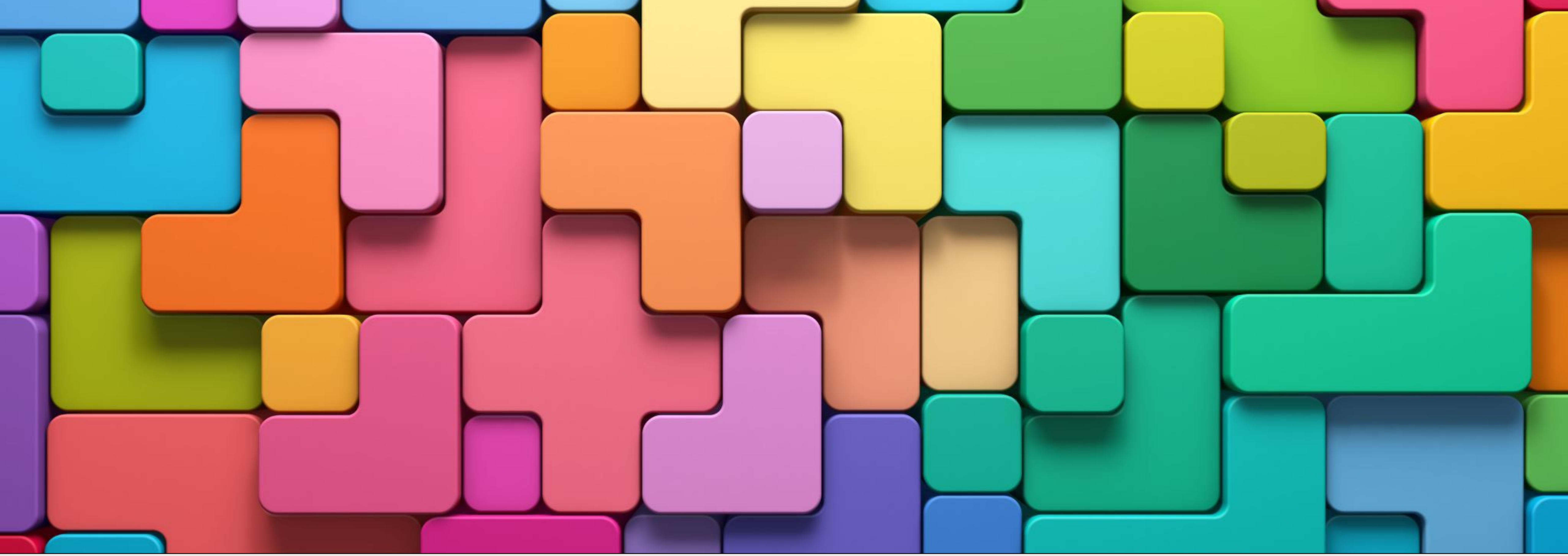
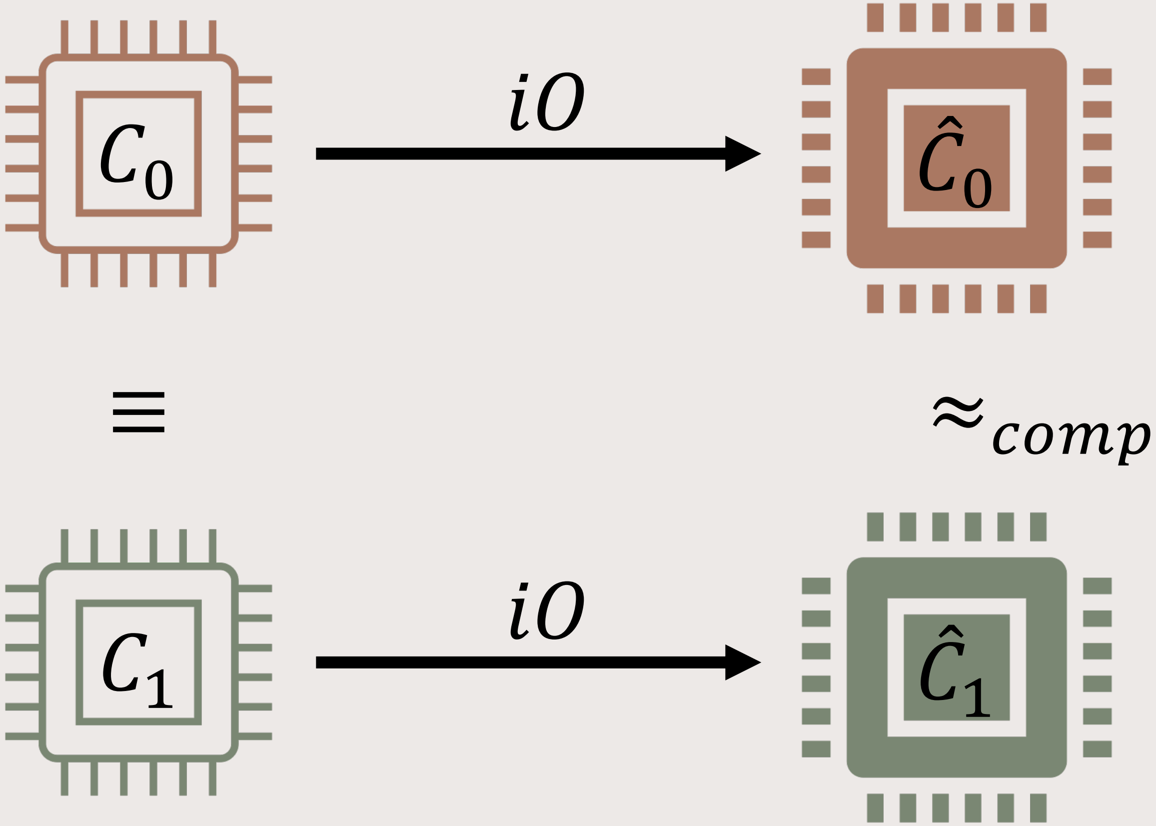


POLYNOMIAL TIME CRYPTANALYSIS OF THE SUBSPACE FLOODING ASSUMPTION FOR POST-QUANTUM *iO*

Aayush Jain (CMU), Huijia [Rachel] Lin (UW), Paul Lou (UCLA), Amit Sahai (UCLA)

Indistinguishability Obfuscation ($i\mathcal{O}$)

[BGI+01, GGH+13]



OBFUSTOPIA

[SW13, GGH+13, BZ13, HKW15, BKW15, HJKSWZ16…]

*i*O

OBFUSTOPIA

iO + Pseudorandom Oracle Model (PrOM) => Ideal Obfuscation [JLLW22]

OBFUSTOPIA

iO + Pseudorandom Oracle Model (PrOM) => Ideal Obfuscation [JLLW22]

can be heuristically instantiated by a hash function.

OBFUSTOPIA

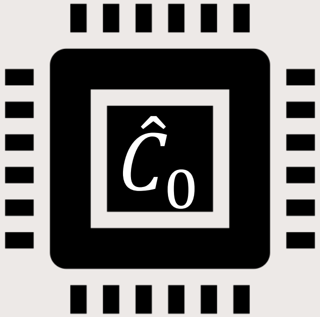
iO + Pseudorandom Oracle Model (PrOM) => Ideal Obfuscation [JLLW22]

Ideal obfuscation implies: Extractable witness encryption [GKPVZ13], Doubly Efficient PIR [BIPW17] , OT from binary erasure channels [AIKNPPR21], Wiretap-channel coding [IKLS22] and more!!

OBFUSTOPIA

iO + Pseudorandom Oracle Model (PrOM) => Ideal Obfuscation [JLLW22]

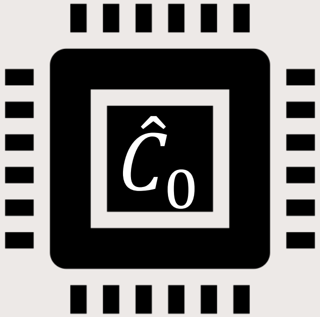
Ideal Obfuscation



OBFUSTOPIA

$i\mathcal{O}$ + Pseudorandom Oracle Model (PrOM) => Ideal Obfuscation [JLLW22]

Ideal Obfuscation



C_0 : Chat-GPT23

- A personal assistant that knows your deepest and darkest secrets.
- Ideal obfuscated version can be captured and tortured, yet reveal nothing beyond input/output behavior.

CONSTRUCTING *iO*

Well-founded Assumptions

[JLS20, JLS21]

- ✓ LPN over $\mathbb{Z}_p$ + DLIN over Bilinear Groups + PRGs in NC^0 + LWE [JLS20]
- ✓ LPN over $\mathbb{Z}_p$ + DLIN over Bilinear Groups + PRGs in NC^0 [JLS21]

⚠️ Not post-quantum secure (DLIN over Bilinear Groups).

PLAUSIBLY POST-QUANTUM CONSTRUCTIONS

[GGH+13, GGH15, GJK18, BIJ+20, CVW18, BDGM20A, BDGM20B, GP20, WW20, DQVWW21,…]

- Multilinear Maps, GGH'15 encodings [GGH+13, GGH15, CVW18] , Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BIJ+20] , Split-FHE Paradigm [BDGM20A]
  - ⚠️ *No reduction to simple, falsifiable assumption.*
- Shielded Randomness Leakage (SRL) [GP20, BDGM20B]
  - ⚠️ *Circuit-dependent hardness assumption: Each circuit being obfuscated gives a different hardness assumption. (Harder to cryptanalyze)*
  - ⚠️ *Explicit counterexample to [GP20] given by [HJL21]. (NOT an attack on obfuscation scheme).*
- Homomorphic Pseudorandom LWE Samples (HPLS) [WW20]
  - ⚠️ *Unspecified circuit implementation of PRF [exploited by [HJL21], (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult to explicitly write down error-distribution, therefore hard to cryptanalyze.*

PLAUSIBLY POST-QUANTUM CONSTRUCTIONS

[GGH+13, GGH15, GJK18, BIJ+20, CVW18, BDGM20A, BDGM20B, GP20, WW20, DQVWW21,…]

- GGH'15 Encodings [GGH+13, GGH15, CVW18] , Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BIJ+20] , Split FHE Paradigm [BDGM20A]
  - *No reduction to simple, fa*
- Shielded Randomness Lea
  - *Circuit-dependent hardnes ption. (Harder to cryptanalyze)*
  - *Explicit counterexample t*
- Homomorphic Pseudorandom LWE Samples (HPLS) [WW20]
  - *Unspecified circuit implementation of PRF [exploited by [HJL21], (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult to explicitly write down error-distribution, therefore hard to cryptanalyze.*

Many beautiful post-quantum iO candidate constructions.

Cryptanalysis refines our assumptions and helps us understand the security. We need to facilitate it.

PLAUSIBLY POST-QUANTUM CONSTRUCTIONS

[GGH+13, GGH15, GJK18, BIJ+20, CVW18, BDGM20A, BDGM20B, GP20, WW20, DQVWW21,…]

- GGH'15 Encodings [GGH+13, GGH15, CVW18] , Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BIJ+20] , Split FHE Paradigm [BDGM20A]
  - *No reduction to simple, fa*
- Shielded Randomness Lea
  - *Circuit-dependent hardnes … ption. (Harder to cryptanalyze)*
  - *Explicit counterexample t*
- Homomorphic Pseudorandom LWE Samples (HPLS) [WW20]
  - *Unspecified circuit implementation of PRF [exploited by [HJL21] (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult t … analyze.*

Many beautiful post-quantum iO candidate constructions.

