

Correlated BGG+ samples tensored with different random vectors remain pseudorandom

$$\boldsymbol{A}, \boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_1^T)(\boldsymbol{A} - \boldsymbol{x}_1 \otimes \boldsymbol{G}) + noise, \boldsymbol{r}_1, \cdots, \boldsymbol{s}\left(\boldsymbol{I} \otimes \boldsymbol{r}_Q^T\right)\left(\boldsymbol{A} - \boldsymbol{x}_Q \otimes \boldsymbol{G}\right) + noise, \boldsymbol{r}_Q$$

$$\approx_c \quad \boldsymbol{A}, random, \boldsymbol{r}_1, \cdots, random, \boldsymbol{r}_Q$$

Construction Warm-Up

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

$\boldsymbol{x}_1$

$\boldsymbol{x}_2$

Construction Warm-Up

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

↓

BGG+ ciphertext

$$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$$

$\boldsymbol{x}_1$

$\boldsymbol{x}_2$

Construction Warm-Up

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

↓

BGG+ ciphertext

$$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$$

$\boldsymbol{x}_1$

$$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$$

$\boldsymbol{x}_2$

$$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$$

Construction Warm-Up

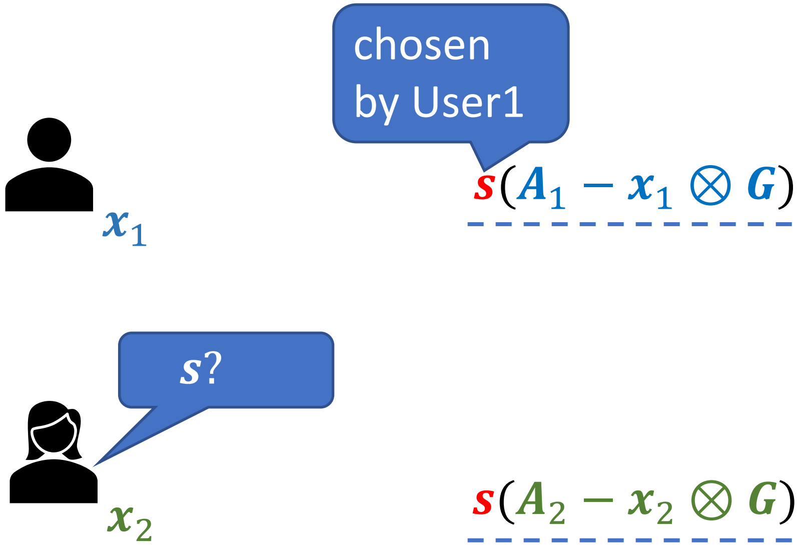
Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

↓

BGG+ ciphertext

$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$



chosen by User1

$\boldsymbol{x}_1$

$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$

$\boldsymbol{s}$?

$\boldsymbol{x}_2$

$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

Construction Warm-Up

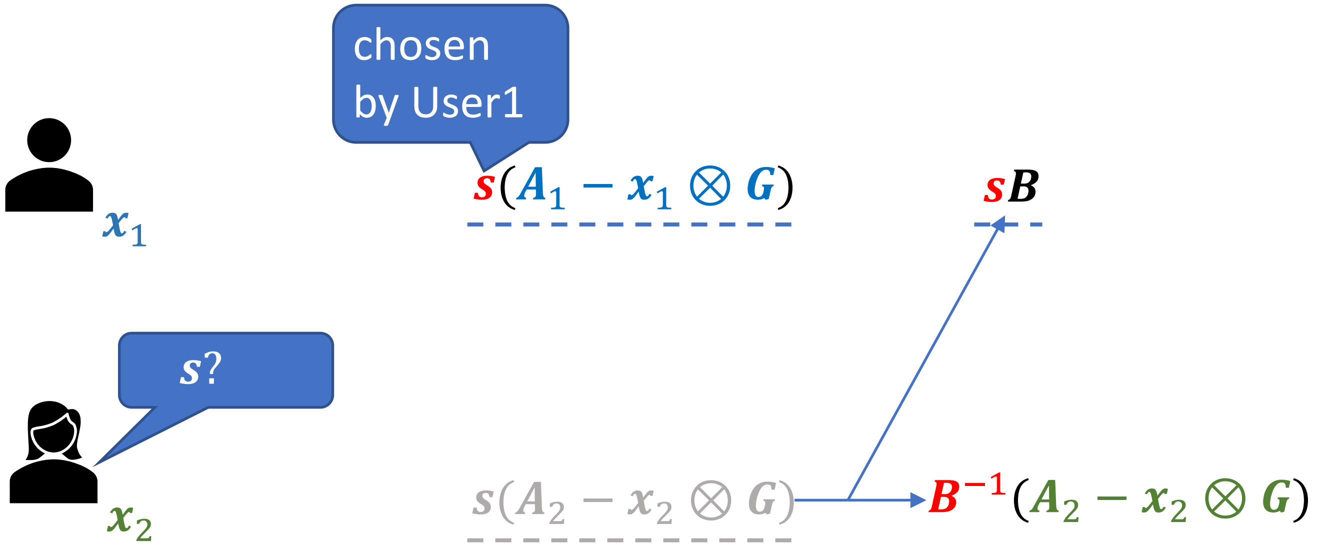
Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

$$\Downarrow$$

BGG+ ciphertext

$$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$$



chosen by User1

$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$

$\boldsymbol{s}\boldsymbol{B}$

$\boldsymbol{x}_1$

$\boldsymbol{s}?$

$\boldsymbol{x}_2$

$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \rightarrow \boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

Construction Warm-Up

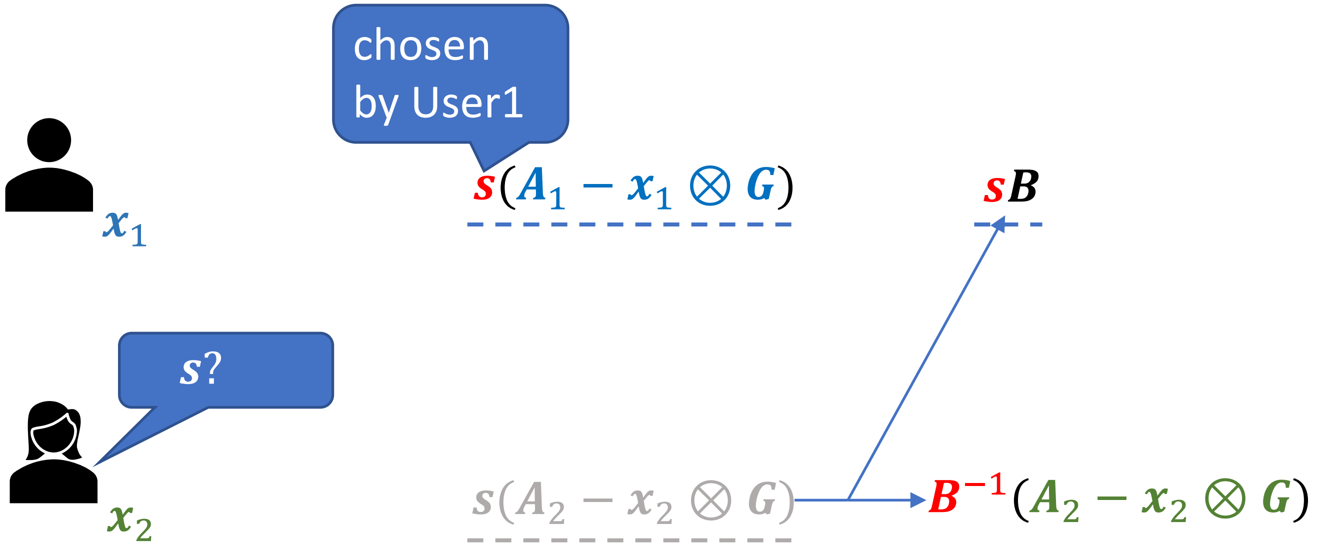
Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1|\boldsymbol{x}_2)$

