Post-Quantum PKE from Unstructured Noisy Linear Algebraic Assumptions: Beyond LWE and Alekhnovich's LPN

Riddhi Ghosal
UCLA

Aayush Jain
CMU

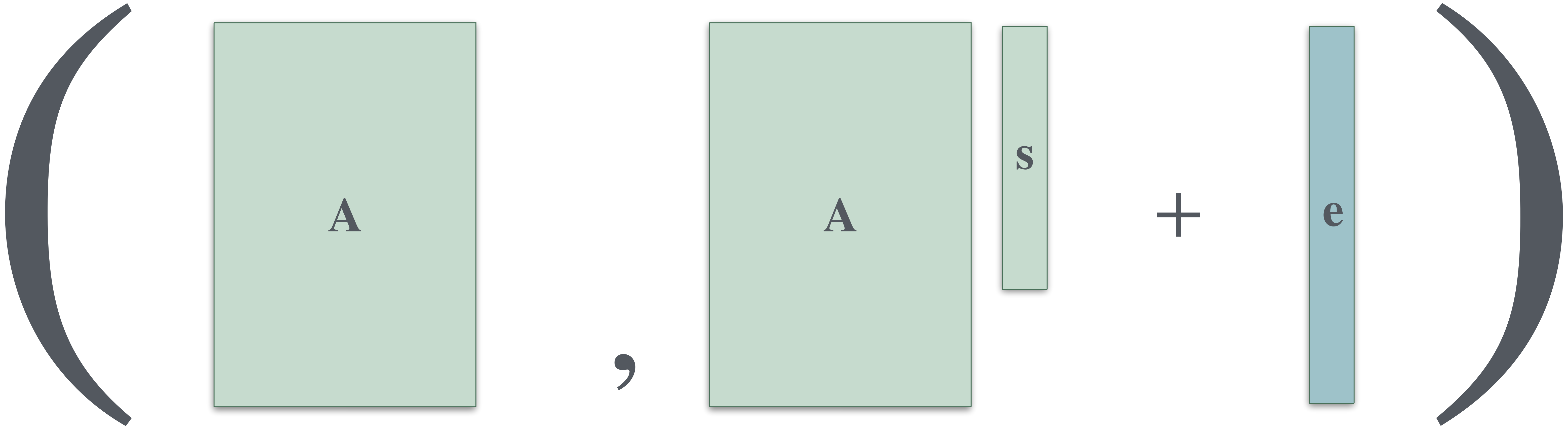
Paul Lou
UCLA

Amit Sahai
UCLA

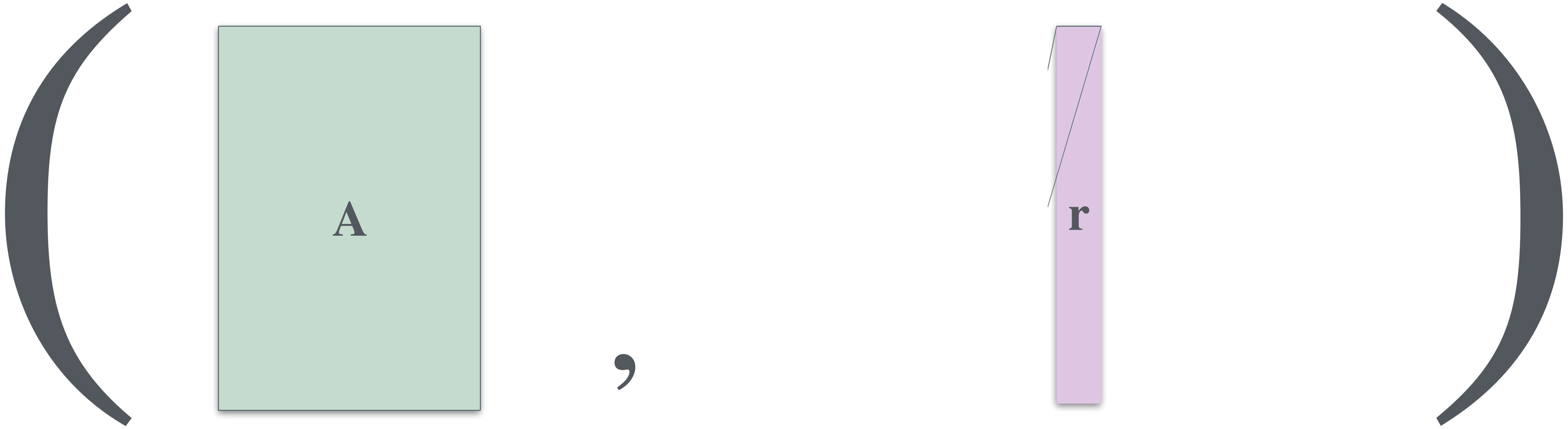
Neekon Vafa
MIT

Presentation adopted from Paul Lou's slides

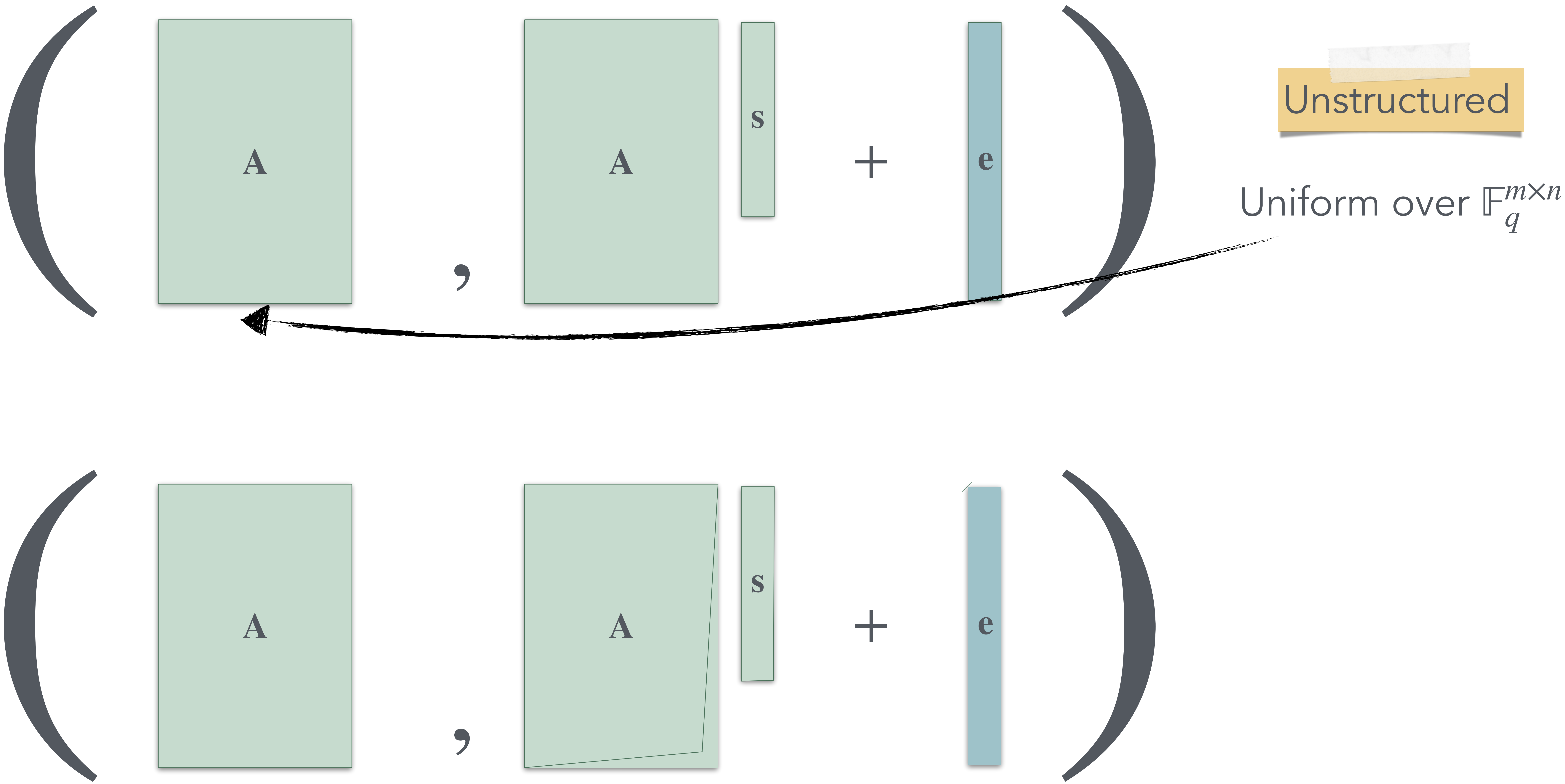
Noisy Linear Algebraic Assumptions (NLA)