Cryptanalysis refines our assumptions and helps us understand the security. We need to facilitate it.

Desiderata for Assumptions

✓ Simple-to-state, falsifiable, fully specified.

PLAUSIBLY POST-QUANTUM CONSTRUCTIONS

[GGH+13, GGH15, GJK18, BIJ+20, CVW18, BDGM20A, BDGM20B, GP20, WW20, DQVWW21,…]

- GGH'15 Encodings [GGH+13, GGH15, CVW18] , Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BIJ+20] , Split-FHE Paradigm [BDGM20A]
  - *No reduction to simple, falsifiable assumption.*
- Shielded Randomness Leakag
  - *Circuit-dependent hardness as* *hardness assumption. (Harder to cryptanalyze)*
  - *Explicit counterexample to [G* *heme).*
- Homomorphic Pseudorando
  - *Unspecified circuit implementation of PRF [exploited by [HJL21], (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult to explicitly write down error-distribution, therefore hard to cryptanalyze.*

[DQVWW21] Candidate construction via

Subspace Flooding Assumption

✓ *First fully specified and falsifiable assumption.*

✓ *Elegant candidate construction.*

✓ *Prior attacks shown to fail.*

SUBSPACE FLOODING ASSUMPTION

[DQVWW21]

Subspace Flooding Assumption

$$\mathbf{P}, \mathbf{P}', \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \widehat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}, \mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}) - b\mathbf{F}$$

Hides bit b

All these givens are matrices drawn from some distribution.

$$\{\mathbf{B}_i = \mathbf{A}_i\mathbf{S}_i + \mathbf{E}_i\}_{i\in[d]} \longrightarrow \mathbf{B}^* = \mathbf{A}^*\mathbf{S}^* + \mathbf{E}^*$$

$\mathbf{E}^*$, which depends on $\{\mathbf{E}_i\}_{i\in[d]}$, drowns out some a specific error distribution dependent on the bit b.

OUR WORK

Subspace Flooding Assumption [DQVWW21]

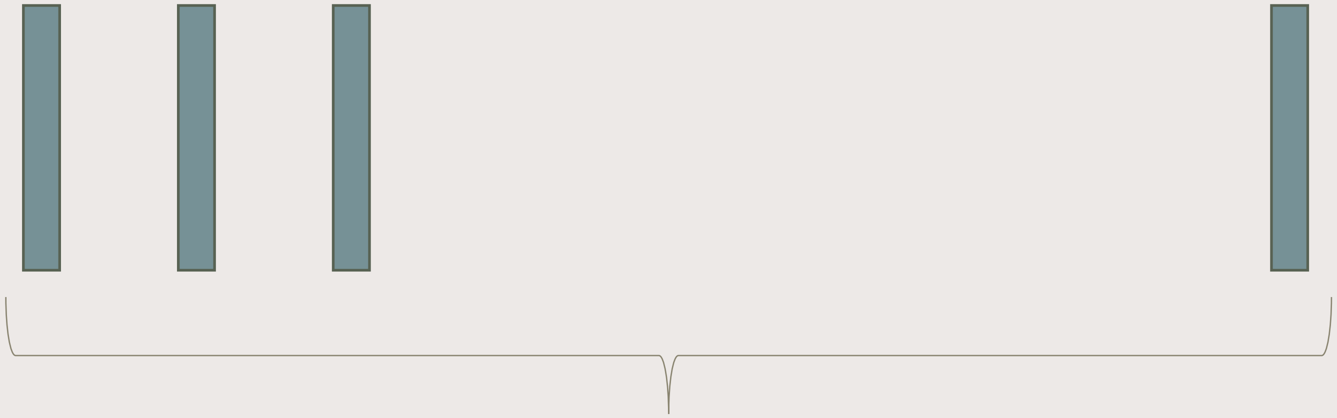
$$\mathbf{P}, \mathbf{P}', \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \widehat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}, \mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}) - b\mathbf{F}$$

Hides bit b

Theorem (informal): Under a reasonable conjecture, when $b = 0$, there exists a PPT algorithm that recovers the $\{\mathbf{E}_i\}_{i\in[d]}$ from the givens.

Corollary (informal): Under a heuristic argument, we obtain a PPT distinguisher for the subspace-flooding assumption.

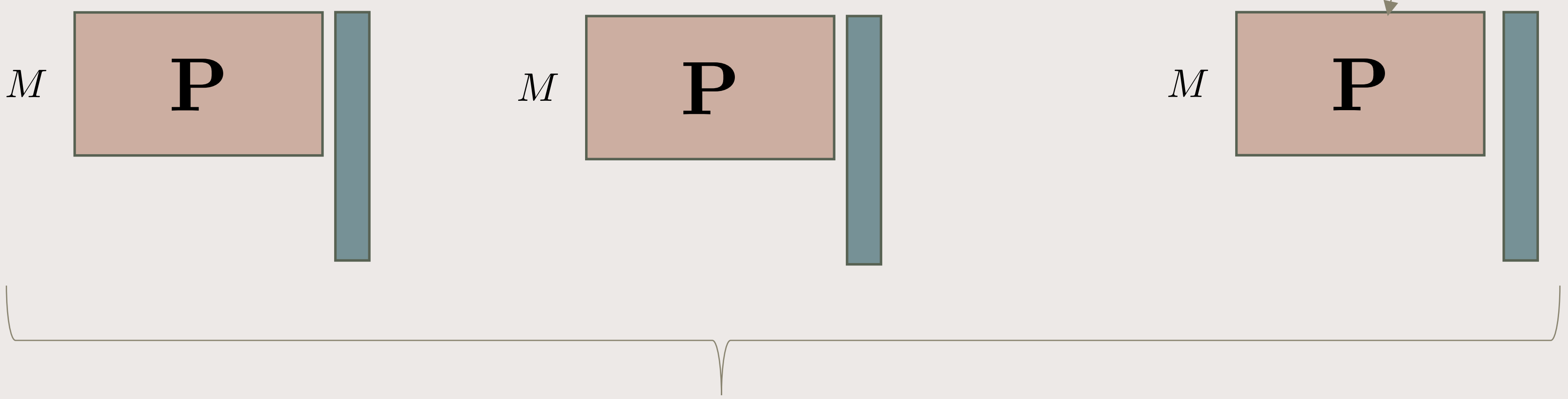
Conjecture



T many linearly independent vectors

CONJECTURE

Entries of $\boldsymbol{P}$ from LWE error distribution (e.g. discrete gaussian).



$T \ll M$. Conjecture is that these vectors remain linearly independent under left-multiplication by $\boldsymbol{P}$.

Provable under entries from uniform dist. and uniform on $[-B, B]$.

THE DQVWW21 CONSTRUCTION APPROACH

[DQVWW21] Construction Approach: Succinct Randomized Encodings (SRE)

[IK00, IK02, AIK04, BGL+15, LPST16, WW21, DQVWW21]

To build $i\mathcal{O}$, it suffices to build SRE.

SRE → $Xi\mathcal{O}$ → $i\mathcal{O}$ [LPST16]

SRE SYNTAX

[IK00, IK02, AIK04, BGL+15, LPST16, WW21, DQVWW21]

To build *iO*, it suffices to build SRE.
SRE → X*iO* → *iO* [LPST16]

$f : \{0,1\}^{\ell} \to \{0,1\}^N$

Correctness: $Enc(f, x) \longrightarrow f(x)$

Security: $\forall x_0, x_1,\ s.t.\ f(x_0) = f(x_1), Enc(f, x_0) \approx_{\mathsf{comp}} Enc(f, x_1)$

Succinctness: $|Enc(f, x)| = O(N^{\delta}), \delta < 1$

SRE FROM SUCCINCT LWE SAMPLING

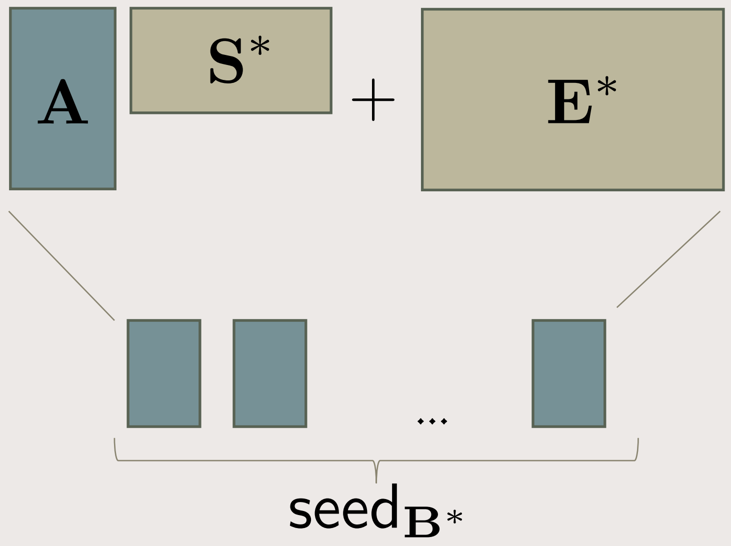
[DQVWW21]

$$f : \{0,1\}^{\ell} \to \{0,1\}^{N}$$

$$Enc(f,x): \quad \underbrace{\mathbf{A}}_{\text{Random matrix.}}\ ,\ \underbrace{\mathbf{C}_x}_{\substack{\text{Homomorphic commitment to } \boldsymbol{x}. \\ \text{(dual GSW)}}}\ ,\ \overbrace{\mathbf{R}_{f,x}}^{\text{Post-evaluation randomness}} + \underbrace{\mathbf{S}^*}_{\text{Random matrix (flooding)}}\ ,\ \underbrace{\overbrace{\square\ \square\ \ldots\ \square}^{\substack{\text{Generates a large pseudorandom LWE} \\ \text{sample of the form } \boldsymbol{B}^* = \boldsymbol{AS}^* + \boldsymbol{E}^*}}}_{\mathsf{seed}_{\mathbf{B}^*}}$$

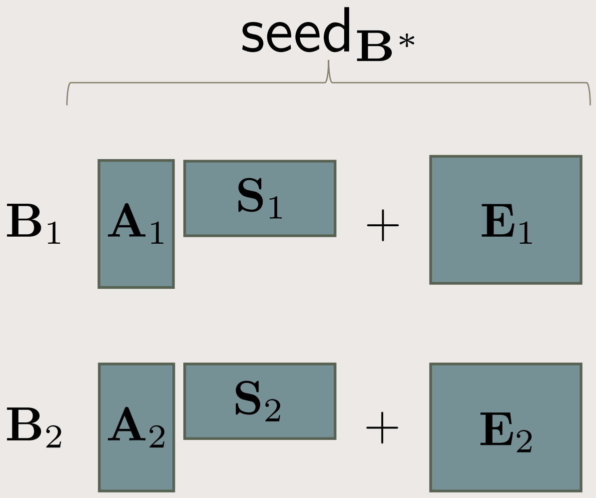
SRE FROM SUCCINCT LWE SAMPLING
[DQVWW21]