↓

BGG+ ciphertext

$\boldsymbol{s}((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})$



chosen by User1
$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$
$\boldsymbol{sB}$
$\boldsymbol{x}_1$
$\boldsymbol{s}?$
$\boldsymbol{x}_2$
$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$
$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

KeyGen(f)

Same as BGG+ key: $\boldsymbol{A}_f^{-1}(\boldsymbol{Gu}^T)$

Construction Warm-Up

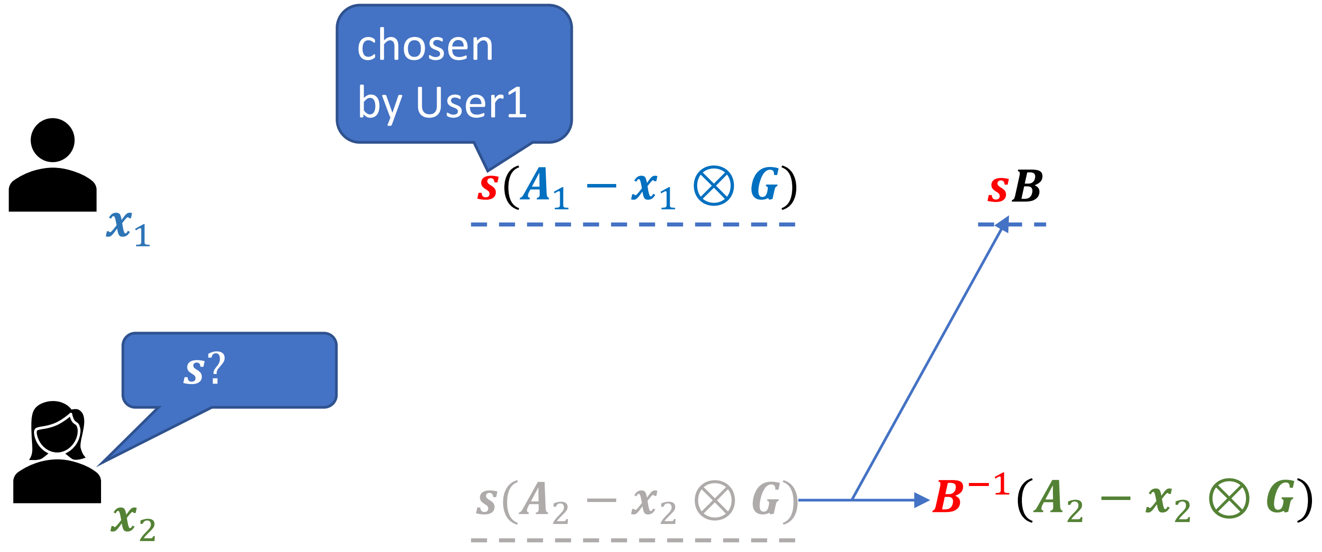
Encryption

$x = (x_1|x_2)$

↓

BGG+ ciphertext

$s((A_1|A_2) - (x_1|x_2) \otimes G)$



chosen by User1

$s(A_1 - x_1 \otimes G)$

sB

x_1

$s?$

x_2

$s(A_2 - x_2 \otimes G)$

$B^{-1}(A_2 - x_2 \otimes G)$

KeyGen(f)

Same as BGG+ key: $A_f^{-1}(Gu^T)$

Construction Warm-Up

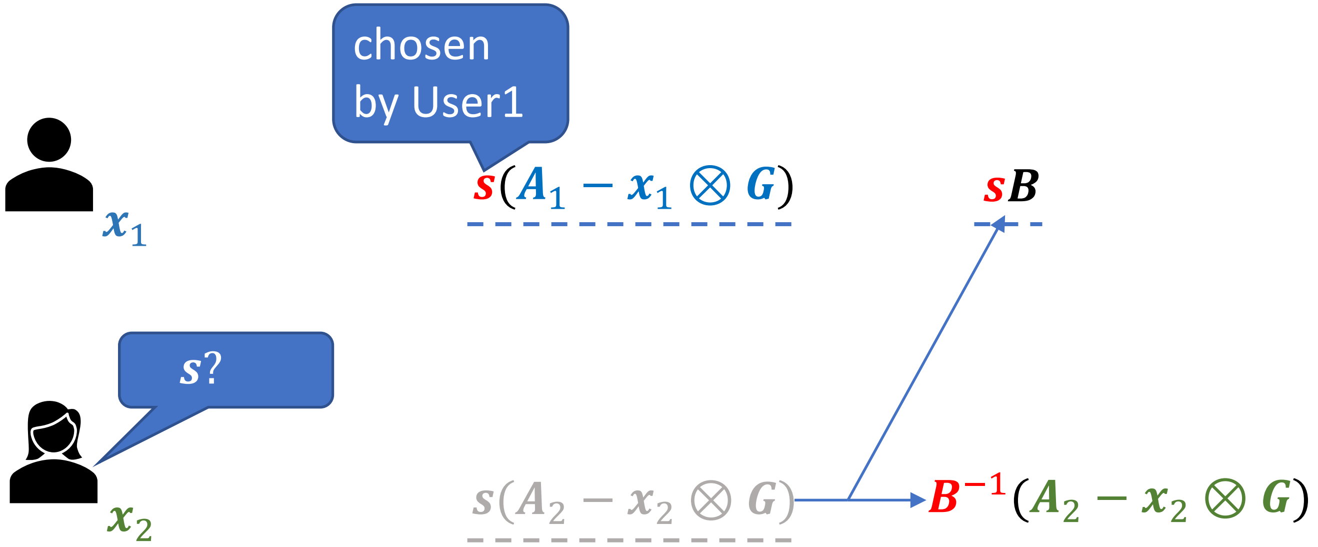
Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

$$\Downarrow$$

BGG+ ciphertext

$$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$$



chosen
by User1
$\boldsymbol{x}_1$
$\boldsymbol{s}?$
$\boldsymbol{x}_2$
$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$
$\boldsymbol{s}\boldsymbol{B}$
$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$
$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

KeyGen(f)

Same as BGG+ key: $\boldsymbol{A}_f^{-1}(\boldsymbol{G}\boldsymbol{u}^T)$

$$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}), \quad \boldsymbol{s}\boldsymbol{B}$$