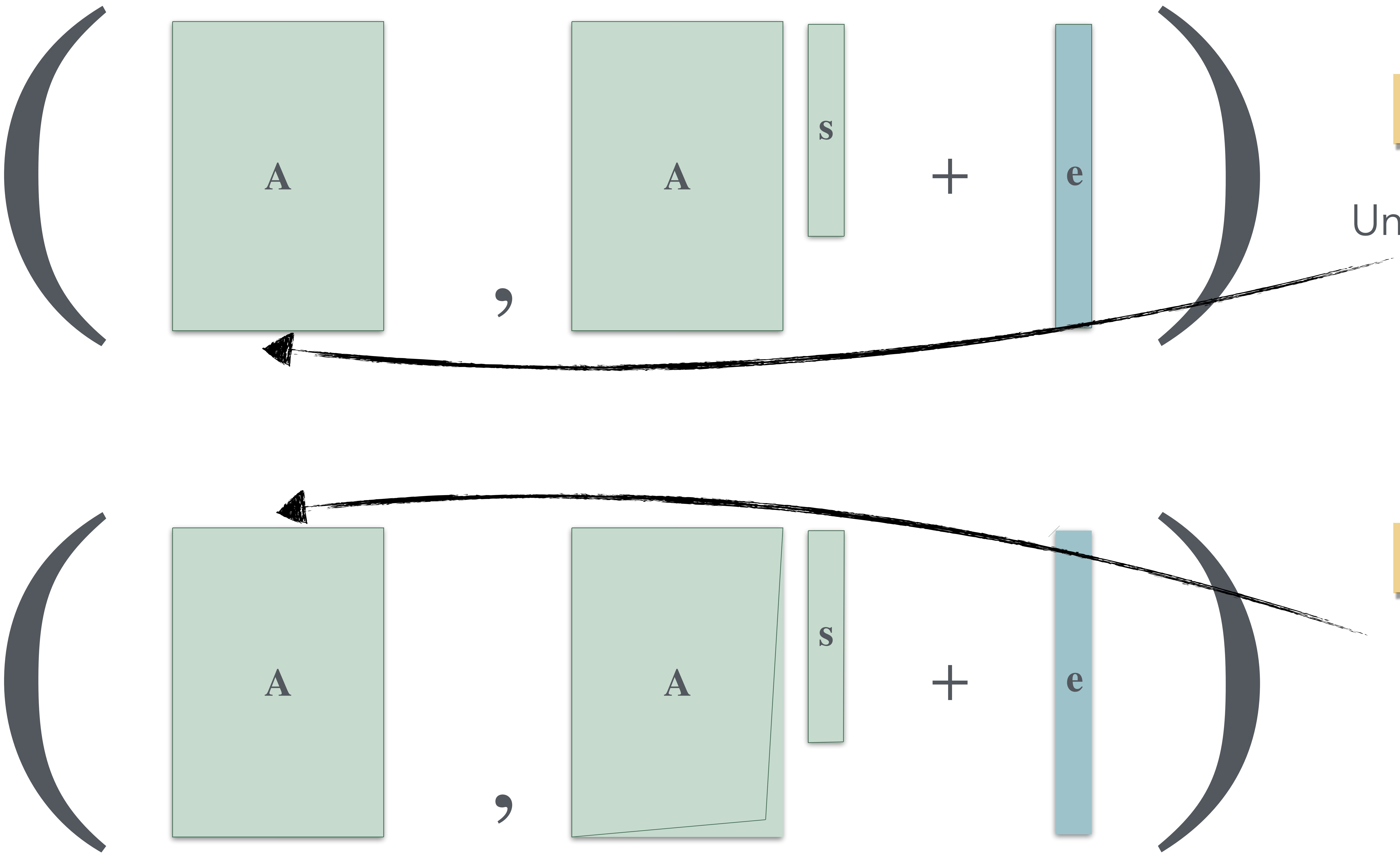
is computationally indistinguishable from



Noisy Linear Algebraic Assumptions (NLA)



Noisy Linear Algebraic Assumptions (NLA)



Unstructured

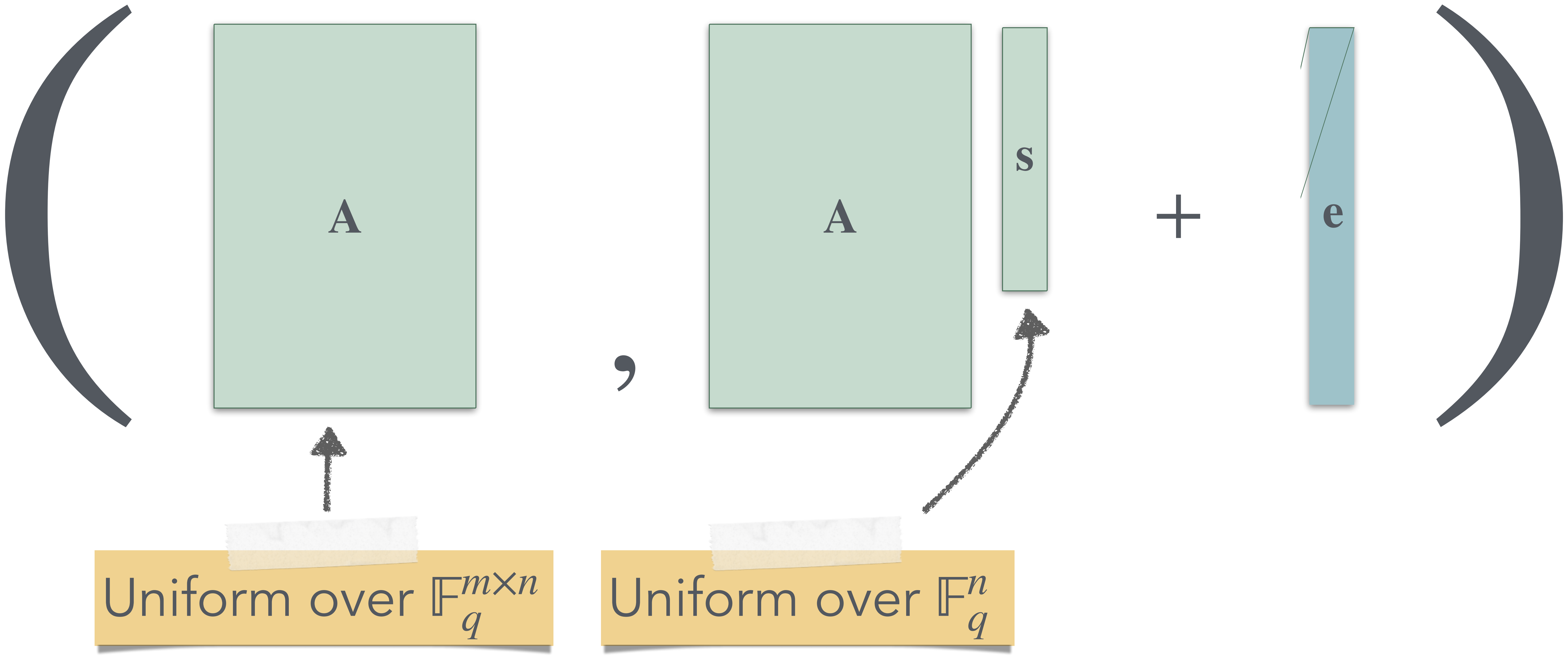
Uniform over $\mathbb{F}_q^{m \times n}$

Structured

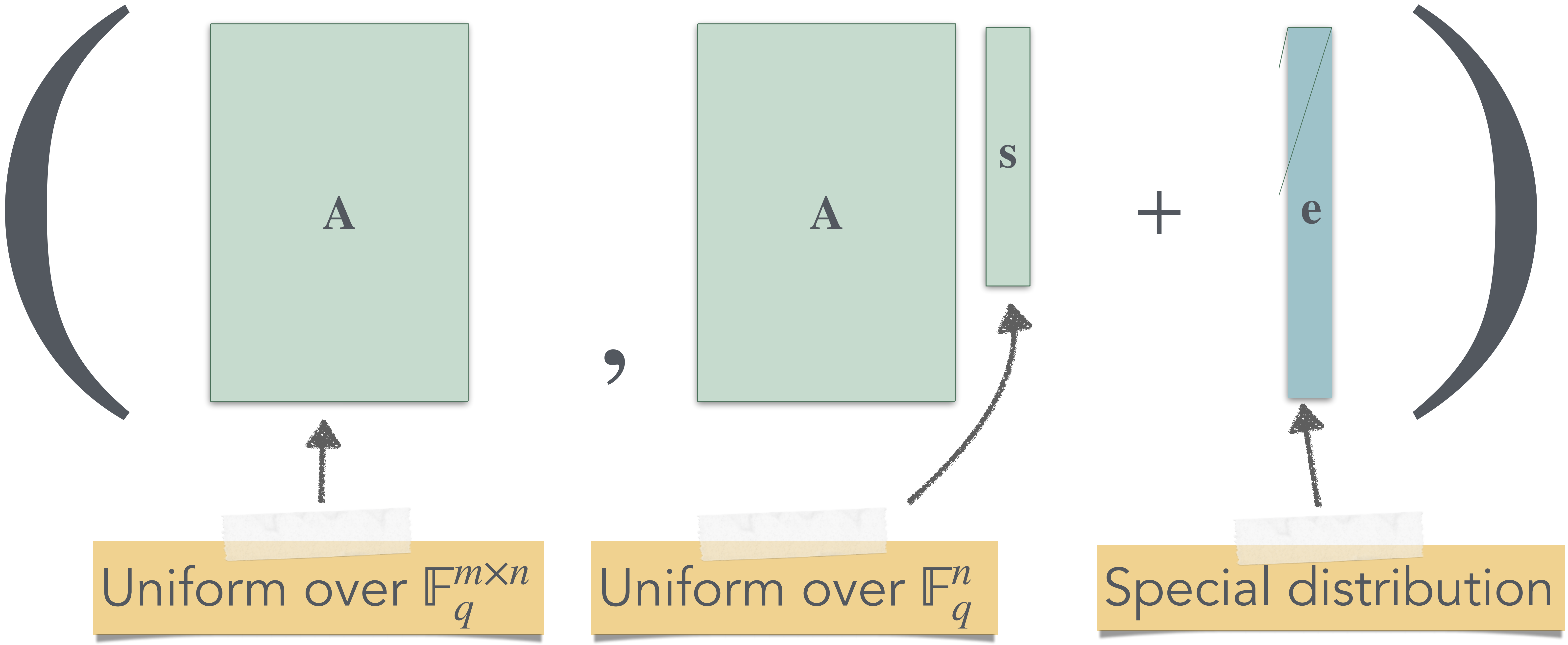
Non-uniform

- Classic McEliece

Unstructured Noisy Linear Algebraic Assumptions (NLA)