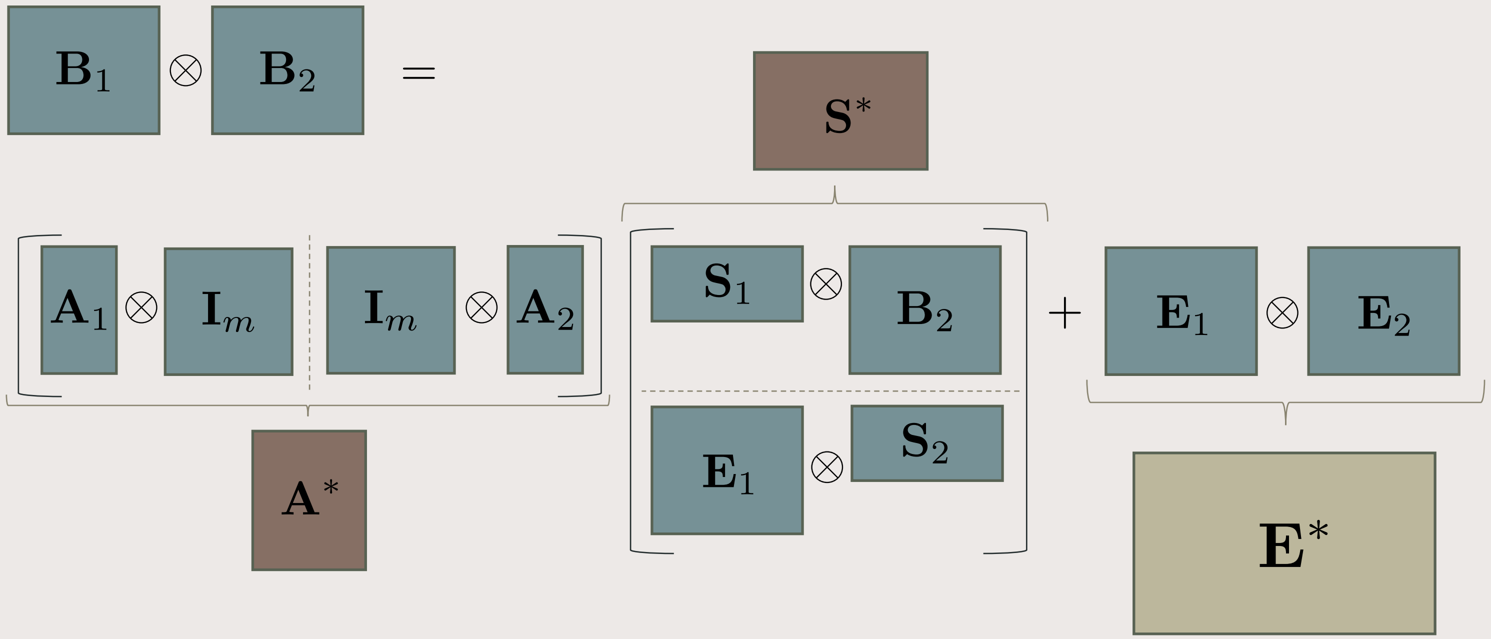
How do you generate a pseudorandom LWE sample?



A Natural Approach: Tensoring

[DQVWW21]





OUR ATTACK (SIMPLIFIED)

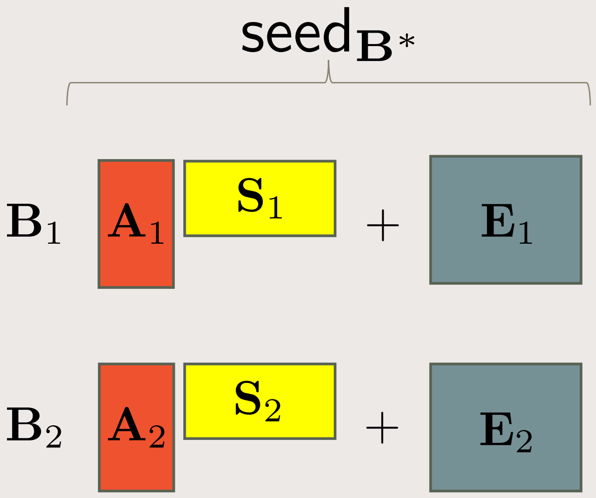
$$\overbrace{\begin{array}{ll} \mathbf{B}_1 & \mathbf{A}_1 \mathbf{S}_1 + \mathbf{E}_1 \\ \mathbf{B}_2 & \mathbf{A}_2 \mathbf{S}_2 + \mathbf{E}_2 \end{array}}^{\text{seed}_{\mathbf{B}^*}}$$

Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^* \boldsymbol{S}^*$. *Do the secrets in the seed remain hidden?*

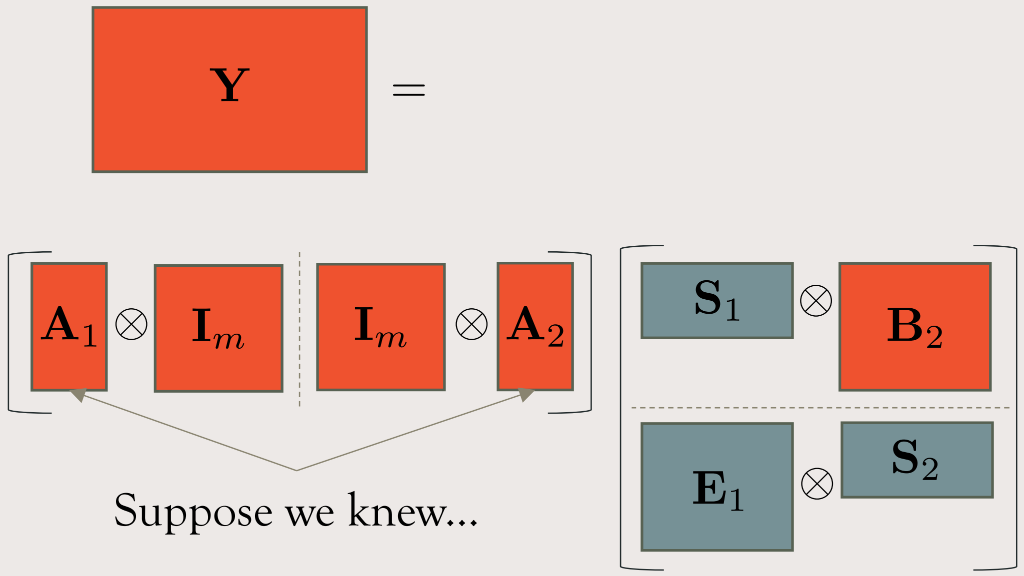
$$\mathbf{Y} = \left[\begin{array}{c:c} \mathbf{A}_1 \otimes \mathbf{I}_m & \mathbf{I}_m \otimes \mathbf{A}_2 \end{array} \right] \left[\begin{array}{c} \mathbf{S}_1 \otimes \mathbf{B}_2 \\ \hdashline \mathbf{E}_1 \otimes \mathbf{S}_2 \end{array} \right]$$

= Known values

OUR ATTACK (SIMPLIFIED)

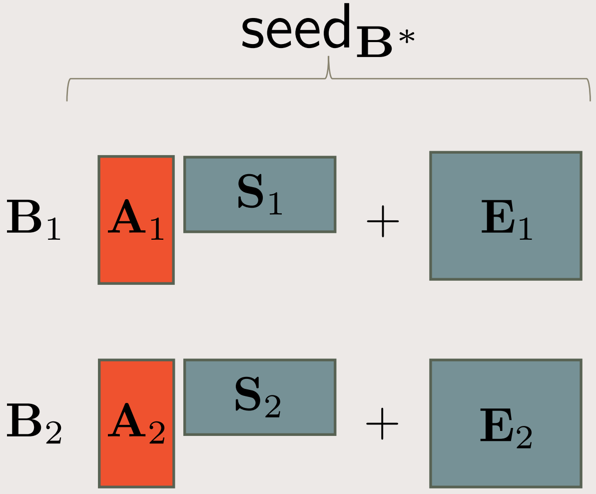


Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^* \boldsymbol{S}^*$. *Do the secrets in the seed remain hidden?*

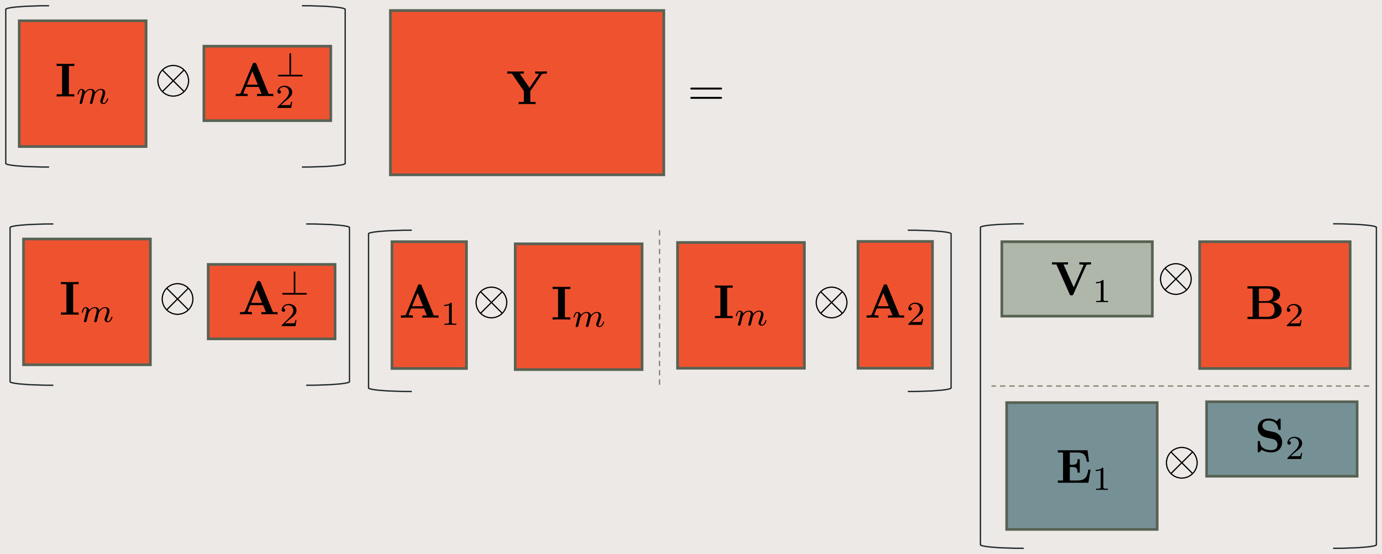


= Known values

OUR ATTACK (SIMPLIFIED)

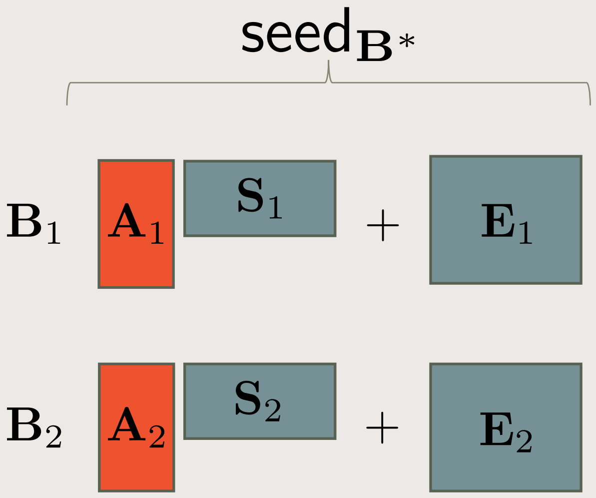


Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^*\boldsymbol{S}^*$ and $\boldsymbol{A_1}, \boldsymbol{A_2}$. Can compute left annihilators!