Construction Warm-Up

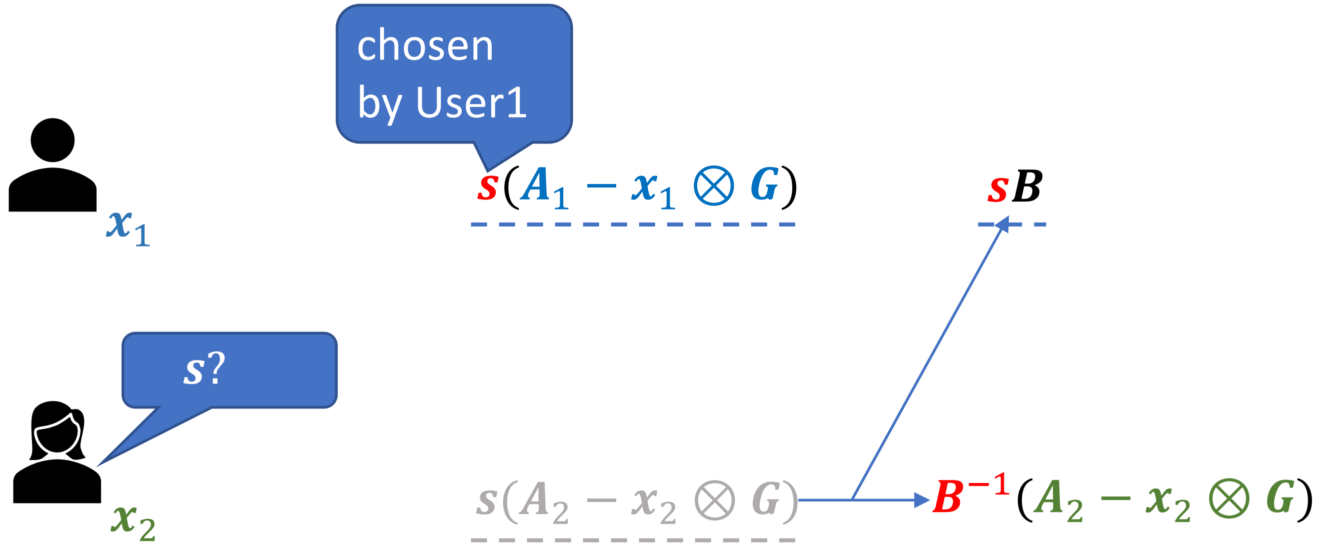
Encryption

$x = (x_1|x_2)$

$$\downarrow$$

BGG+ ciphertext

$\underline{s((A_1|A_2) - (x_1|x_2) \otimes G)}$



chosen by User1

x_1

$\underline{s(A_1 - x_1 \otimes G)}$

$\underline{sB}$

s?

x_2

$\underline{s(A_2 - x_2 \otimes G)} \longrightarrow B^{-1}(A_2 - x_2 \otimes G)$

KeyGen(f)

Same as BGG+ key: $A_f^{-1}(Gu^T)$

$\underline{s(A_1 - x_1 \otimes G)}$, $\underline{sB}$

$B^{-1}(A_2 - x_2 \otimes G)$

$B^{-1}(A_2 - \overline{x}_2 \otimes G)$

Construction Warm-Up

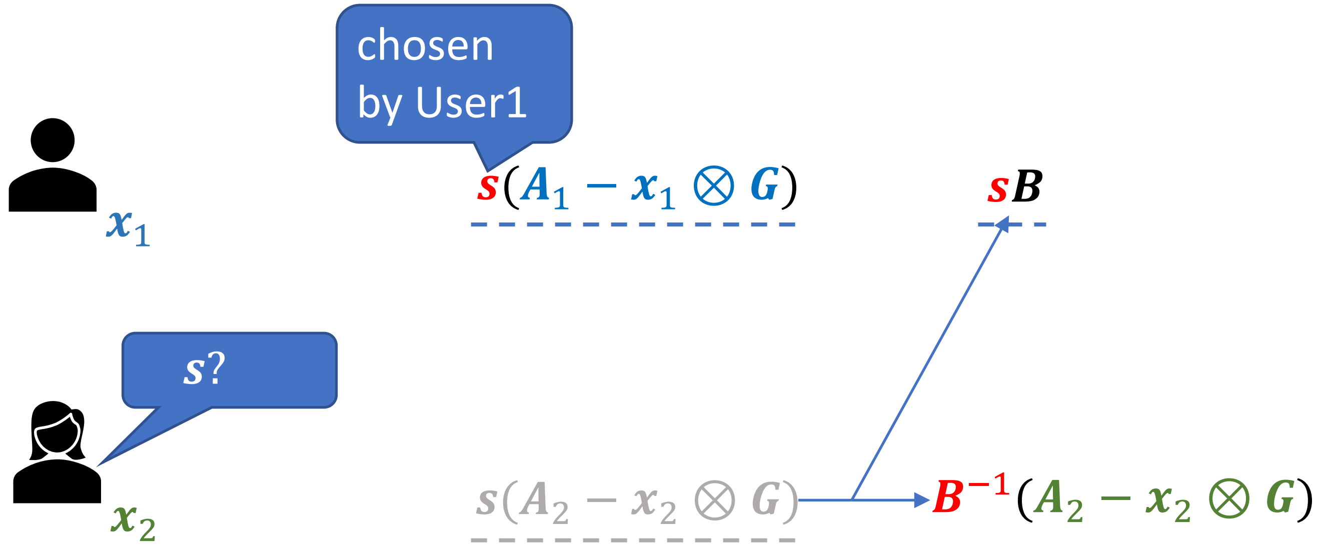
Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1|\boldsymbol{x}_2)$

↓

BGG+ ciphertext

$\underline{\boldsymbol{s}((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})}$



$\boldsymbol{x}_1$
chosen by User1
$\underline{\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})}$
$\underline{\boldsymbol{s}\boldsymbol{B}}$
$\boldsymbol{s}$?
$\boldsymbol{x}_2$
$\underline{\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})}$
$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

KeyGen(f)

Same as BGG+ key: $\boldsymbol{A}_f^{-1}(\boldsymbol{G}\boldsymbol{u}^T)$

$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

$\underline{\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})}$, $\underline{\boldsymbol{s}\boldsymbol{B}}$

$\underline{\boldsymbol{s}((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})}$

$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \overline{\boldsymbol{x}}_2 \otimes \boldsymbol{G})$

Construction Warm-Up

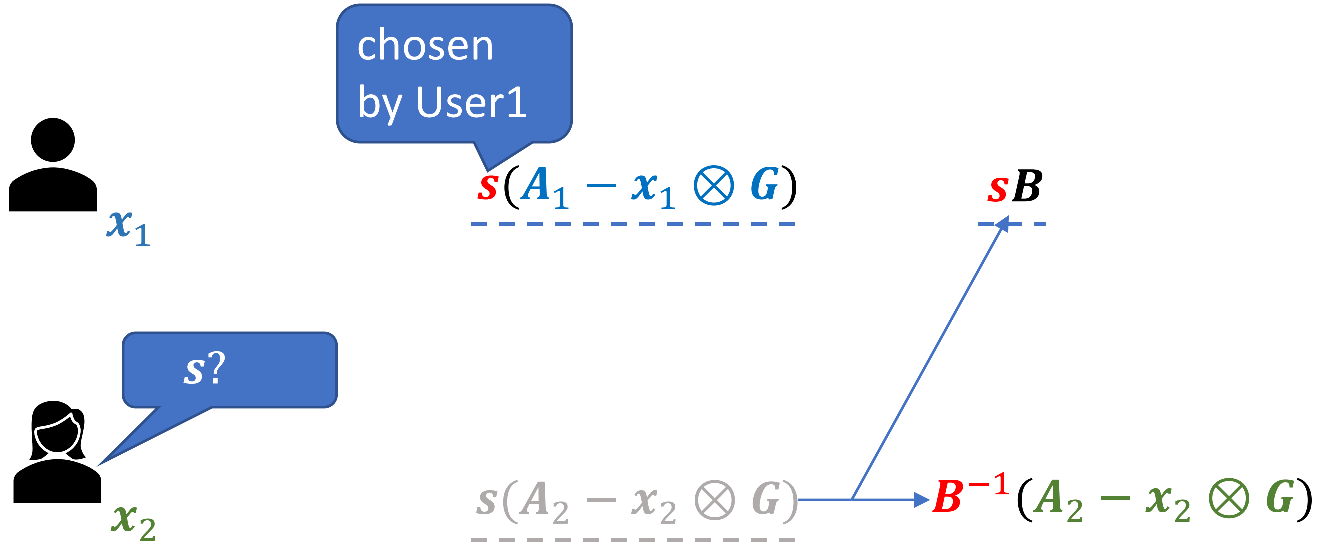
Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1|\boldsymbol{x}_2)$