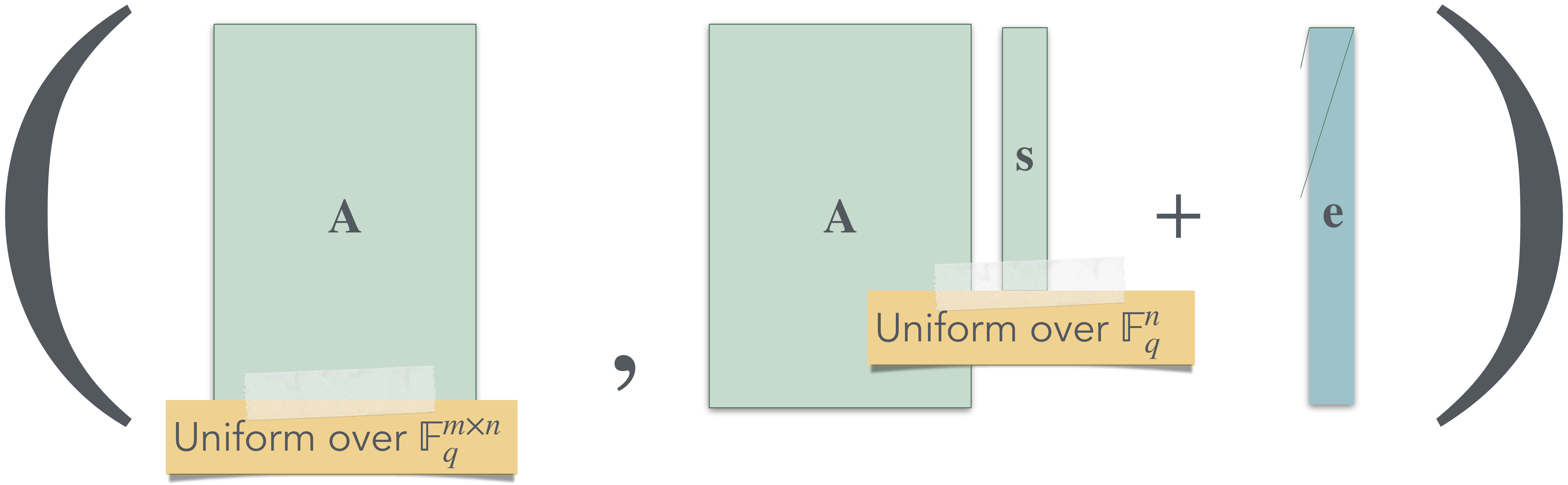
Unstructured Noisy Linear Algebraic Assumptions (NLA)



Learning with Errors (LWE): Small error (Discrete Gaussian)
(Lattice based)

Learning Parity with Noise (LPN): Sparse, large error
(Code based)

Unstructured Noisy Linear Algebraic Assumptions (NLA)

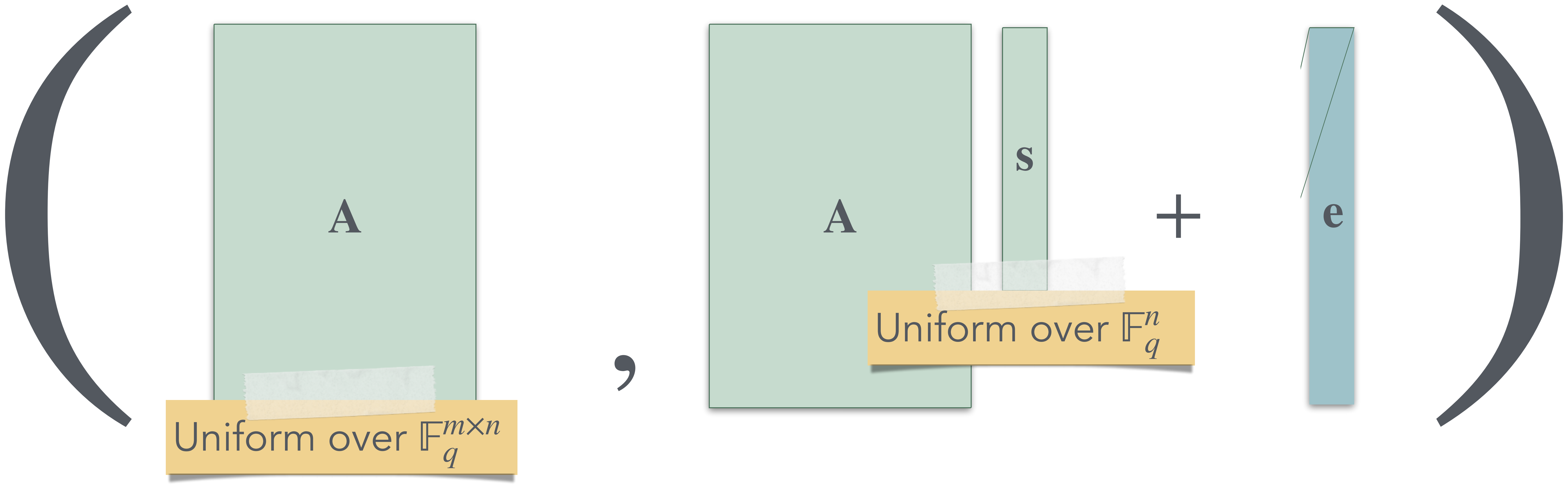


Learning with Errors (LWE): Small error (Discrete Gaussian)

p-sparse means p probability of a non-zero entry chosen uniformly from $\mathbb{F}_q$.

Learning Parity with Noise (LPN): Sparse, large error

Unstructured Noisy Linear Algebraic Assumptions (NLA)



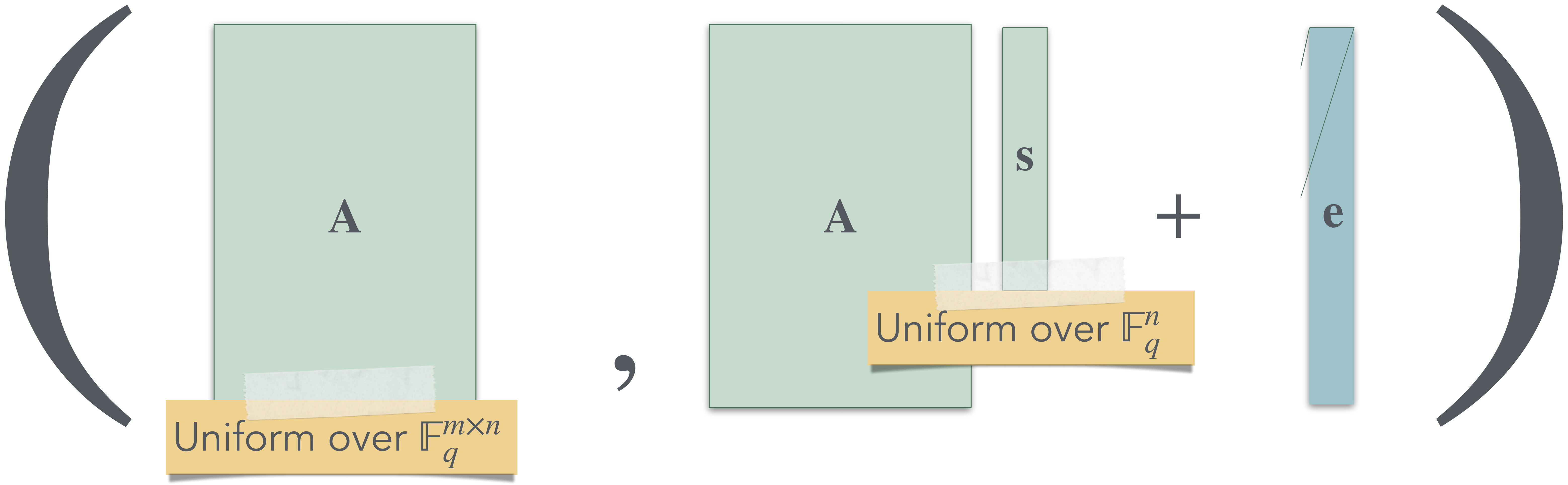
Learning with Errors (LWE): Small error (Discrete Gaussian)

Learning Parity with Noise (LPN): Sparse, large error

p-sparse means p probability of a non-zero entry chosen uniformly from $\mathbb{F}_q$.

Sparsity is parameterized by the secret dimension n. Think of $p = n^{-\delta}, \delta \in (0,1)$.

Unstructured Noisy Linear Algebraic Assumptions (NLA)



Learning with Errors (LWE): Small error (Discrete Gaussian)

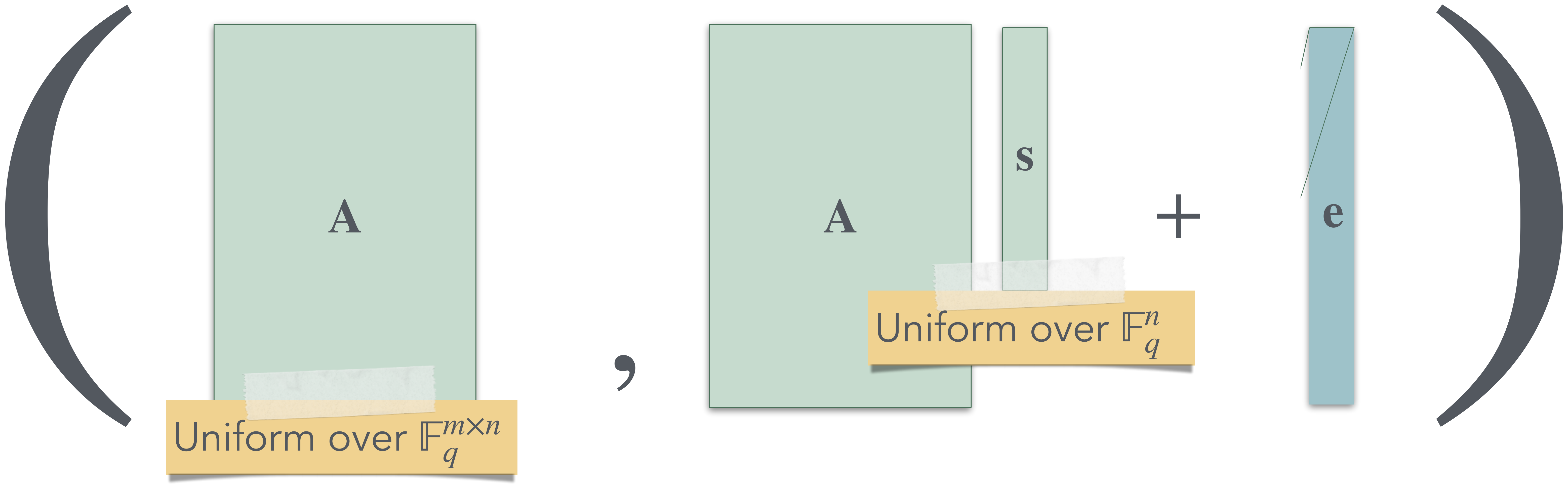
Implies PKE

Learning Parity with Noise (LPN): Sparse, large error

p-sparse means p probability of a non-zero entry chosen uniformly from $\mathbb{F}_q$.