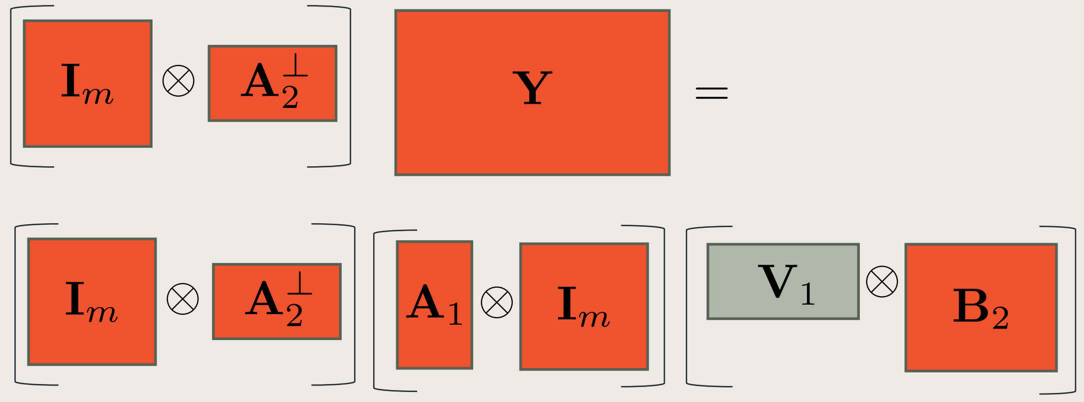


■ = Known values

OUR ATTACK (SIMPLIFIED)



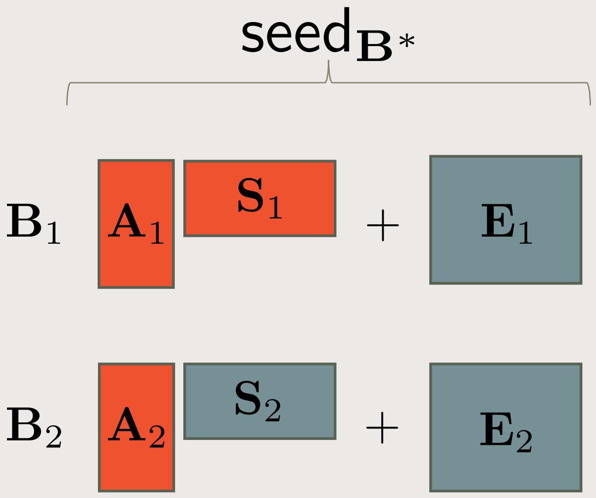
Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^*\boldsymbol{S}^*$ and $\boldsymbol{A_1}, \boldsymbol{A_2}$.



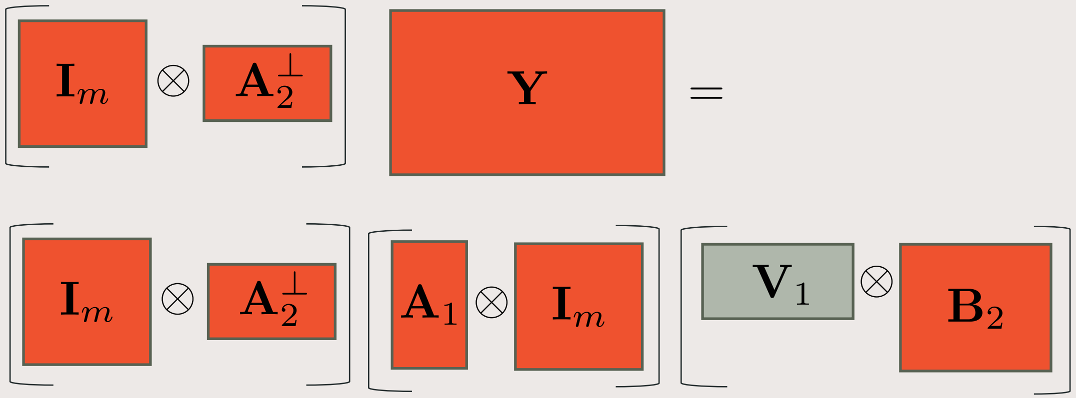
...then we can recover $\mathbf{S}_1$ by solving an affine system of equations

= Known values

OUR ATTACK (SIMPLIFIED)



Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^*\boldsymbol{S}^*$ and $\boldsymbol{A_1}, \boldsymbol{A_2}$.



...then we can recover $\mathbf{S}_1$ by solving an affine system of equations

= Known values

OUR ATTACK (SIMPLIFIED)

$$\overbrace{\mathbf{B}_1 \quad \cancel{\mathbf{A}_1 \mathbf{S}_1} + \mathbf{E}_1}^{\text{seed}_{\mathbf{B}^*}}$$

...and we can recover $\mathbf{E}_1$

$$\mathbf{B}_2 \quad \mathbf{A}_2 \mathbf{S}_2 + \mathbf{E}_2$$

Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^* \boldsymbol{S}^*$ and $\boldsymbol{A}_1, \boldsymbol{A}_2$.

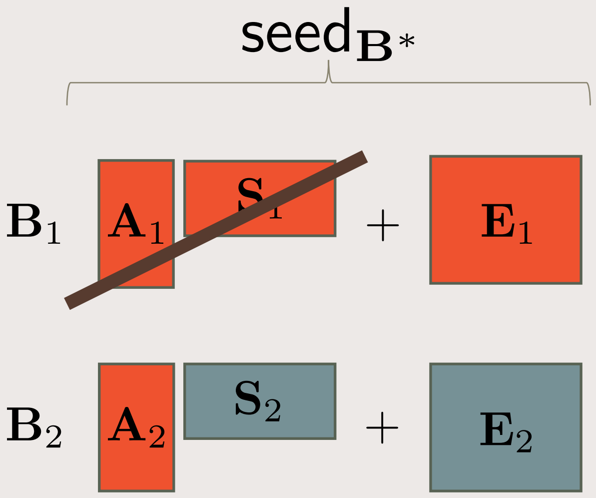
$$\left[\mathbf{I}_m \otimes \mathbf{A}_2^{\perp}\right] \mathbf{Y} =$$

$$\left[\mathbf{I}_m \otimes \mathbf{A}_2^{\perp}\right] \left[\mathbf{A}_1 \otimes \mathbf{I}_m\right] \left[\mathbf{V}_1 \otimes \mathbf{B}_2\right]$$

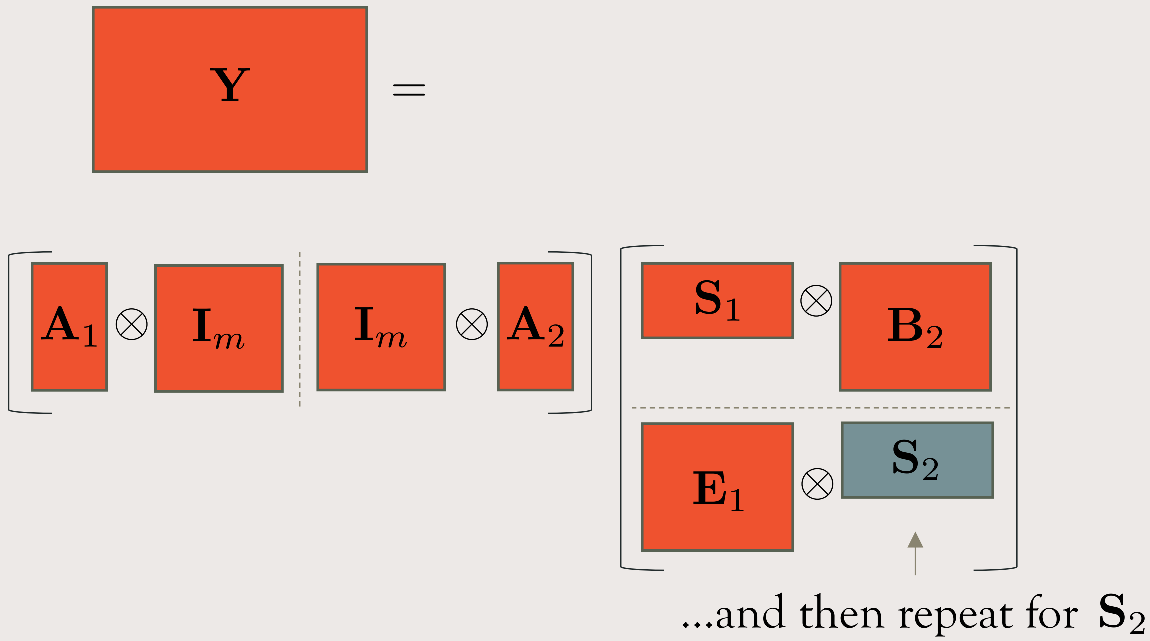
...then we can recover $\mathbf{S}_1$ by solving an affine system of equations

= Known values

OUR ATTACK (SIMPLIFIED)

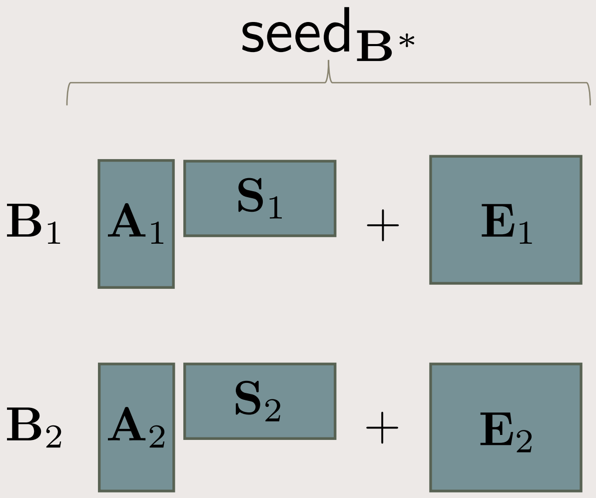


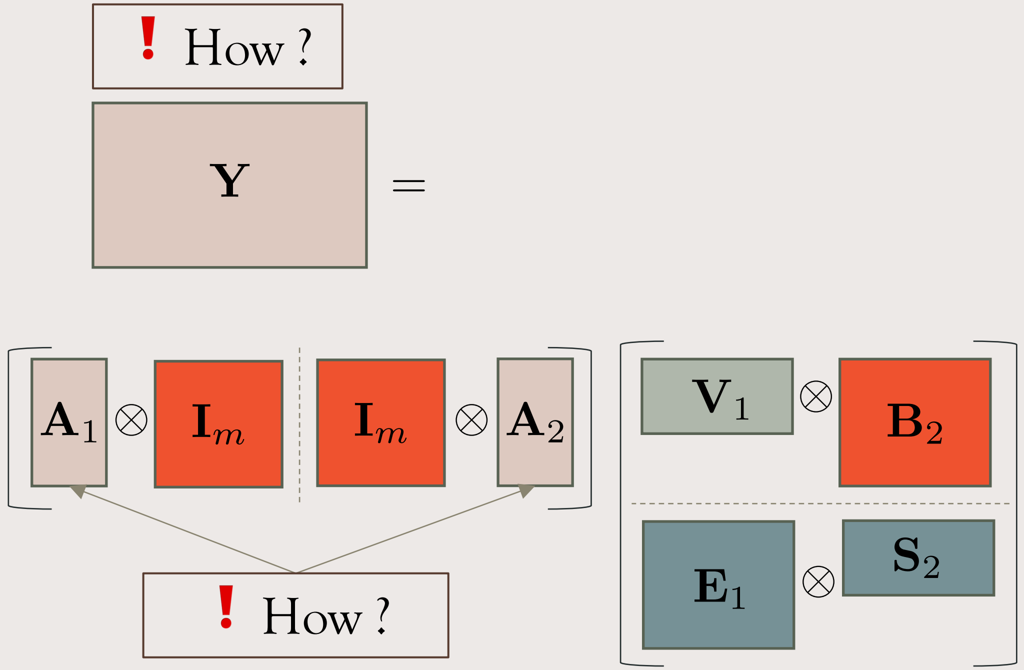
Suppose we knew $\boldsymbol{Y} \triangleq \boldsymbol{A}^*\boldsymbol{S}^*$ and $\boldsymbol{A_1}, \boldsymbol{A_2}$.