$\Downarrow$

BGG+ ciphertext

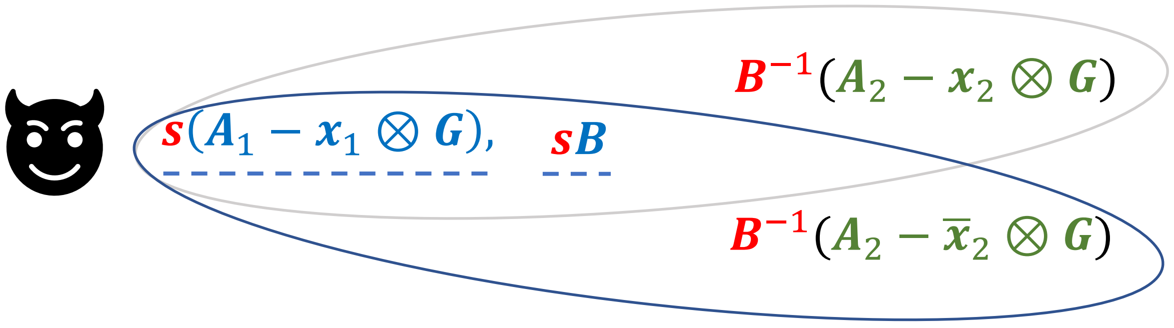
$\boldsymbol{s}((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})$



chosen by User1
$\boldsymbol{x}_1$
$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$
$\boldsymbol{sB}$
$s?$
$\boldsymbol{x}_2$
$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$
$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

KeyGen(f)

Same as BGG+ key: $\boldsymbol{A}_f^{-1}(\boldsymbol{G}\boldsymbol{u}^T)$



$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$
$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$, $\boldsymbol{sB}$
$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \bar{\boldsymbol{x}}_2 \otimes \boldsymbol{G})$

$\boldsymbol{s}((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})$

$\boldsymbol{s}((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\bar{\boldsymbol{x}}_2) \otimes \boldsymbol{G})$

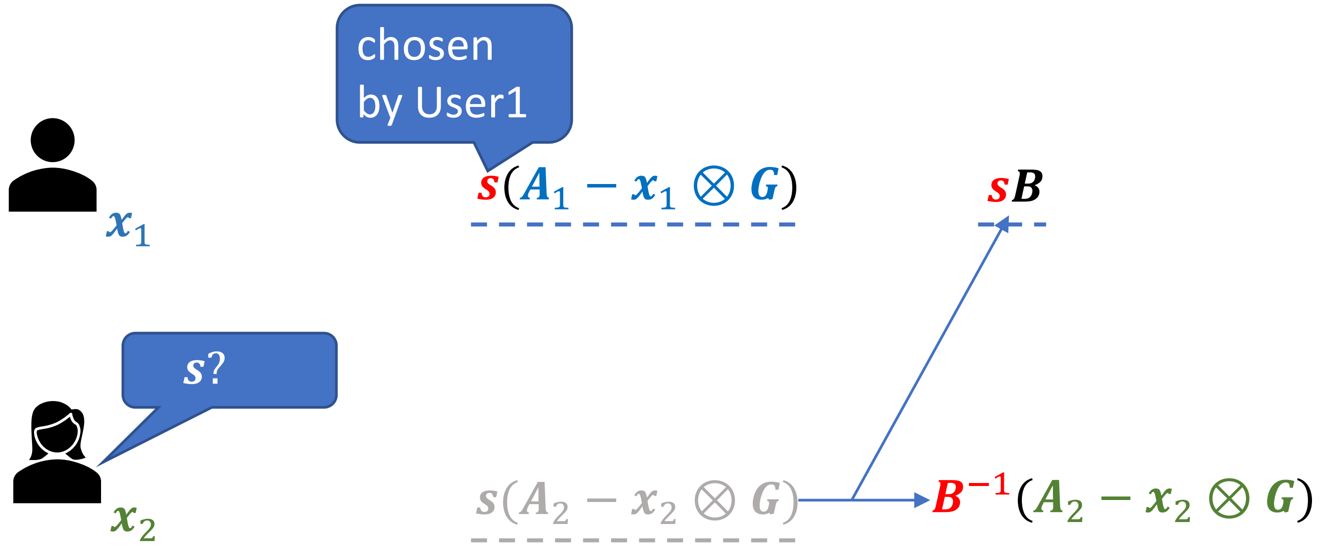
Construction Warm-Up

Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$

BGG+ ciphertext

$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$



chosen by User1

$\boldsymbol{x}_1$

$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$

$\boldsymbol{sB}$

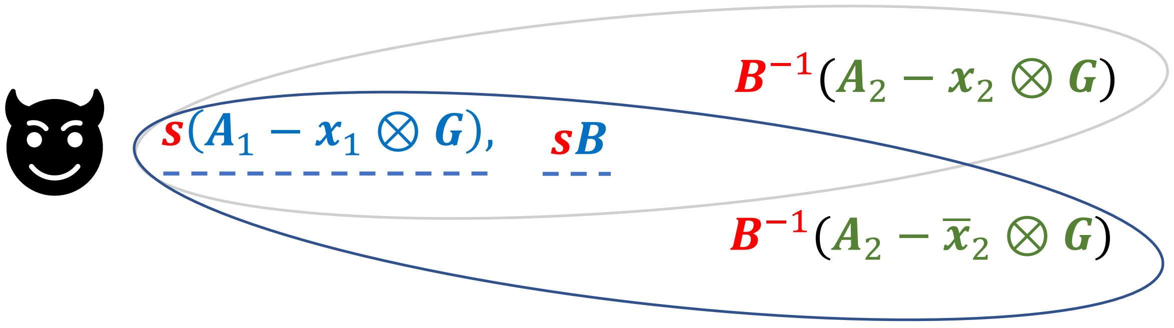
$\boldsymbol{s}?$

$\boldsymbol{x}_2$

$\boldsymbol{s}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \rightarrow \boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

KeyGen(f)

Same as BGG+ key: $\boldsymbol{A}_f^{-1}(\boldsymbol{G}\boldsymbol{u}^T)$



$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G})$

$\boldsymbol{s}(\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G})$, $\boldsymbol{sB}$

$\boldsymbol{B}^{-1}(\boldsymbol{A}_2 - \overline{\boldsymbol{x}}_2 \otimes \boldsymbol{G})$

$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})$

$\boldsymbol{s}((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \overline{\boldsymbol{x}}_2) \otimes \boldsymbol{G})$

Two BGG+ ciphertexts with same secret – Insecure!