Sparsity is parameterized by the secret dimension n. Think of $p = n^{-\delta}, \delta \in (0,1)$.

Unstructured Noisy Linear Algebraic Assumptions (NLA)



Learning with Errors (LWE): Small error (Discrete Gaussian)

Implies PKE

Learning Parity with Noise (LPN): Sparse, large error

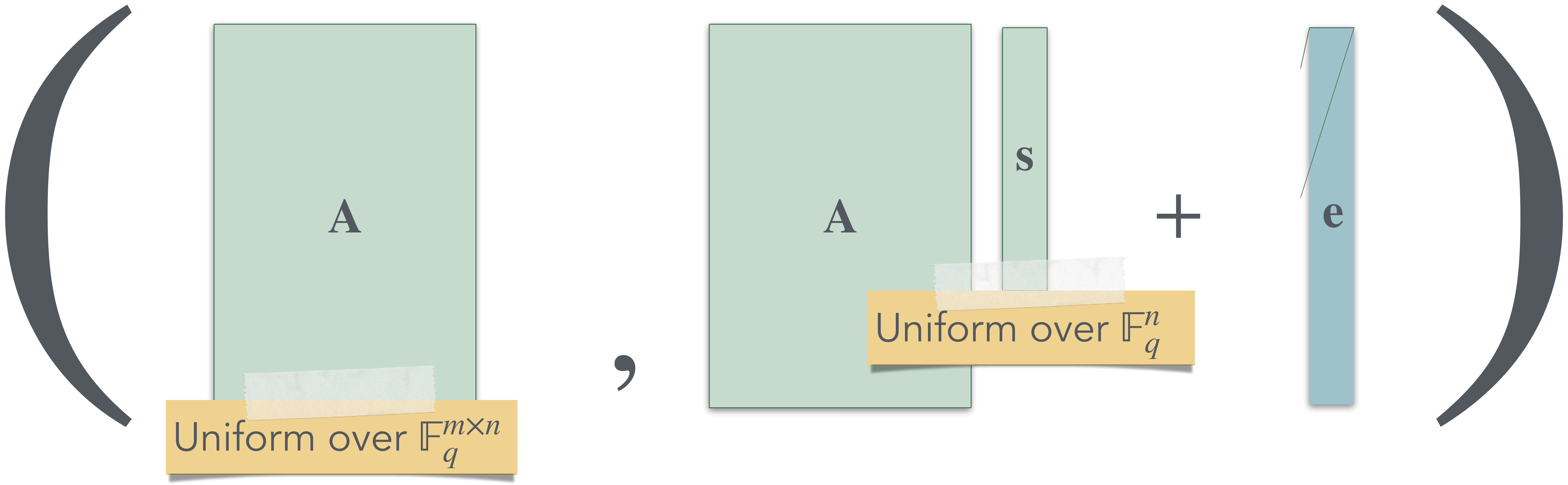
Implies PKE if $\delta \geq 0.5$

Alekhnovich's LPN

p-sparse means p probability of a non-zero entry chosen uniformly from $\mathbb{F}_q$.

Sparsity is parameterized by the secret dimension n. Think of $p = n^{-\delta}, \delta \in (0,1)$.

Unstructured Noisy Linear Algebraic Assumptions (NLA)



Learning with Errors (LWE): Small error (Discrete Gaussian)

Implies PKE

p-sparse means p probability of a non-zero entry chosen uniformly from $\mathbb{F}_q$.

Learning Parity with Noise (LPN): Sparse, large error

Implies PKE if $\delta \geq 0.5$

No PKE if $\delta < 0.5$

Alekhnovich's LPN

Alekhnovich's Barrier*

Sparsity is parameterized by the secret dimension n. Think of $p = n^{-\delta}, \delta \in (0,1)$.

Why NLAs?

LWE and LPN have been most reliable and most widely studied assumptions

believed to be Quantum secure

Why NLAs?

LWE and LPN have been most reliable and most widely studied assumptions

believed to be Quantum secure

NIST Post-quantum Cryptography Standardization Competition Round 3 Finalists for Key-Encapsulation Mechanism (KEM):

- NTRU [Lattice-based].
- SABER [Lattice-based].

Selected Algorithms for KEM

- CRYSTALS-Kyber (2022), FIPS 203. [Lattice-based].
- HQC (2025), FIPS coming soon.[Code-based].

Round 4 Submissions for KEM:

- BIKE [Code-based].
- Classic McEliece [Code-based].

ALL of these are NLA-based.

Why NLAs?

LWE and LPN have been most reliable and most widely studied assumptions

NIST Post-quantum C
Competition Round 3
Encapsulation Mecha

•NTRU [Lattice-based

•SABER [Lattice-based

for KEM

22), FIPS 203.

ming soon.[Code-

What if

both

LWE and (Alekhnovich) LPN

are (quantum) broken!!!

Round 4 Submissions

•BIKE [Code-based].

•Classic McEliece [Code-based].

ALL of these are NLA-based.

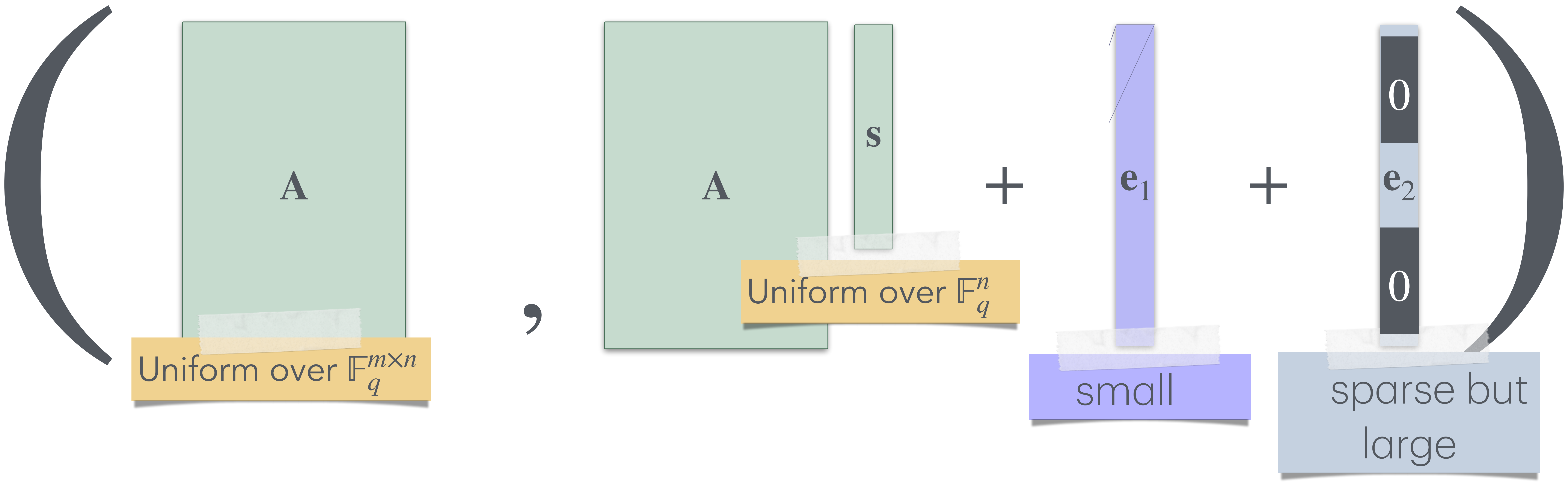
Main Question

Can we build PKE from Unstructured Noisy Linear Algebraic assumptions that are potentially secure in the world where

BOTH LWE and Alekhnovich's LPN are broken?