$=$ Known values

Our attack (simplified)

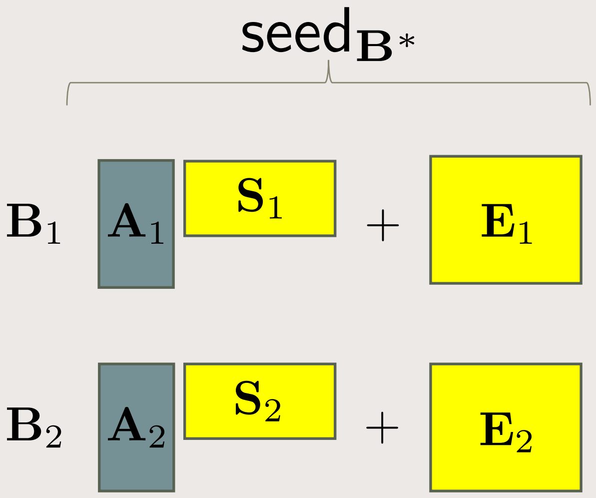


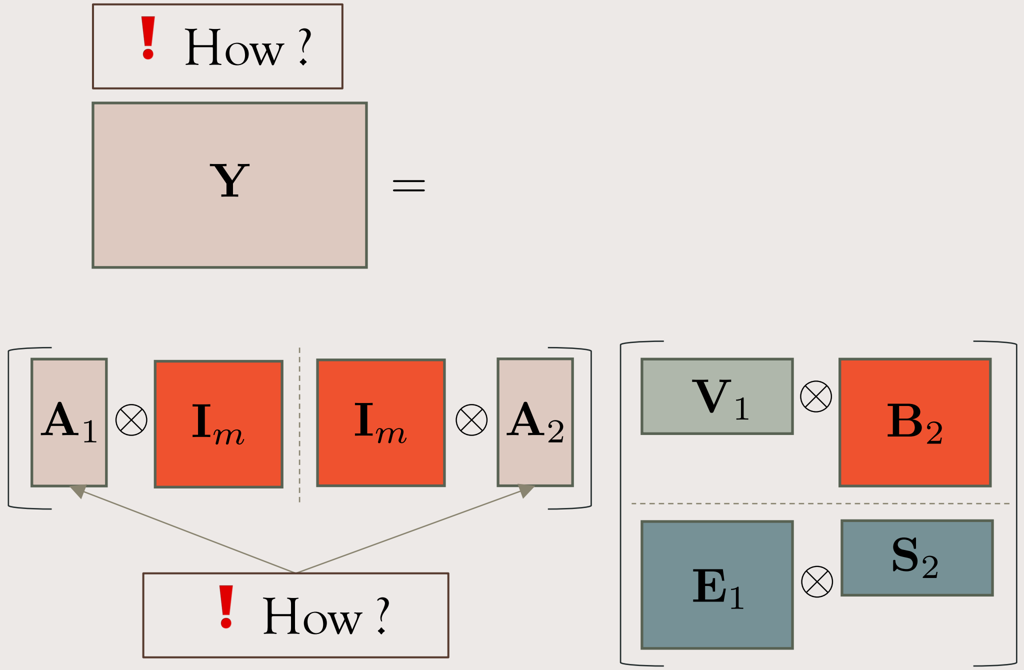


If we knew these values, we'd be able to recover the error terms in the seed!

= Known values

OUR ATTACK (SIMPLIFIED)



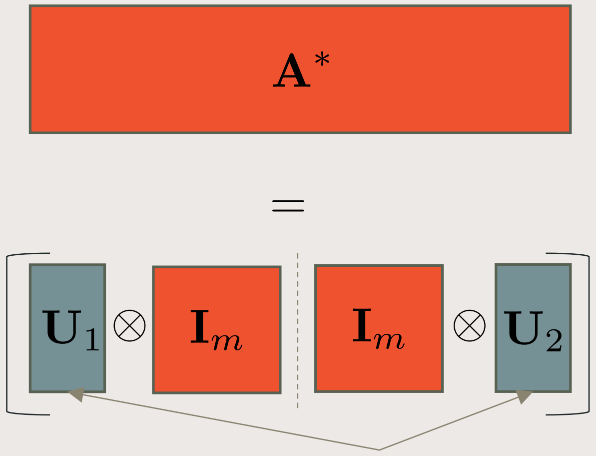


= Known values

Intended attack to recover components:

1. Recover A_1, A_2.
2. Compute $Y = A^* S^*$.
3. Recover S_1.
4. Repeat for next index.

Unique Representations (Simplified)



Can you recover the components $\boldsymbol{A}_1, \boldsymbol{A}_2$ from $\boldsymbol{A}^*$?

= Known values

UNIQUE REPRESENTATIONS (SIMPLIFIED)

Hypothetical Constraints

$$\overbrace{\hspace{6cm}}^{\mathsf{seed}_{\mathbf{B}^*}}$$

$$\mathbf{B}_1 \quad \mathbf{U}_1 \mathbf{V}_1 + \mathbf{E}_1$$

$$\mathbf{B}_2 \quad \mathbf{U}_2 \mathbf{V}_2 + \mathbf{E}_2$$

Equations

$$\mathbf{A}^* = \left[\mathbf{U}_1 \otimes \mathbf{I}_m \;\middle|\; \mathbf{I}_m \otimes \mathbf{U}_2 \right]$$

- Many possible solutions.
- **A unique solution** is necessary to recover a unique secret.

■ = Known values

Unique representations of A_i (simplified)

Hypothetical Constraints

$$\overbrace{\begin{array}{l} \mathbf{B}_1 \quad \mathbf{U}_1 \mathbf{V}_1 + \mathbf{E}_1 \\ \mathbf{B}_2 \quad \mathbf{U}_2 \mathbf{V}_2 + \mathbf{E}_2 \end{array}}^{\mathsf{seed}_{\mathbf{B}^*}}$$

Equations

$$\mathbf{A}^* = \left[\mathbf{U}_1 \otimes \mathbf{I}_m \;\middle|\; \mathbf{I}_m \otimes \mathbf{U}_2 \right]$$

A possible solution to U_1:

$$\mathbf{A}_1$$

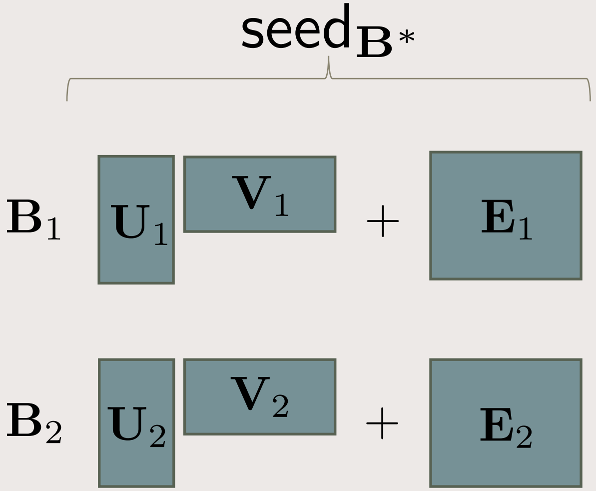
Corresponding V_1 solution:

$$\mathbf{S}_1$$

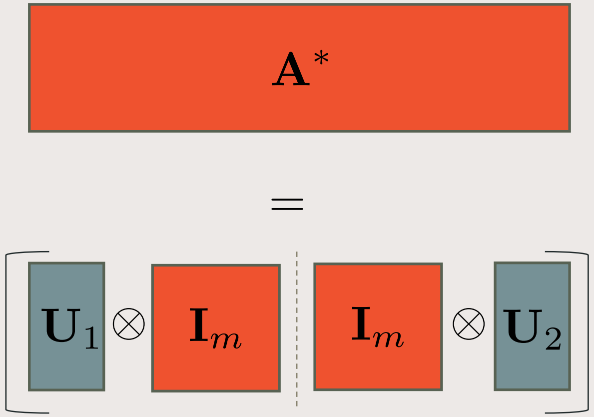
$\blacksquare$ = Known values

UNIQUE REPRESENTATIONS OF A_i (SIMPLIFIED)

Hypothetical Constraints

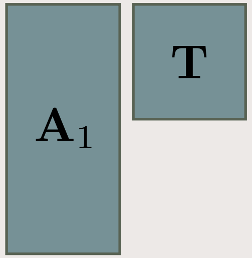


Equations



$=$ Known values

A possible solution to U_1:



Corresponding V_1 solution:

Unique Representations of A_i (Simplified)

Hypothetical Constraints

$$\overbrace{\begin{aligned} \mathbf{B}_1 &= \mathbf{U}_1 \mathbf{V}_1 + \mathbf{E}_1 \\ \mathbf{B}_2 &= \mathbf{U}_2 \mathbf{V}_2 + \mathbf{E}_2 \end{aligned}}^{\mathsf{seed}_{\mathbf{B}^*}}$$

Equations

$$\mathbf{A}^* = \left[\, \mathbf{U}_1 \otimes \mathbf{I}_m \;\middle|\; \mathbf{I}_m \otimes \mathbf{U}_2 \,\right]$$

$\blacksquare$ = Known values

A possible solution to U_1:

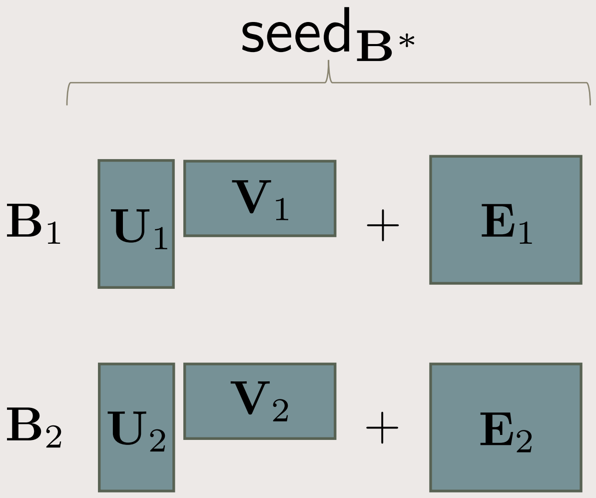
$$\begin{bmatrix} \mathbf{A}_{1,\top} \\ \mathbf{A}_{1,\perp} \end{bmatrix} \mathbf{T}$$