Construction Warm-Up

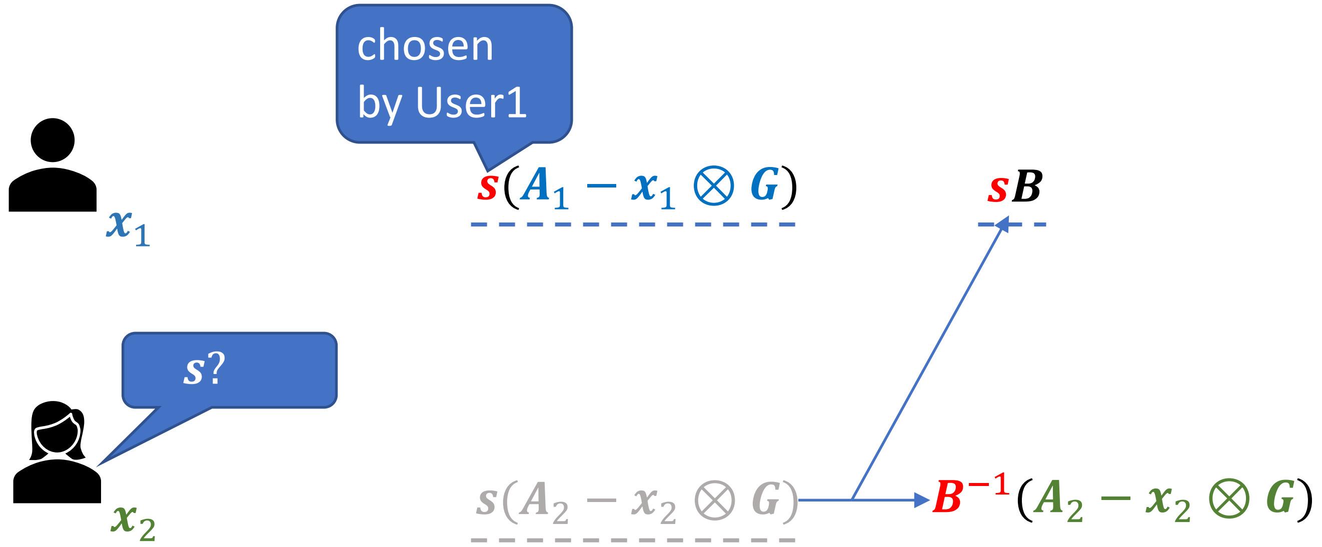
Encryption

$x = (x_1|x_2)$

↓

BGG+ ciphertext

$\underline{s((A_1|A_2) - (x_1|x_2) \otimes G)}$



x_1

x_2

chosen by User1

$s?$

$\underline{s(A_1 - x_1 \otimes G)}$

$\underline{sB}$

$\underline{s(A_2 - x_2 \otimes G)} \rightarrow B^{-1}(A_2 - x_2 \otimes G)$

Fix [Wee22]

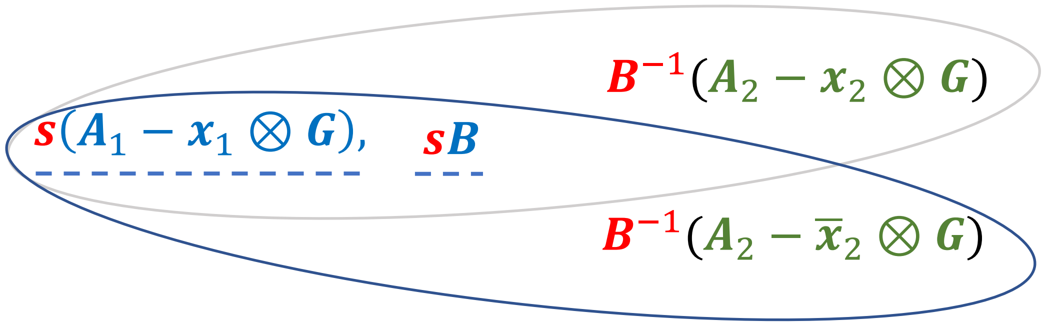
Ensure different random secret s_i for each BGG+ ciphertext as

$s_i = s(I \otimes r_i^T)$

Freshly sampled by User 2

KeyGen(f)

Same as BGG+ key: $A_f^{-1}(Gu^T)$



$B^{-1}(A_2 - x_2 \otimes G)$

$\underline{s(A_1 - x_1 \otimes G)}$, $\underline{sB}$

$B^{-1}(A_2 - \overline{x}_2 \otimes G)$

$\underline{s((A_1|A_2) - (x_1|\overline{x}_2) \otimes G)}$

Two BGG+ ciphertexts with same secret – Insecure!

Construction Attempt 1

Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1|\boldsymbol{x}_2)$

↓

BGG+ ciphertext

$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})}$

$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$

$\boldsymbol{x}_1$

$\underline{\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big)}$, $\underline{\boldsymbol{s}\boldsymbol{B}}$

$\boldsymbol{x}_2$

$\boldsymbol{B}^{-1}\left((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right)$, $\boldsymbol{r}_i^T$

Construction Attempt 1

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

$$\downarrow$$

BGG+ ciphertext

$$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})}$$

$$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$$

$\boldsymbol{x}_1$

$$\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)$$
$$= \boldsymbol{s}\left((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right)$$

$$\underline{\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}}\big), \qquad \underline{\boldsymbol{s}\boldsymbol{B}}$$

$\boldsymbol{x}_2$

$$\boldsymbol{B}^{-1}\left((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right), \quad \boldsymbol{r}_i^T$$

Construction Attempt 1

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1|\boldsymbol{x}_2)$$

↓

BGG+ ciphertext

$$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})}$$

$$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$$

$\boldsymbol{x}_1$

$$\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})(\boldsymbol{I} \otimes \boldsymbol{r}_i^T) = \boldsymbol{s}\left((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right)$$

$$\underline{\boldsymbol{s}\left((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\right)}, \quad \underline{\boldsymbol{s}\boldsymbol{B}}$$

$\boldsymbol{x}_2$

$$\boldsymbol{B}^{-1}\left((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right), \quad \boldsymbol{r}_i^T$$

[Wee22] - Homomorphism is preserved even after tensoring

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Construction Attempt 1

Encryption

$x = (x_1|x_2)$

↓

BGG+ ciphertext

$\underline{s(I \otimes r_i^T)((A_1|A_2) - (x_1|x_2) \otimes G)}$

$= \underline{s(((A_1|A_2) - (x_1|x_2) \otimes G) \otimes r_i^T)}$

x_1 $\underline{s((A_1 - x_1 \otimes G) \otimes I)}$, $\underline{sB}$

$s((A_1 - x_1 \otimes G) \otimes I)(I \otimes r_i^T)$
$= s\left((A_1 - x_1 \otimes G) \otimes r_i^T\right)$

x_2 $B^{-1}\left((A_2 - x_2 \otimes G) \otimes r_i^T\right)$, r_i^T

KeyGen(f)