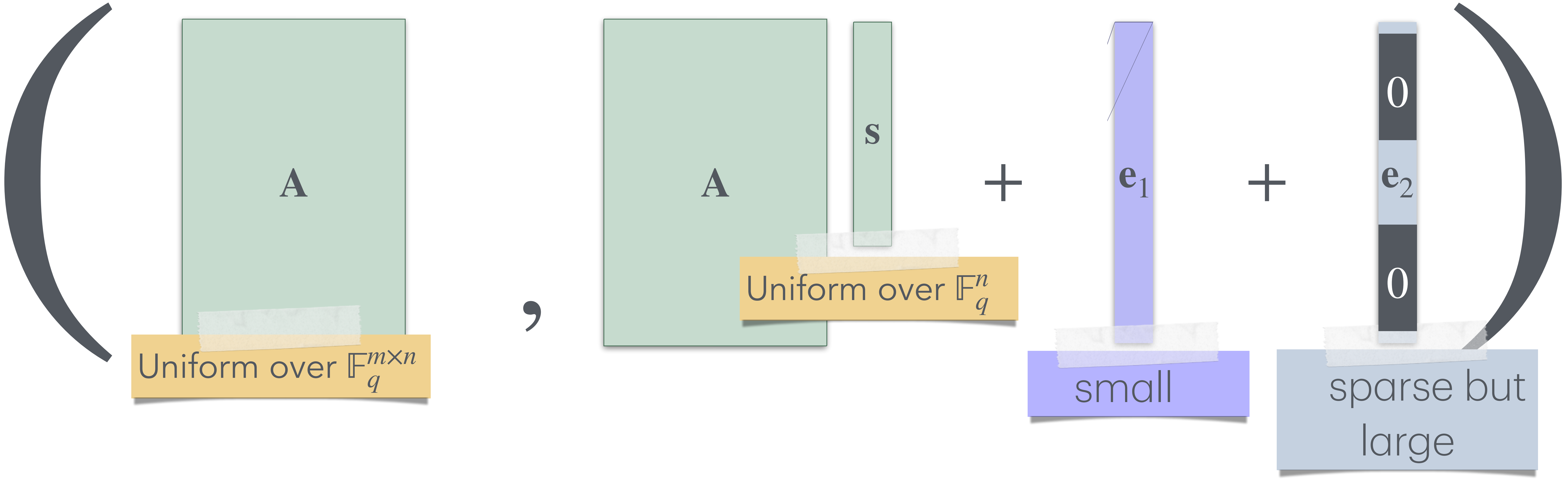
Our Hardness Assumption

Learning with Two Errors (LW2E)



Our Hardness Assumption

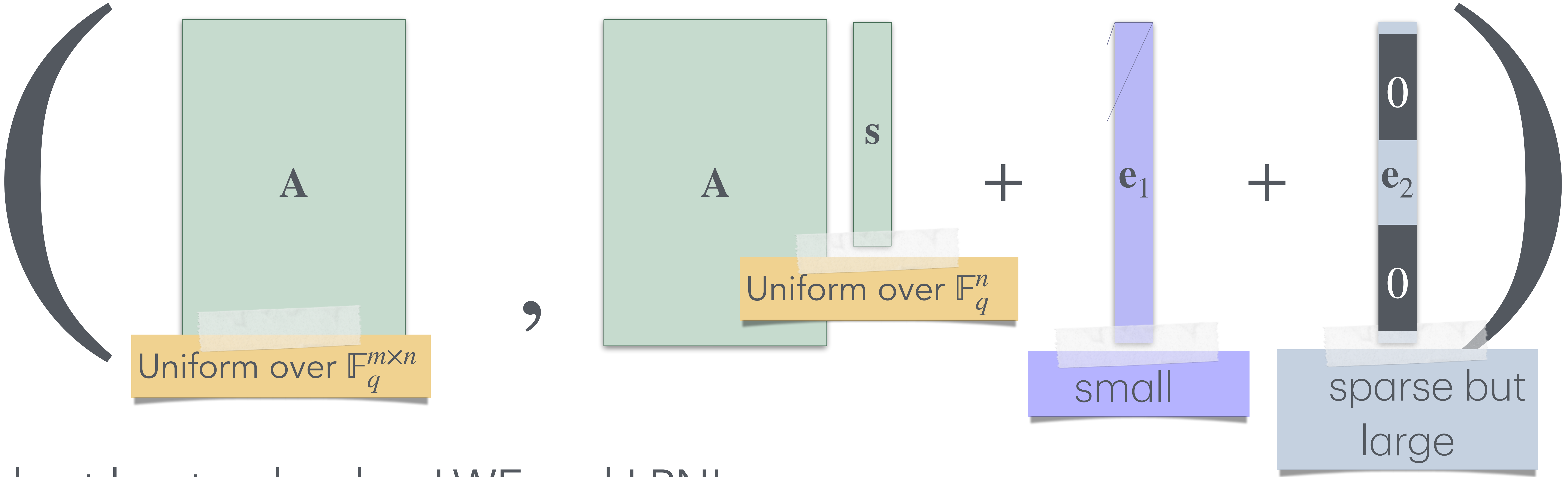
Learning with Two Errors (LW2E)



Think of e_2 as $n^{-0.6}$ sparse

Our Hardness Assumption

Learning with Two Errors (LW2E)

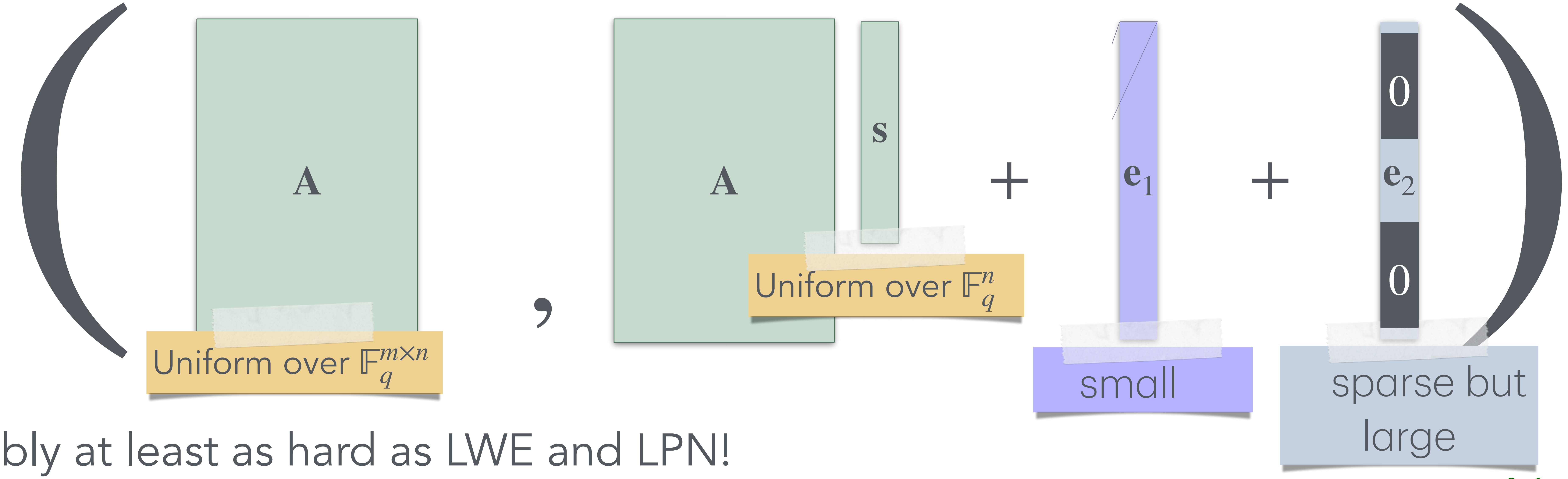


- Provably at least as hard as LWE and LPN!

Think of e_2 as $n^{-0.6}$ sparse

Our Hardness Assumption

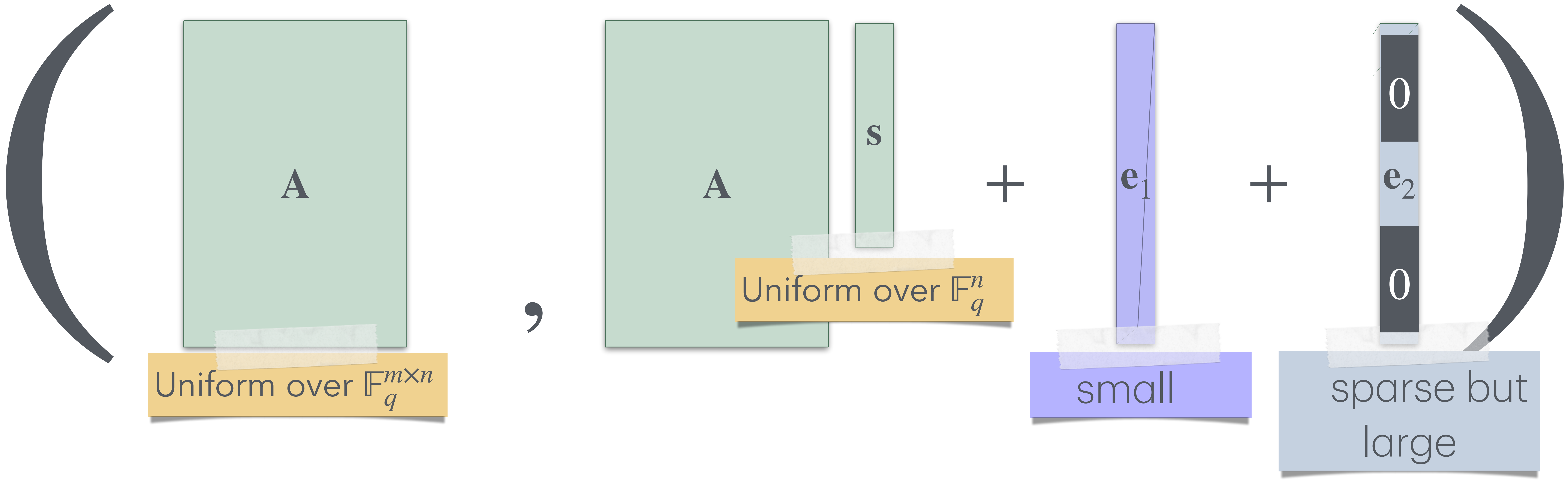
Learning with Two Errors (LW2E)



Think of e_2 as $n^{-0.6}$ sparse

- Provably at least as hard as LWE and LPN!
- Error is neither small nor sparse—can conjecture to be strictly harder!