Corresponding V_1 solution:

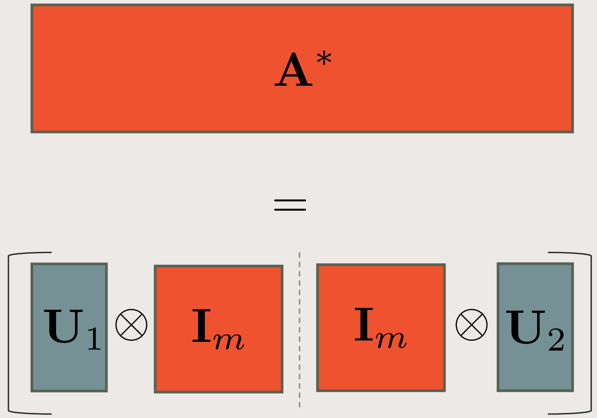
$$\begin{bmatrix} \mathbf{T}^{-1} & \mathbf{S}_1 \end{bmatrix}$$

UNIQUE REPRESENTATIONS OF A_i (SIMPLIFIED)

Hypothetical Constraints

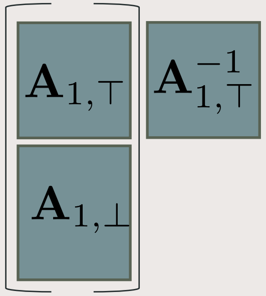


Equations



= Known values

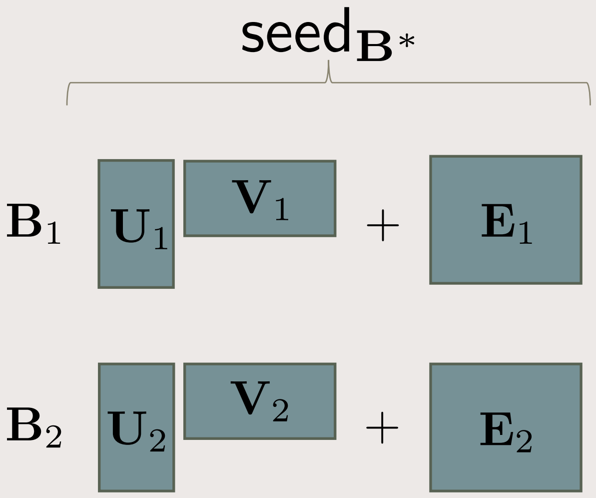
A possible solution to U_1:



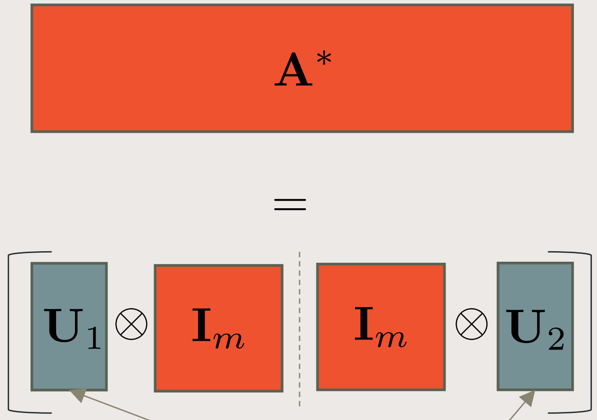
Corresponding V_1 solution:

UNIQUE REPRESENTATIONS OF A_i (SIMPLIFIED)

Hypothetical Constraints



Equations



For uniqueness, insist on a solution of the form: $\mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix}$

= Known values

UNIQUE REPRESENTATIONS OF A_i (SIMPLIFIED)

Hypothetical Constraints

$$\overbrace{\begin{array}{l} \mathbf{B}_1 \quad \mathbf{U}_1 \mathbf{V}_1 + \mathbf{E}_1 \\ \mathbf{B}_2 \quad \mathbf{U}_2 \mathbf{V}_2 + \mathbf{E}_2 \end{array}}^{\mathsf{seed}_{\mathbf{B}^*}}$$

Equations

$$\mathbf{A}^* = \left[\begin{array}{c|c} \mathbf{U}_1 \otimes \mathbf{I}_m & \mathbf{I}_m \otimes \mathbf{U}_2 \end{array}\right]$$

For uniqueness, insist on a solution of the form: $\mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix}$

Intended solution to U_1, V_1:

$$\begin{bmatrix} \mathbf{A}_{1,\top} \\ \mathbf{A}_{1,\perp} \end{bmatrix} \mathbf{A}_{1,\top}^{-1} \quad \mathbf{A}_{1,\top} \, \mathbf{S}_1$$

$$= \mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix}$$

■ = Known values

UNIQUE REPRESENTATIONS OF A_i (SIMPLIFIED)

Hypothetical Constraints

$$\underbrace{\begin{aligned}\mathbf{B}_1 &= \mathbf{U}_1\mathbf{V}_1 + \mathbf{E}_1\\ \mathbf{B}_2 &= \mathbf{U}_2\mathbf{V}_2 + \mathbf{E}_2\end{aligned}}_{\text{seed}_{\mathbf{B}^*}}$$

Equations

$$\mathbf{A}^* = \left[\,\mathbf{U}_1 \otimes \mathbf{I}_m \;\middle|\; \mathbf{I}_m \otimes \mathbf{U}_2\,\right]$$

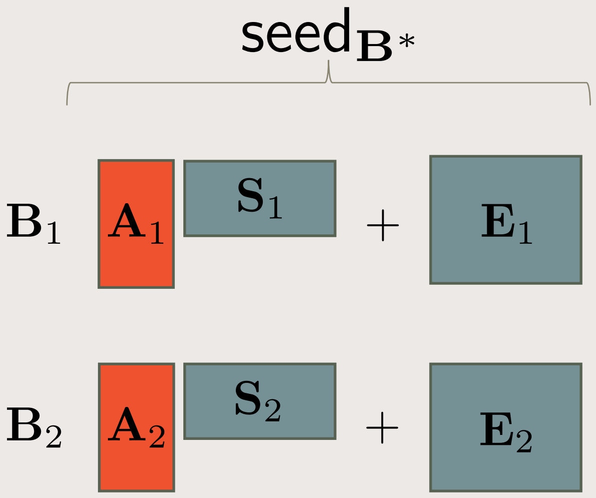
To prove uniqueness, we use a linear independence argument made possible by both the tensoring and the structure of the solutions.

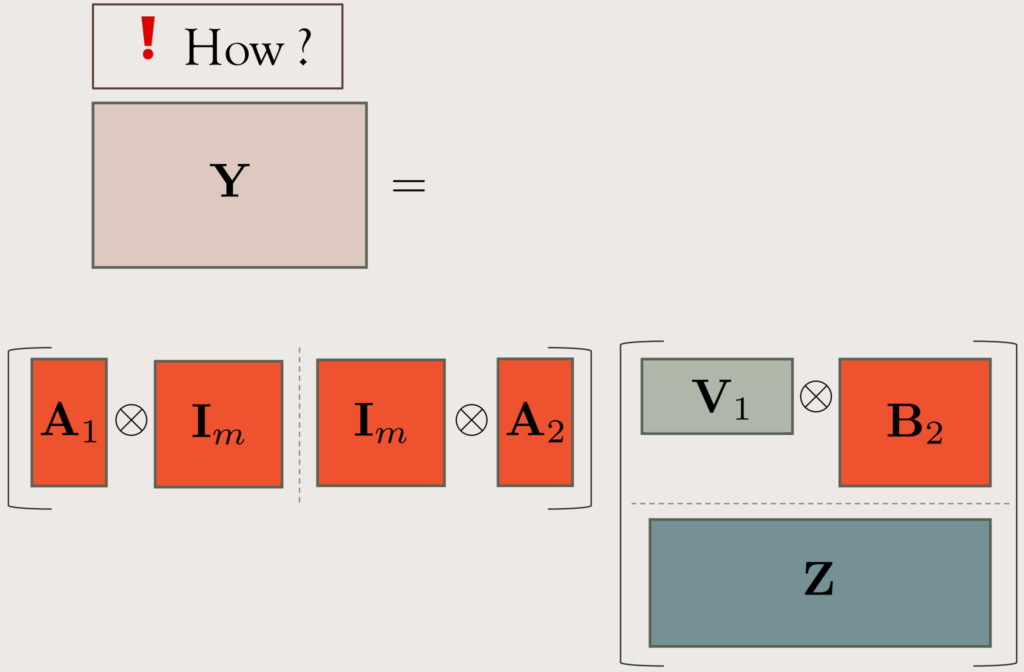
For uniqueness, insist on a solution of the form:

$$\mathbf{U}_1 = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix}$$

= Known values

OUR ATTACK (SIMPLIFIED)



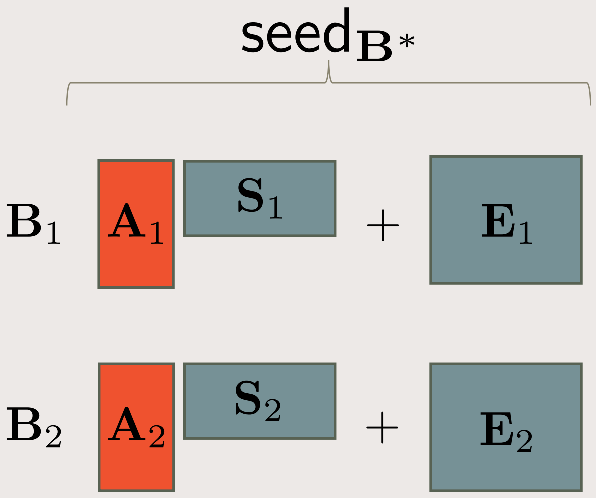


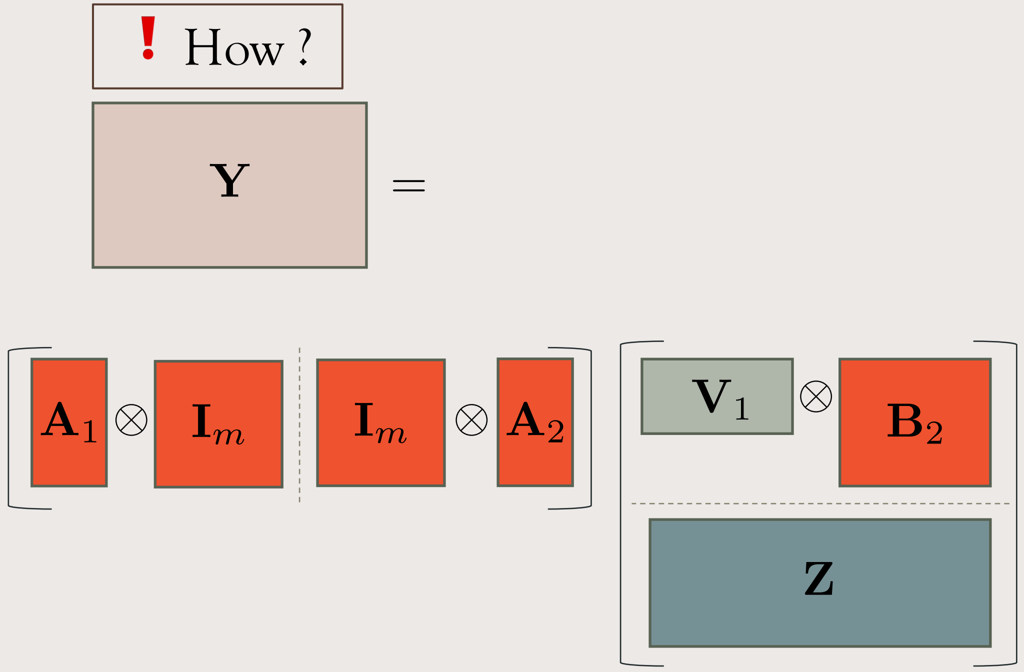
= Known values

✓ Recover A_1, A_2 up to unique representation.