Same as BGG+ key: $A_f^{-1}(Gu^T)$

[Wee22] - Homomorphism is preserved even after tensoring

$$\left((A - x \otimes G) \otimes r^T\right)H = (A_f - f(x)G) \otimes r^T$$

Construction Attempt 1

Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$

↓

BGG+ ciphertext

$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})}$

$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$

$\boldsymbol{x}_1$

$\underline{\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}}\big)$, $\underline{\boldsymbol{s}\boldsymbol{B}}$

$\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)$
$= \boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\big)$

$\boldsymbol{x}_2$

$\boldsymbol{B}^{-1}\big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\big)$, $\boldsymbol{r}_i^T$

KeyGen(f)

Same as BGG+ key: $\boldsymbol{A}_f^{-1}(\boldsymbol{G}\boldsymbol{u}^T)$

[Wee22] - Homomorphism is preserved even after tensoring

$$\big((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Structured matrix

Proving Security: Cannot apply evasive LWE with $\boldsymbol{A}_f^{-1}(\cdot)$

Construction Attempt 2

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

↓

BGG+ ciphertext

$$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})}$$

$$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$$

$\boldsymbol{x}_1$

$$\boldsymbol{s}\big(\boldsymbol{(}\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I} \big)(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)$$
$$= \boldsymbol{s}\Big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\Big)$$

$$\underline{\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}}\big), \qquad \underline{\boldsymbol{s}\boldsymbol{B}}$$

$\boldsymbol{x}_2$

$$\boldsymbol{B}^{-1}\Big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\Big), \quad \boldsymbol{r}_i^T$$

KeyGen(f)

Construction Attempt 2

Encryption

$$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$$

↓

BGG+ ciphertext

$$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G})}$$

$$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1 | \boldsymbol{A}_2) - (\boldsymbol{x}_1 | \boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$$

$\boldsymbol{x}_1$

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big)(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)$$
$$= \boldsymbol{s}\left((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right)$$

$$\underline{\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}}\big), \qquad \underline{\boldsymbol{s}\boldsymbol{B}}$$

$\boldsymbol{x}_2$

$$\boldsymbol{B}^{-1}\left((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right), \quad \boldsymbol{r}_i^T$$

KeyGen(f)

Modify the key as : $\boldsymbol{B}^{-1}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})$

Construction Attempt 2

$$\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)$$
$$= \boldsymbol{s}\left((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right)$$

Encryption

$\boldsymbol{x} = (\boldsymbol{x}_1 | \boldsymbol{x}_2)$

↓

BGG+ ciphertext

$\underline{\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G})}$

$= \underline{\boldsymbol{s}(((\boldsymbol{A}_1|\boldsymbol{A}_2) - (\boldsymbol{x}_1|\boldsymbol{x}_2) \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T)}$

$\boldsymbol{x}_1$ $\underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})}$, $\underline{\boldsymbol{s}\boldsymbol{B}}$

$\boldsymbol{x}_2$ $\boldsymbol{B}^{-1}\left((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T\right)$, $\boldsymbol{r}_i^T$

KeyGen(f)

Modify the key as : $\boldsymbol{B}^{-1}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})$

<ins>Proving Security:</ins> Can now apply evasive LWE

Construction Attempt 2

Encryption

$$x = (x_1 | x_2)$$

↓

BGG+ ciphertext

$\underline{s(I \otimes r_i^T)((A_1|A_2) - (x_1|x_2) \otimes G)}$

$= \underline{s(((A_1|A_2) - (x_1|x_2) \otimes G) \otimes r_i^T)}$

x_1 $\underline{s((A_1 - x_1 \otimes G) \otimes I)}$, $\underline{sB}$

$s((A_1 - x_1 \otimes G) \otimes I)(I \otimes r_i^T)$
$= s\left((A_1 - x_1 \otimes G) \otimes r_i^T\right)$

x_2 $B^{-1}\left((A_2 - x_2 \otimes G) \otimes r_i^T\right)$, r_i^T

KeyGen(f)

Modify the key as : $B^{-1}(A_f u^T \otimes I)$

<u>Proving Security:</u> Can now apply evasive LWE ↓

Prove pseudorandomness of $\underline{s((A_1 - x_1 \otimes G) \otimes I)}$, $\underline{sB}$, $\underline{s\left((A_2 - x_2 \otimes G) \otimes r_i^T\right)}$, $\underline{s(A_f u^T \otimes I)}$

Construction Attempt 2

$$\mathbf{s}((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{r}_i^T)$$
$$= \mathbf{s}\left((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{r}_i^T\right)$$

Encryption

$\mathbf{x} = (\mathbf{x}_1|\mathbf{x}_2)$

↓

BGG+ ciphertext

$\underline{\mathbf{s}(\mathbf{I} \otimes \mathbf{r}_i^T)((\mathbf{A}_1|\mathbf{A}_2) - (\mathbf{x}_1|\mathbf{x}_2) \otimes \mathbf{G})}$

$= \underline{\mathbf{s}(((\mathbf{A}_1|\mathbf{A}_2) - (\mathbf{x}_1|\mathbf{x}_2) \otimes \mathbf{G}) \otimes \mathbf{r}_i^T)}$

$\mathbf{x}_1$ $\underline{\mathbf{s}((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{I})}$, $\underline{\mathbf{s}\mathbf{B}}$

$\mathbf{x}_2$ $\mathbf{B}^{-1}\left((\mathbf{A}_2 - \mathbf{x}_2 \otimes \mathbf{G}) \otimes \mathbf{r}_i^T\right)$, $\mathbf{r}_i^T$

KeyGen(f)

Modify the key as : $\mathbf{B}^{-1}(\mathbf{A}_f\mathbf{u}^T \otimes \mathbf{I})$

<u>Proving Security:</u> Can now apply evasive LWE ↓

Prove pseudorandomness of $\underline{\mathbf{s}((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{I})}$, $\underline{\mathbf{s}\mathbf{B}}$, $\underline{\mathbf{s}\left((\mathbf{A}_2 - \mathbf{x}_2 \otimes \mathbf{G}) \otimes \mathbf{r}_i^T\right)}$, $\underline{\mathbf{s}(\mathbf{A}_f\mathbf{u}^T \otimes \mathbf{I})}$

Use Tensor LWE assumption, but…

Construction Attempt 2

$$s((A_1 - x_1 \otimes G) \otimes I)(I \otimes r_i^T)$$
$$= s\left((A_1 - x_1 \otimes G) \otimes r_i^T\right)$$

Encryption

$x = (x_1|x_2)$

↓

BGG+ ciphertext

$\underline{s(I \otimes r_i^T)((A_1|A_2) - (x_1|x_2) \otimes G)}$

$= \underline{s(((A_1|A_2) - (x_1|x_2) \otimes G) \otimes r_i^T)}$

x_1 $\underline{s((A_1 - x_1 \otimes G) \otimes I)}$, $\underline{sB}$

x_2 $B^{-1}\left((A_2 - x_2 \otimes G) \otimes r_i^T\right)$, r_i^T

KeyGen(f)

Modify the key as : $B^{-1}(A_f u^T \otimes I)$

<u>Proving Security:</u> Can now apply evasive LWE ↓

Prove pseudorandomness of $\underline{s((A_1 - x_1 \otimes G) \otimes I)}$, $\underline{sB}$, $\underline{s\left((A_2 - x_2 \otimes G) \otimes r_i^T\right)}$, $\underline{s(A_f u^T \otimes I)}$