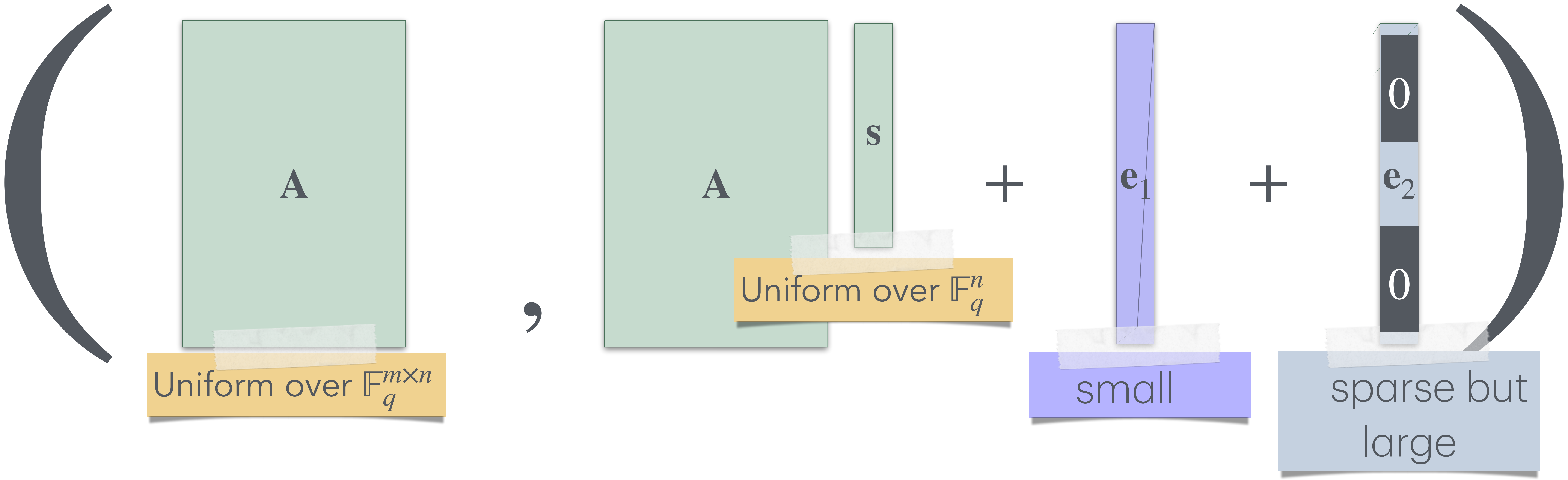
More on the hardness of LW2E



LW2E with parameters that we use in the PKE is potentially not a lattice problem!

No known reduction to Approximate CVP with our PKE parameters

More on the hardness of LW2E



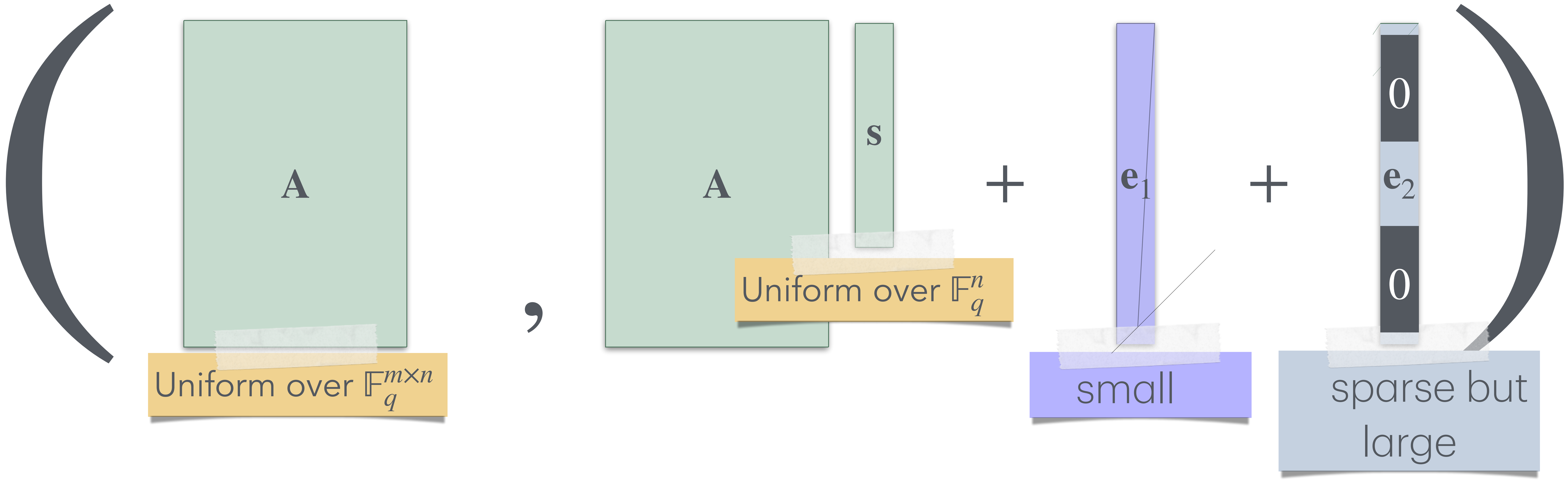
LW2E with parameters that we use in the PKE is potentially not a lattice problem!

No known reduction to Approximate CVP with our PKE parameters

For parameters outside of the PKE regime, LW2E reduces to Approx-CVP with approximation parameter $O\left(\frac{n^{\delta/2}}{q^{\frac{n}{m}}}\right)$

Note: $\delta < 1$

More on the hardness of LW2E



LW2E with parameters that we use in the PKE is potentially not a lattice problem!

No known reduction to Approximate CVP with our PKE parameters

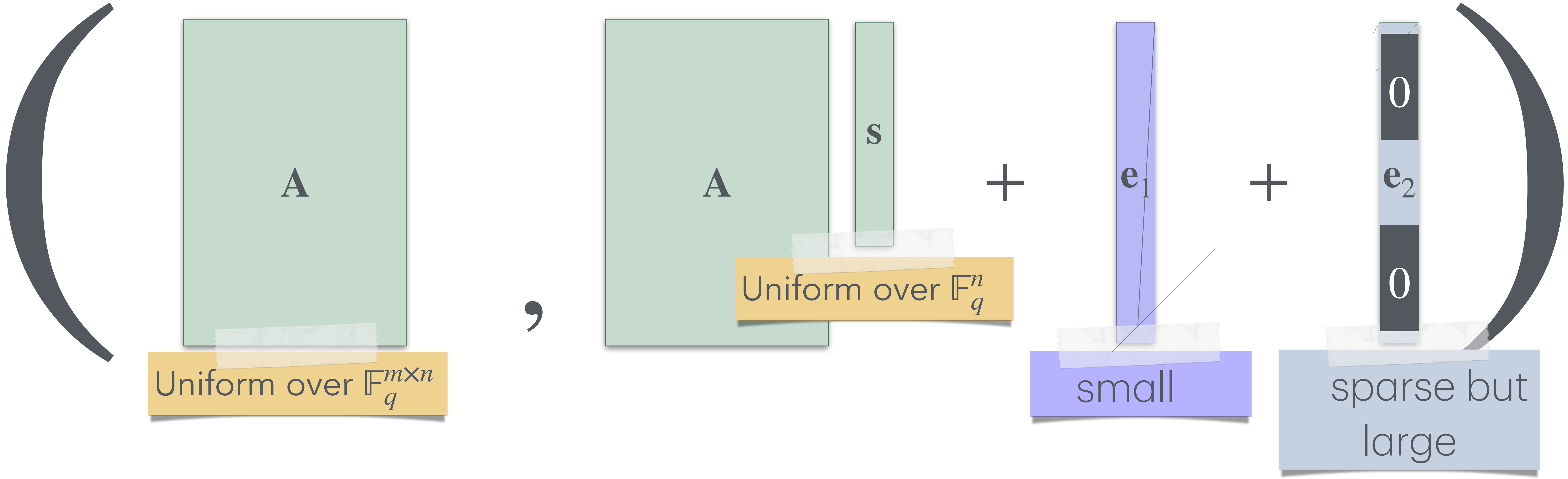
For parameters outside of the PKE regime, LW2E reduces to Approx-CVP with approximation parameter $O\left(\frac{n^{\delta/2}}{q^{\frac{n}{m}}}\right)$

Conjecture: LW2E is secure in the presence of an Approx-CVP oracle with weaker parameter.

Note: $\delta < 1$

For context, LWE reduces to $\sqrt{n}$-CVP

More on the hardness of LW2E



LW2E with parameters that we use in the PKE is potentially not a lattice problem!

No known reduction to Approximate CVP with our PKE parameters

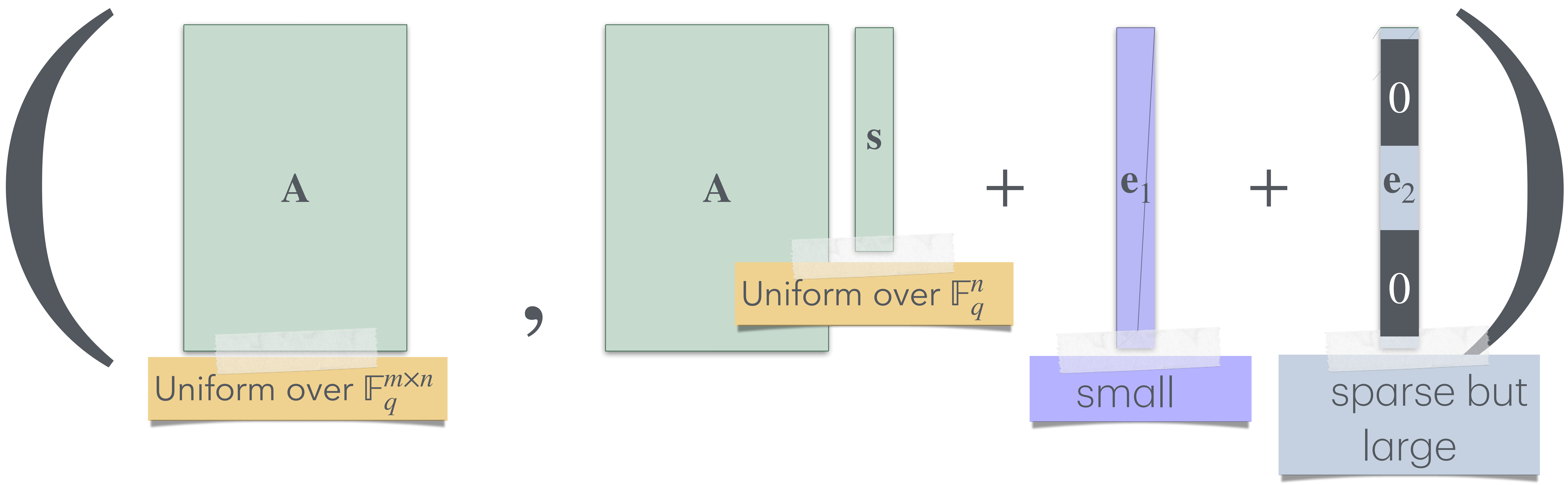
For parameters outside of the PKE regime, LW2E reduces to Approx-CVP with approximation parameter $O\left(\frac{n^{\delta/2}}{q^{\frac{n}{m}}}\right)$

Conjecture: LW2E is secure in the presence of an Approx-CVP oracle with weaker parameter.