2. Compute $Y = A^* S^*$?
3. Recover S_1 up to unique representation.

OUR ATTACK (SIMPLIFIED)





From the givens, we can compute:

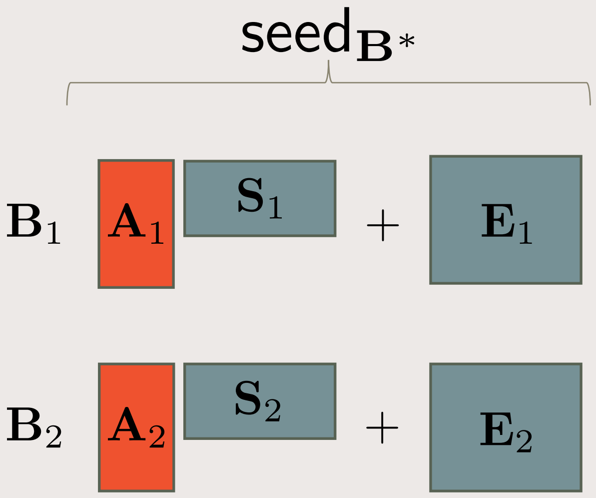
$$\mathbf{Y}' = \mathbf{A}^* \cdot (\mathbf{S}^* + \mathbf{R} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}))$$

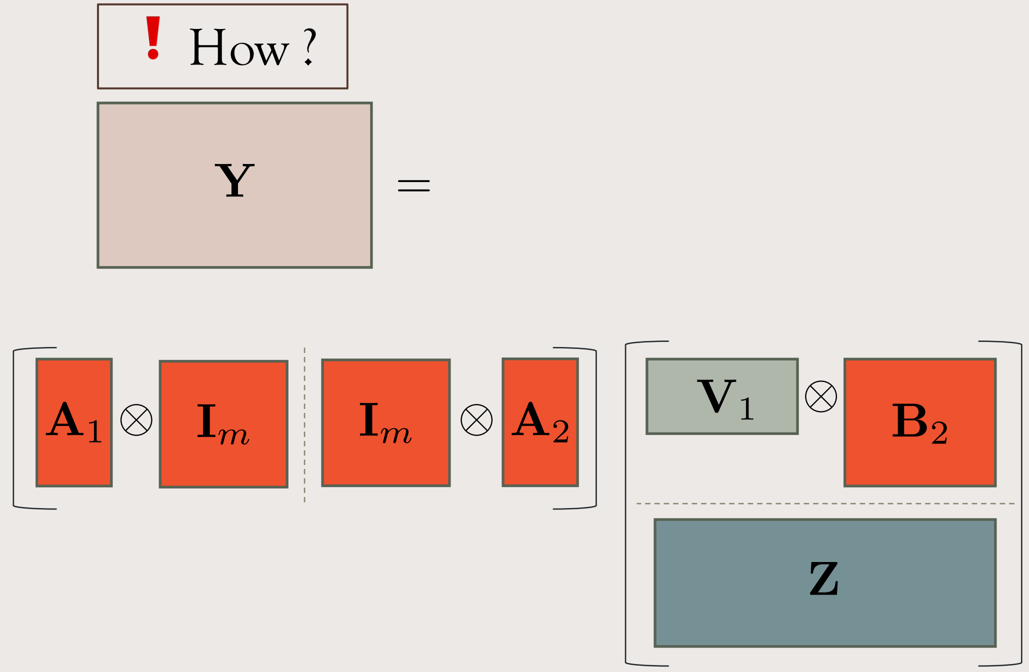
= Known values

✓ Recover A_1, A_2 up to unique representation.

2. Compute $Y = A^* S^*$?
3. Recover S_1 up to unique representation.

OUR ATTACK (SIMPLIFIED)





From the givens, we can compute:

$$\mathbf{Y}' = \mathbf{A}^* \cdot (\mathbf{S}^* \boxed{+ \mathbf{R} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}))}$$

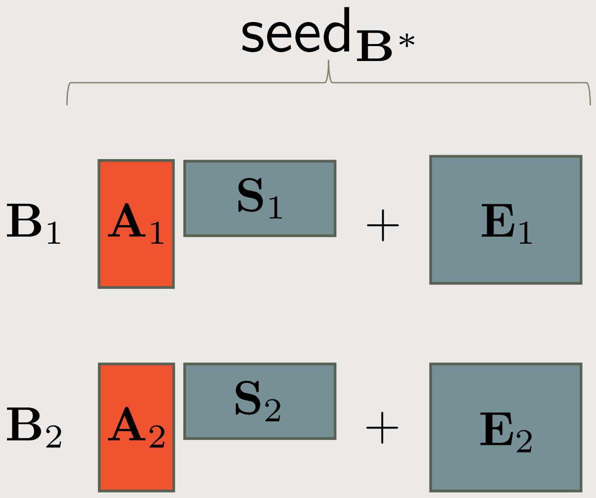
= Known values

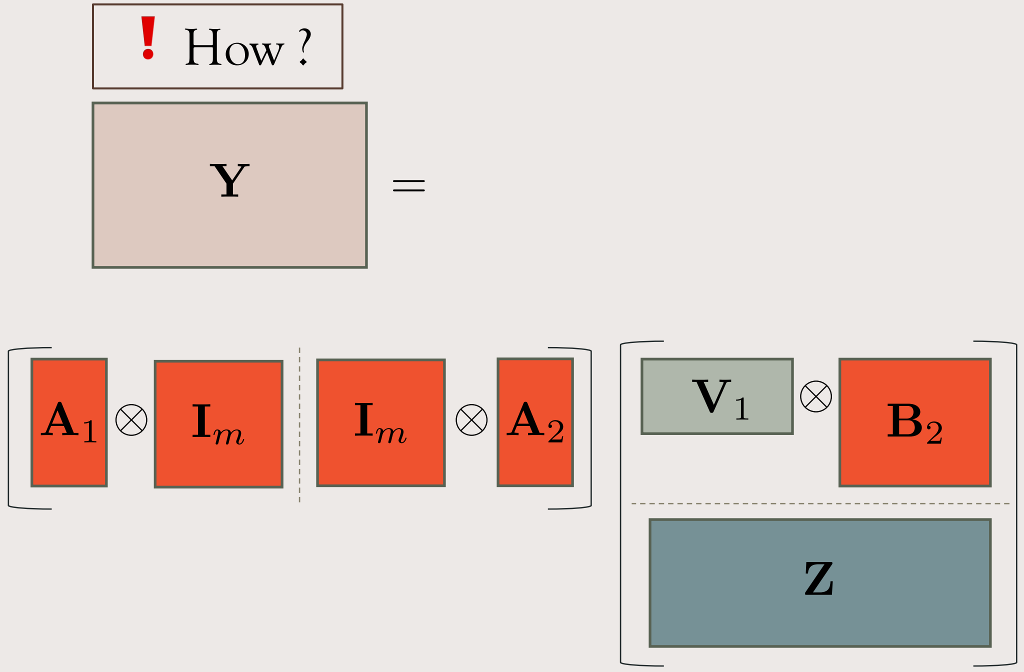
✓ Recover A_1, A_2 up to unique representation.

2. Compute $Y = A^* S^*$?
3. Recover S_1 up to unique representation.

Compute right annihilator $\mathbf{Q}$ for $\mathbf{G}^{-1}(\widehat{\mathbf{B}})$

OUR ATTACK (SIMPLIFIED)





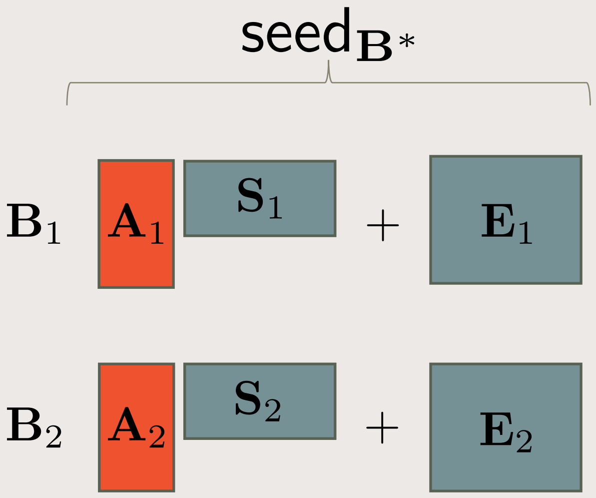
From the givens, we can compute:

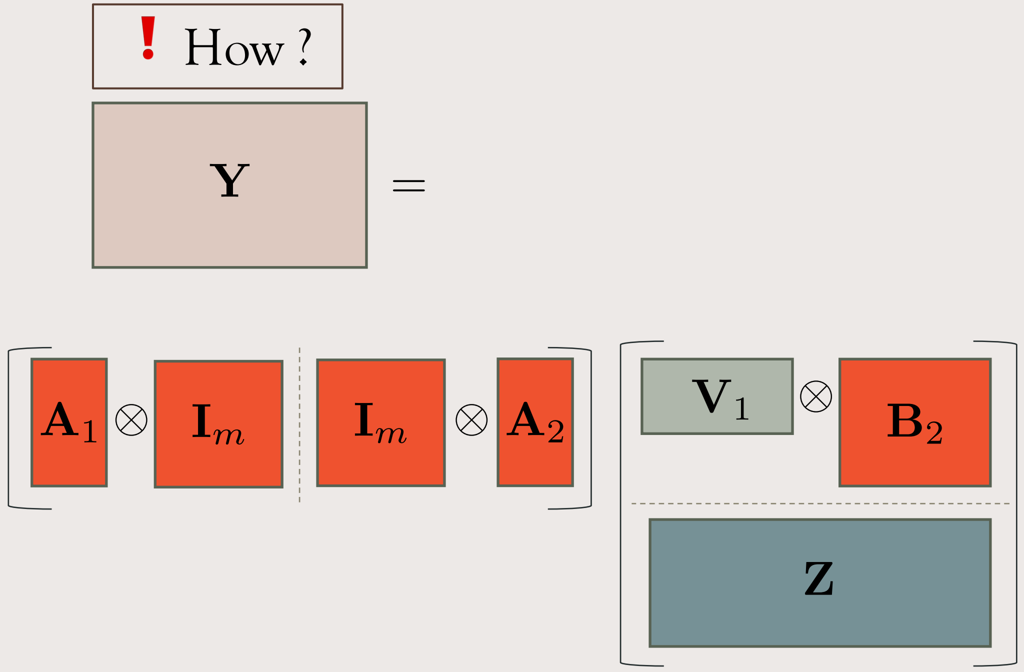
$$\mathbf{Y}' \cdot \mathbf{Q} = \mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q}$$

= Known values

✓ Recover A_1, A_2 up to unique representation.
2. Compute $Y = A^* S^* Q$.
3. Recover S_1 up to unique representation.