Use Tensor LWE assumption, but… misfit

Construction Attempt 2

$$\mathbf{s}((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{r}_i^T) = \mathbf{s}\left((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{r}_i^T\right)$$

Encryption

$\mathbf{x} = (\mathbf{x}_1 | \mathbf{x}_2)$

BGG+ ciphertext

$\underline{\mathbf{s}(\mathbf{I} \otimes \mathbf{r}_i^T)((\mathbf{A}_1|\mathbf{A}_2) - (\mathbf{x}_1|\mathbf{x}_2) \otimes \mathbf{G})}$

$= \underline{\mathbf{s}(((\mathbf{A}_1|\mathbf{A}_2) - (\mathbf{x}_1|\mathbf{x}_2) \otimes \mathbf{G}) \otimes \mathbf{r}_i^T)}$

$\mathbf{x}_1$ $\quad \underline{\mathbf{s}((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{I})}, \qquad \underline{\mathbf{s}\mathbf{B}}$

$\mathbf{x}_2$ $\quad \mathbf{B}^{-1}\left((\mathbf{A}_2 - \mathbf{x}_2 \otimes \mathbf{G}) \otimes \mathbf{r}_i^T\right), \quad \mathbf{r}_i^T$

KeyGen(f)

Modify the key as : $\mathbf{B}^{-1}(\mathbf{A}_f \mathbf{u}^T \otimes \mathbf{I})$

<u>Proving Security:</u> Can now apply evasive LWE

Prove pseudorandomness of $\underline{\mathbf{s}((\mathbf{A}_1 - \mathbf{x}_1 \otimes \mathbf{G}) \otimes \mathbf{I})}, \quad \underline{\mathbf{s}\mathbf{B}}, \quad \underline{\mathbf{s}\left((\mathbf{A}_2 - \mathbf{x}_2 \otimes \mathbf{G}) \otimes \mathbf{r}_i^T\right)}, \quad \underline{\mathbf{s}(\mathbf{A}_f \mathbf{u}^T \otimes \mathbf{I})}$

Use Tensor LWE assumption, but… misfit

Fix: Hide these terms using LWE samples

Construction Attempt 3

Applyig the Fix

sampled by user 1

Part of mpk

$\boldsymbol{x}_1$ $\underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})}$ $\longrightarrow$ $\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})}$

Construction Attempt 3

Applyig the Fix

$\boldsymbol{x}_1$ $\quad \underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \underline{\overbrace{\boldsymbol{s}_0}^{\text{sampled by user 1}}\overbrace{(\boldsymbol{A}_0 \otimes \boldsymbol{I})}^{\text{Part of mpk}}}$

$\underline{\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{I})}$

Construction Attempt 3

Applyig the Fix

$\boldsymbol{x}_1$ $\quad \underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})}$

$\underline{\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{I})}$

sampled by user 1

Part of mpk

sampled by user 1

Part of mpk

Construction Attempt 3

Applyig the Fix

sampled by user 1

Part of mpk

👤 $\boldsymbol{x}_1$ $\underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})}$ 😇

🔑 $\underline{\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{I})}$

sampled by user 1

Part of mpk

Construction Attempt 3

Applyig the Fix

x_1 $\quad \underline{s((A_1 - x_1 \otimes G) \otimes I)} \longrightarrow s((A_1 - x_1 \otimes G) \otimes I) + \underline{\overset{\text{sampled by user 1}}{s_0}\overset{\text{Part of mpk}}{(A_0 \otimes I)}}$ 😇

$\underline{s(A_f u^T \otimes I)} \longrightarrow s(A_f u^T \otimes I) + \underline{\underset{\text{sampled by user 1}}{s_1}\underset{\text{Part of mpk}}{(D \otimes I)}}$ ☹

Construction Attempt 3

Applyig the Fix

sampled by user 1

Part of mpk

$\boldsymbol{x}_1$ $\quad \underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})}$ 😇

$\underline{\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{I})}$ ☹

Same mask for different functions - insecure

sampled by user 1

Part of mpk

Construction Attempt 3

Applyig the Fix

sampled by user 1

Part of mpk

$\boldsymbol{x}_1$ $\quad \underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \boldsymbol{s}_0\underline{(\boldsymbol{A}_0 \otimes \boldsymbol{I})}$ ☺

$\underline{\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \boldsymbol{s}_1\underline{(\boldsymbol{D} \otimes \boldsymbol{I})}$ ☹

sampled by user 1

Part of mpk

Same mask for different functions - insecure

Fix: KeyGen must introduce its own randomness

Construction Attempt 3 (Final)

Applyig the Fix

👤 $\boldsymbol{x}_1$ $$\underline{\boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}) + \underline{\overset{\text{sampled by user 1}}{\boldsymbol{s}_0}\overset{\text{Part of mpk}}{(\boldsymbol{A}_0 \otimes \boldsymbol{I})}}$$ 😇

🔑 $$\underline{\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\underset{\text{sampled by user 1}}{\boldsymbol{s}_1}\underset{\text{Part of mpk}}{(\boldsymbol{D} \otimes \boldsymbol{I})}}$$ ☹

Same mask for different functions - insecure

Fix: KeyGen must introduce its own randomness

$$\boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{I})} \longrightarrow \boldsymbol{s}(\boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I}) + \underline{\boldsymbol{s}_1(\boldsymbol{D} \otimes \overset{\text{sampled by KeyGen}}{\boldsymbol{t}^T} \otimes \boldsymbol{I})}$$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise$$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise$$

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{I}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise$$

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{I}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Low norm if $f \in NC1$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise$$

$$= \boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^{\boldsymbol{T}})(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{I}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Low norm if $f \in NC1$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^T) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^T\right) + noise$$

$$= \boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T)(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$$\approx (\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^T) + noise)(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{I}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Low norm if $f \in NC1$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise$$

$$= \boldsymbol{s}\left(\boldsymbol{I} \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right)(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$$\approx \left(\boldsymbol{s}\left(\boldsymbol{I} \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise\right)(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$$\approx \boldsymbol{s}_i(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

Fresh random secret

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{I}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Low norm if $f \in NC1$

Evasive LWE Suffices for NC1

Low norm

$$\boldsymbol{s}((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{G}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise \longrightarrow \boldsymbol{s}\left((\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) \otimes \boldsymbol{r}_i^{\boldsymbol{T}}\right) + noise$$

$$= \boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^{\boldsymbol{T}})(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$$\approx (\boldsymbol{s}(\boldsymbol{I} \otimes \boldsymbol{r}_i^{\boldsymbol{T}}) + noise)(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

Fresh random secret

$$\approx \boldsymbol{s}_i(\boldsymbol{A}_i - \boldsymbol{x}_i \otimes \boldsymbol{I}) + noise$$

$\approx$ random (from LWE)

$$\left((\boldsymbol{A} - \boldsymbol{x} \otimes \boldsymbol{I}) \otimes \boldsymbol{r}^T\right)\boldsymbol{H} = (\boldsymbol{A}_f - f(\boldsymbol{x})\boldsymbol{G}) \otimes \boldsymbol{r}^T$$

Low norm if $f \in NC1$

Summary and Open Problems

We constructed constant arity ABE from evasive and tensor LWE

Evasive LWE suffices for NC1 circuits

We also studied tensor LWE assumption and show new implications

Summary and Open Problems

We constructed constant arity ABE from evasive and tensor LWE

Evasive LWE suffices for NC1 circuits

We also studied tensor LWE assumption and show new implications

Open Problems

Construction of constant arity miABE from standard LWE

Going beyond constant arity

Supporting corruptions

Thank You!