Note: $\delta < 1$

For context, LWE reduces to $\sqrt{n}$-CVP

PKE from LW2E



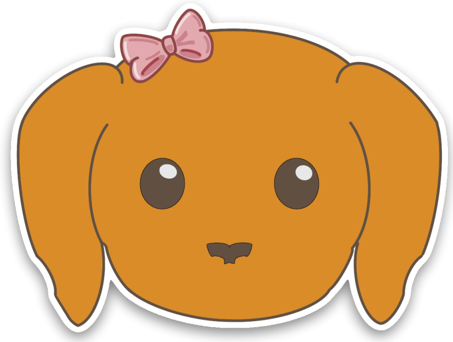
Is this useful for **public-key cryptography**?

General PKE template for NLAs

$$\mathbf{A} \leftarrow_{\$} \mathbb{F}_q^{m \times n},\ \mathbf{s} \leftarrow_{\$} \mathbb{F}_q^{n},\ \mathbf{e} \leftarrow_{\$} \mathcal{D}_{\text{error}}$$

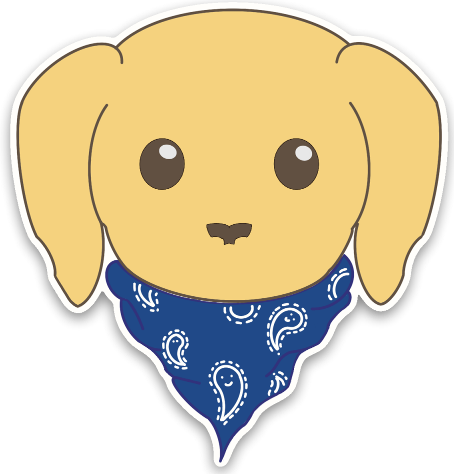
public key

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^{m}$$



Alice

$x \in \{0,1\}$



Bob

private key

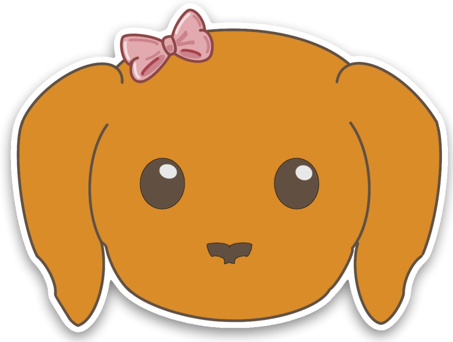
$\mathbf{s} \in \mathbb{F}_q^{n}$

General PKE template for NLAs

$\mathbf{A} \leftarrow_\$ \mathbb{F}_q^{m\times n}$, $\mathbf{s} \leftarrow_\$ \mathbb{F}_q^n$, $\mathbf{e} \leftarrow_\$ \mathscr{D}_{\text{error}}$

public key

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A}\cdot\mathbf{s} + \mathbf{e}) \in \mathbb{F}_q^{m\times n} \times \mathbb{F}_q^m$$

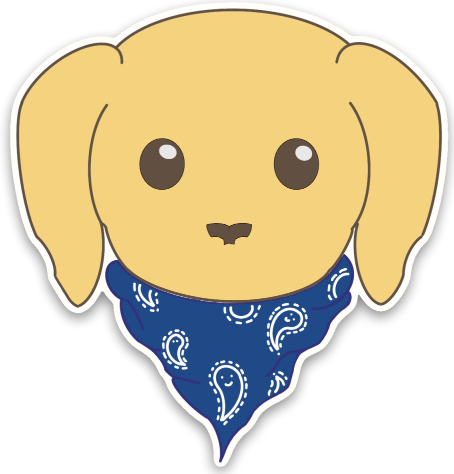


Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$
where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.



Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General PKE template for NLAs

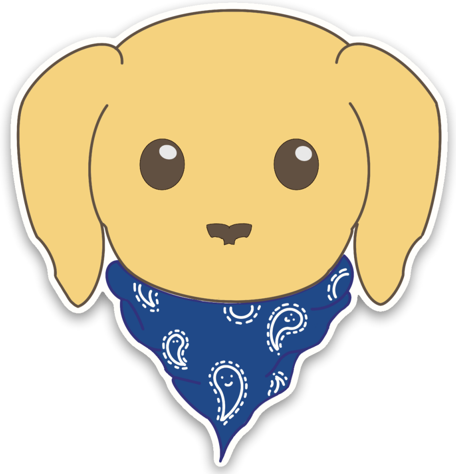
public key

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^m$$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.



Bob

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

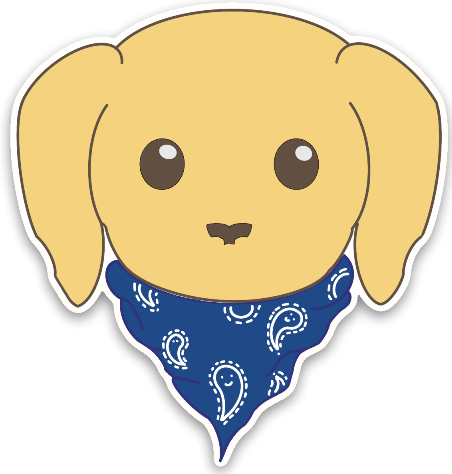
if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot \mathbf{e}$

General PKE template for NLAs

if $x = 1$, $\mathbf{r}^\top \cdot \mathbf{e}$

In the case of LWE, **small**.



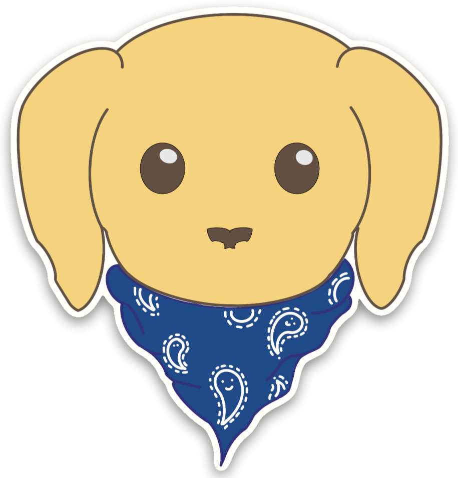
Bob

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (**large**)

General PKE template for NLAs



Bob

To decrypt, Bob computes:

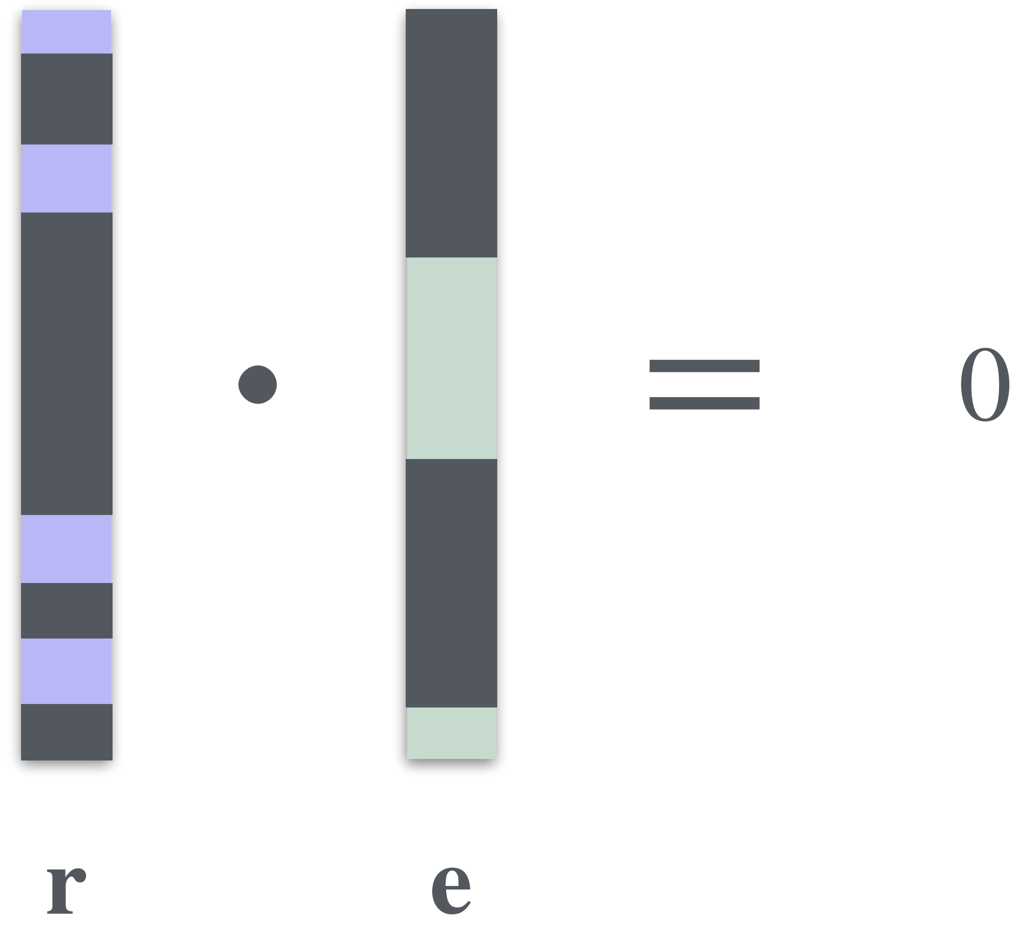
$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot \mathbf{e}$

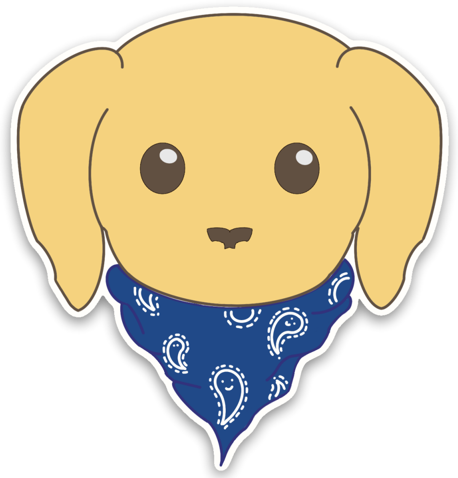
In the case of LWE, **small**.