OUR ATTACK (SIMPLIFIED)





From the givens, we can compute:

$$\mathbf{Y}' \cdot \mathbf{Q} = \mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q}$$

= Known values

- ✓ Recover A_1, A_2 up to unique representation.
- ✓ Compute $Y = A^* S^* Q$.
- 3. Recover S_1 up to unique representation.

OUR ATTACK (SIMPLIFIED)

$$\overbrace{\begin{aligned}\mathbf{B}_1 &= \mathbf{A}_1\mathbf{S}_1 + \mathbf{E}_1\\ \mathbf{B}_2 &= \mathbf{A}_2\mathbf{S}_2 + \mathbf{E}_2\end{aligned}}^{\text{seed}_{\mathbf{B}^*}}$$

$$\mathbf{Y} = \left[\mathbf{A}_1 \otimes \mathbf{I}_m \;\middle|\; \mathbf{I}_m \otimes \mathbf{A}_2\right] \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}_2 \\ \hline \mathbf{Z} \end{bmatrix} \mathbf{Q}$$

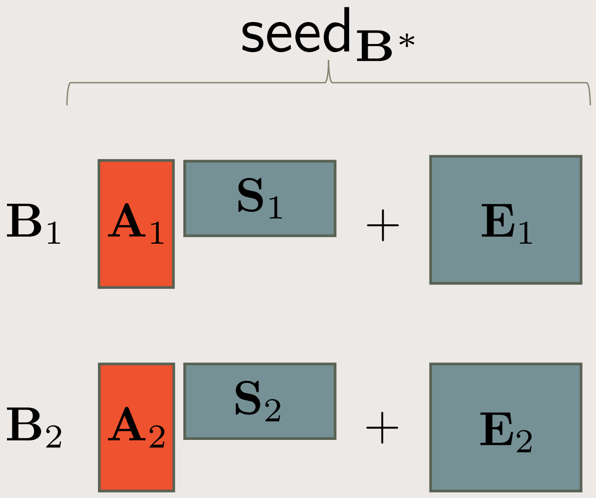
From the givens, we can compute:

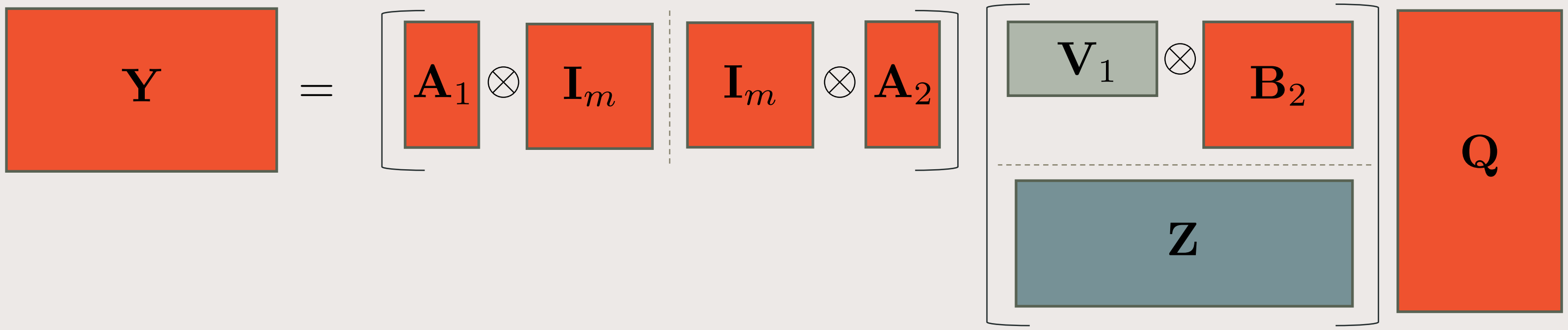
$$\mathbf{Y}' \cdot \mathbf{Q} = \mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q}$$

= Known values

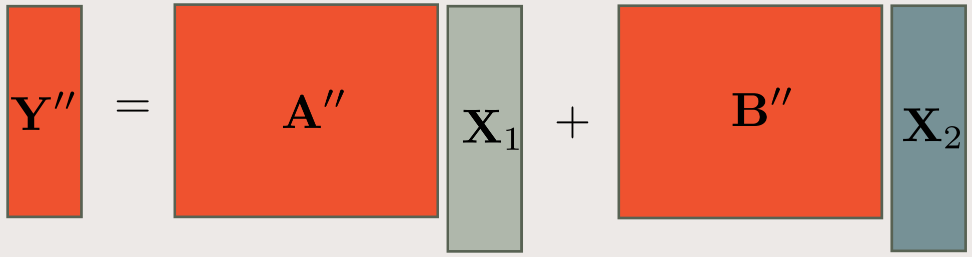
✓ Recover A_1, A_2 up to unique representation.
✓ Compute $Y = A^* S^* Q$.
3. Recover S_1 up to unique representation.

OUR ATTACK (SIMPLIFIED)





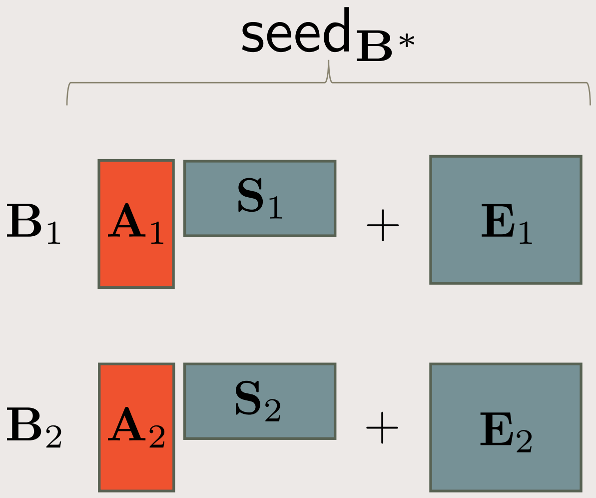
Expand above:

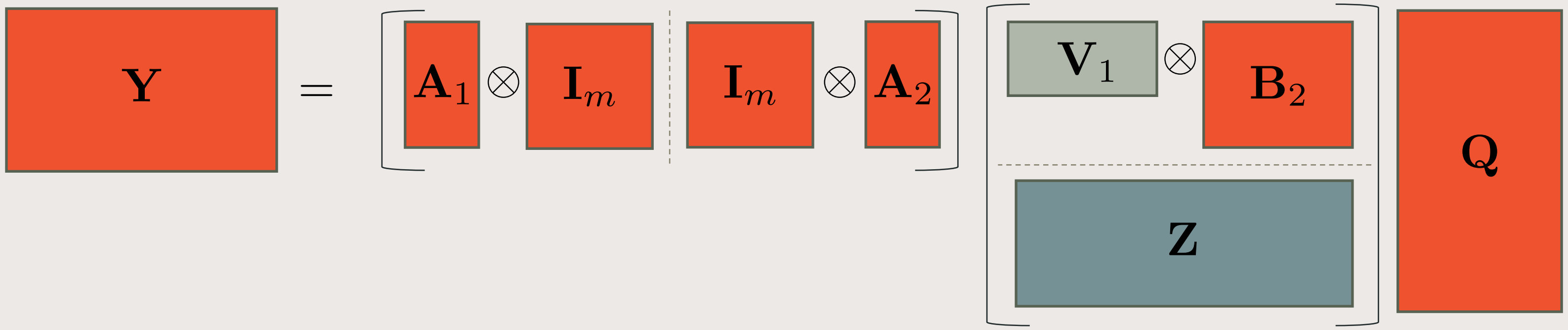


= Known values

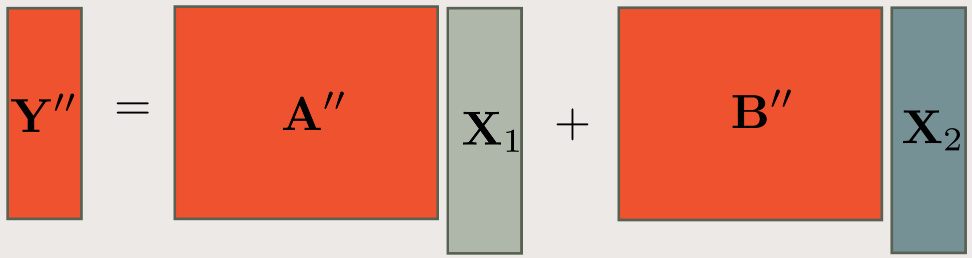
- ✓ Recover A_1, A_2 up to unique representation.
- ✓ Compute $Y = A^* S^* Q$.
- ✓ Recover S_1 up to unique representation.

OUR ATTACK (SIMPLIFIED)





Generically, want to show that X_1 has unique solutions:



...involves analyzing overlap in column span of A'' and B''

- ✓ Recover A_1, A_2 up to unique representation.
- ✓ Compute $Y = A^* S^* Q$.
- ✓ Recover S_1 up to unique representation.

= Known values

Breaking the FULL assumption

$$\mathbf{P}, \mathbf{P}', \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \widehat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}, \mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}) - b\mathbf{F}$$

Several randomization tricks were used in the construction in [DQVWW21].

BREAKING THE FULL ASSUMPTION

$$\mathbf{P}, \mathbf{P}', \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \widehat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}, \mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}) - b\mathbf{F}$$

Several randomization tricks were used in the construction in [DQVWW21].

Final Remark 1: Under a reasonable conjecture on **P** preserving rank of small subspaces**,** the toy analysis given extends to when **P** and **P'** are present.

BREAKING THE FULL ASSUMPTION

$$\mathbf{P}, \mathbf{P}', \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \widehat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}, \mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}) - b\mathbf{F}$$

Several randomization tricks were used in the construction in [DQVWW21].

Final Remark 1: Under a reasonable conjecture on **P** preserving rank of small subspaces**,** the toy analysis given extends to when **P** and **P'** are present.

Final Remark 2: We show that Kilian randomization on $\boldsymbol{A}^*, \boldsymbol{S}^*$ does not hide the tensor structure.

BREAKING THE FULL ASSUMPTION

$$\mathbf{P}, \mathbf{P}', \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \widehat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}, \mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\widehat{\mathbf{B}}) - b\mathbf{F}$$

Several randomization tricks were used in the construction in [DQVWW21].

Final Remark 1: Under a reasonable conjecture on **P** preserving rank of small subspaces, the toy analysis given extends to when **P** and **P'** are present.

Final Remark 2: We show that Kilian randomization on $\boldsymbol{A}^*, \boldsymbol{S}^*$ does not hide the tensor structure.

Final Remark 3: We show that the attack extends to the "*T*-sum" candidate construction in [DQVWW21]

THANK YOU!