Final Construction

User1$(\boldsymbol{x}_1, m)$

$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \quad)}\boldsymbol{B},$ if $m = 0$, else random

Final Construction

User1($\boldsymbol{x}_1, m$)

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \quad)\boldsymbol{B}}$, if $m = 0$, else random

User2($\boldsymbol{x}_2$)

$$\boldsymbol{B}^{-1}\begin{pmatrix} \big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big) & \\ & (\boldsymbol{A}_0 \otimes \boldsymbol{r}^T) \\ & \end{pmatrix}$$

Final Construction

User1$(\boldsymbol{x}_1, m)$

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \boldsymbol{s}_1)\boldsymbol{B}},$ if $m = 0$, else random

KeyGen(f)

$$\boldsymbol{B}^{-1}\begin{pmatrix} \boldsymbol{A}_f\boldsymbol{u}^T \otimes \boldsymbol{I} \\ \boldsymbol{0} \\ (\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{I}) \end{pmatrix},$$

User2$(\boldsymbol{x}_2)$

$$\boldsymbol{B}^{-1}\begin{pmatrix} \big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big) & \\ & (\boldsymbol{A}_0 \otimes \boldsymbol{r}^T) \\ & \end{pmatrix}$$

Final Construction

User1$(\boldsymbol{x}_1, m)$

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \boldsymbol{s}_1)\boldsymbol{B}}$, if $m = 0$, else random

KeyGen(f)

$$\boldsymbol{B}^{-1} \begin{pmatrix} \boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I} \\ \boldsymbol{0} \\ (\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{I}) \end{pmatrix},$$

User2$(\boldsymbol{x}_2)$

$$\boldsymbol{B}^{-1} \begin{pmatrix} \big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big) & \\ & (\boldsymbol{A}_0 \otimes \boldsymbol{r}^T) \\ & \end{pmatrix}$$

Recovering the mask $\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{r}^T)$

Final Construction

User1$(\boldsymbol{x}_1, m)$

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \boldsymbol{s}_1)\boldsymbol{B}}$, if $m = 0$, else random

KeyGen(f)

$$\boldsymbol{B}^{-1}\begin{pmatrix} \boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I} \\ \boldsymbol{0} \\ (\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{I}) \end{pmatrix},$$

User2$(\boldsymbol{x}_2)$

$$\boldsymbol{B}^{-1}\begin{pmatrix} \big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big) & \\ & (\boldsymbol{A}_0 \otimes \boldsymbol{r}^T) \\ & \end{pmatrix}$$

Recovering the mask $\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{r}^T)$

$$= \boldsymbol{s}_1(\boldsymbol{I} \otimes \boldsymbol{r}^T)(\boldsymbol{D} \otimes \boldsymbol{t}^T)$$

Final Construction

User1$(\boldsymbol{x}_1, m)$

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \boldsymbol{s}_1)\boldsymbol{B}},$ if $m = 0$, else random

KeyGen(f)

$$\boldsymbol{B}^{-1}\begin{pmatrix} \boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I} \\ \boldsymbol{0} \\ (\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{I}) \end{pmatrix},$$

User2$(\boldsymbol{x}_2)$

$$\boldsymbol{B}^{-1}\begin{pmatrix} \big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big) \\ (\boldsymbol{A}_0 \otimes \boldsymbol{r}^T) \\ \end{pmatrix}$$

Recovering the mask $\boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{r}^T)$

$$= \boldsymbol{s}_1(\boldsymbol{I} \otimes \boldsymbol{r}^T)(\boldsymbol{D} \otimes \boldsymbol{t}^T)$$

$$= \boldsymbol{s}_1\ (\boldsymbol{I} \otimes \boldsymbol{r}^T)\boldsymbol{C}\,\boldsymbol{C}^{-1}(\boldsymbol{D} \otimes\ \boldsymbol{t}^T)$$

Final Construction

User1$(\boldsymbol{x}_1, m)$

$$\boldsymbol{s}\big((\boldsymbol{A}_1 - \boldsymbol{x}_1 \otimes \boldsymbol{G}) \otimes \boldsymbol{I}\big) + \underline{\boldsymbol{s}_0(\boldsymbol{A}_0 \otimes \boldsymbol{I})},$$

$\underline{(\boldsymbol{s}, \boldsymbol{s}_0, \boldsymbol{s}_1)\boldsymbol{B}}$, if $m = 0$, else random

KeyGen(f)

$$\boldsymbol{B}^{-1}\begin{pmatrix} \boldsymbol{A}_f \boldsymbol{u}^T \otimes \boldsymbol{I} \\ \boldsymbol{0} \\ (\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{I}) \end{pmatrix}, \quad \boldsymbol{C}^{-1}(\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{I})$$

User2$(\boldsymbol{x}_2)$

$$\boldsymbol{B}^{-1}\begin{pmatrix} \big((\boldsymbol{A}_2 - \boldsymbol{x}_2 \otimes \boldsymbol{G}) \otimes \boldsymbol{r}^T\big) & & \\ & (\boldsymbol{A}_0 \otimes \boldsymbol{r}^T) & \\ & & (\boldsymbol{C} \otimes \boldsymbol{r}^T) \end{pmatrix}$$

Recovering the mask

$$\begin{aligned} & \boldsymbol{s}_1(\boldsymbol{D} \otimes \boldsymbol{t}^T \otimes \boldsymbol{r}^T) \\ &= \boldsymbol{s}_1(\boldsymbol{I} \otimes \boldsymbol{r}^T)(\boldsymbol{D} \otimes \boldsymbol{t}^T) \\ &= \boldsymbol{s}_1\ (\boldsymbol{I} \otimes \boldsymbol{r}^T)\boldsymbol{C}\,\boldsymbol{C}^{-1}(\boldsymbol{D} \otimes\ \boldsymbol{t}^T) \end{aligned}$$

Tensor Product

Tensoring

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \qquad \boldsymbol{B} \qquad\qquad \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} \end{pmatrix}$$

Tensor Product

Tensoring

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \qquad \boldsymbol{B} \qquad\qquad \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} \end{pmatrix}$$

$$(\boldsymbol{A} \otimes \boldsymbol{B})(\boldsymbol{C} \otimes \boldsymbol{D}) = \boldsymbol{AC} \otimes \boldsymbol{BD}$$

Tensor Product

Tensoring

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad \boldsymbol{B} \qquad\qquad \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} \end{pmatrix}$$

$$(\boldsymbol{A} \otimes \boldsymbol{B})(\boldsymbol{C} \otimes \boldsymbol{D}) = \boldsymbol{AC} \otimes \boldsymbol{BD}$$

$$\Downarrow$$

$$(\boldsymbol{A} \otimes \boldsymbol{I})(\boldsymbol{I} \otimes \boldsymbol{r}^T) = \boldsymbol{A} \otimes \boldsymbol{r}^T$$

$$(\boldsymbol{A} \otimes \boldsymbol{r}^T)\boldsymbol{B} = \boldsymbol{AB} \otimes \boldsymbol{r}^T$$