In the case of LPN, when the error is $n^{-\delta}$-sparse, for $\delta \geq 0.5$, then 0.

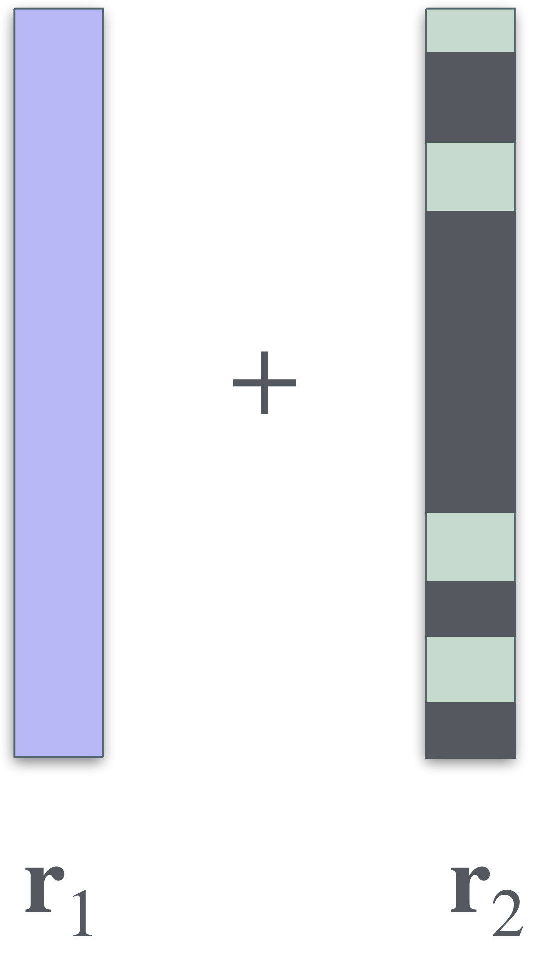


Does this work with LW2E?

Does this work with LW2E?



Bob



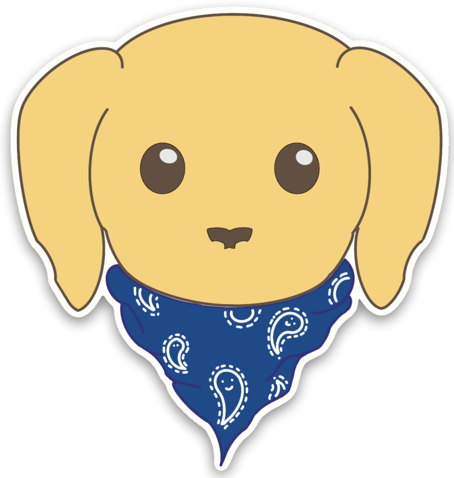
To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2 \leftarrow_\$ \mathscr{D}_{\text{error}}$

Does this work with LW2E?



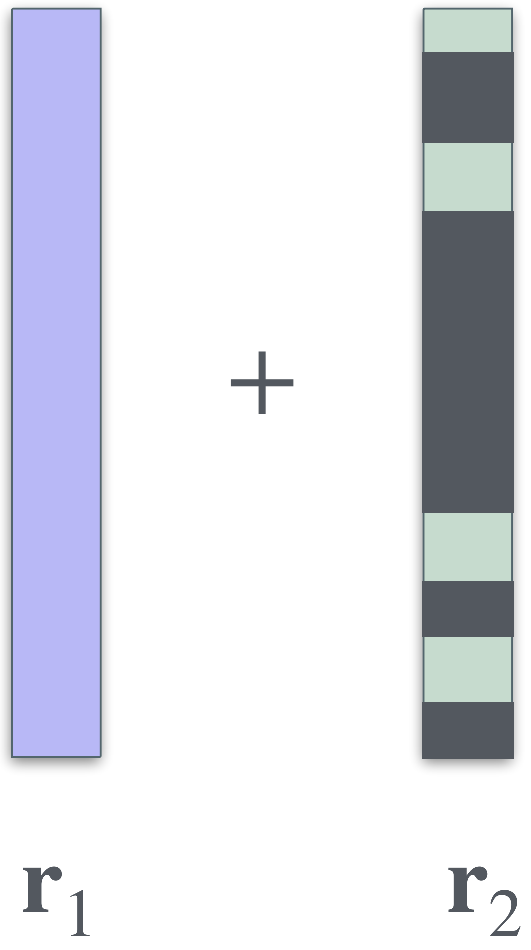
Bob

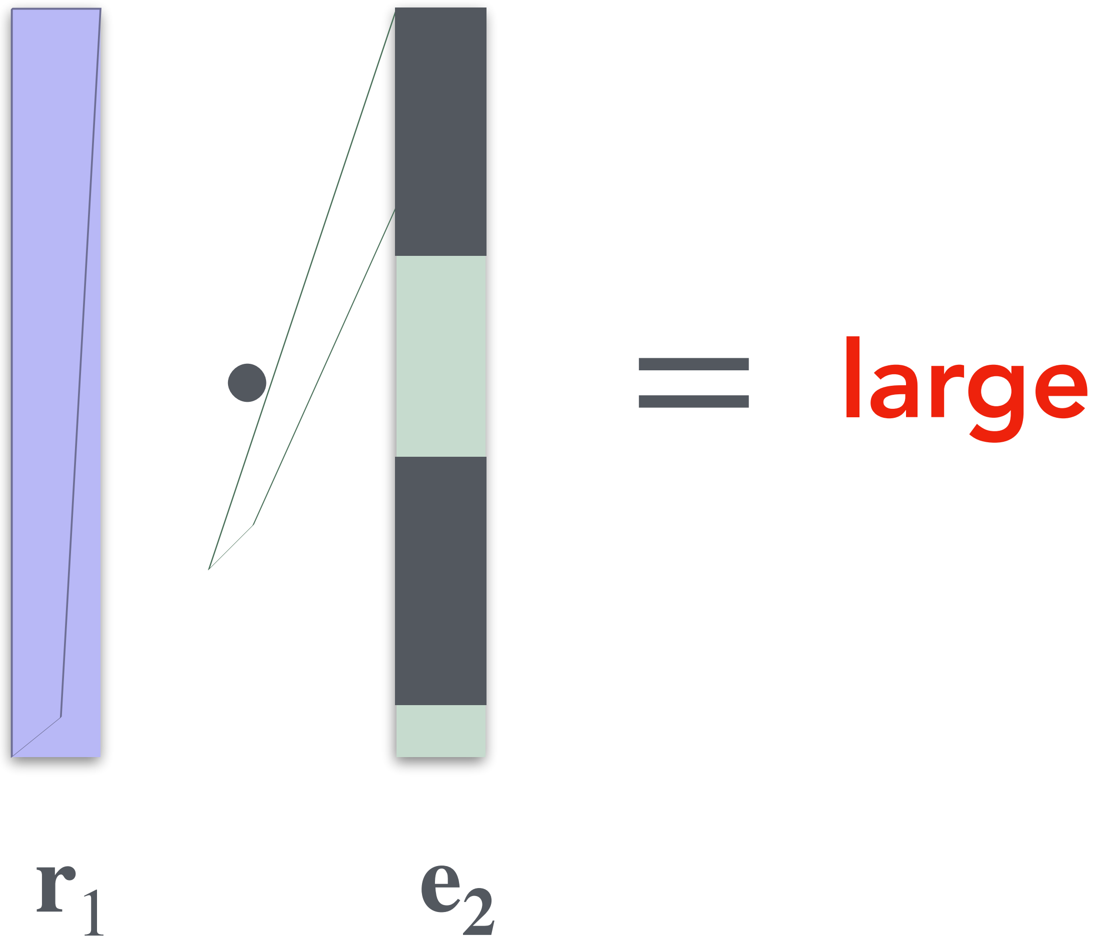
To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

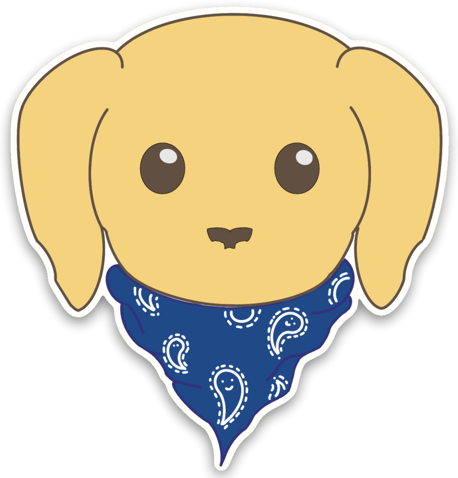
if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2 \leftarrow_\$ \mathscr{D}_{\text{error}}$





Does this work with LW2E?



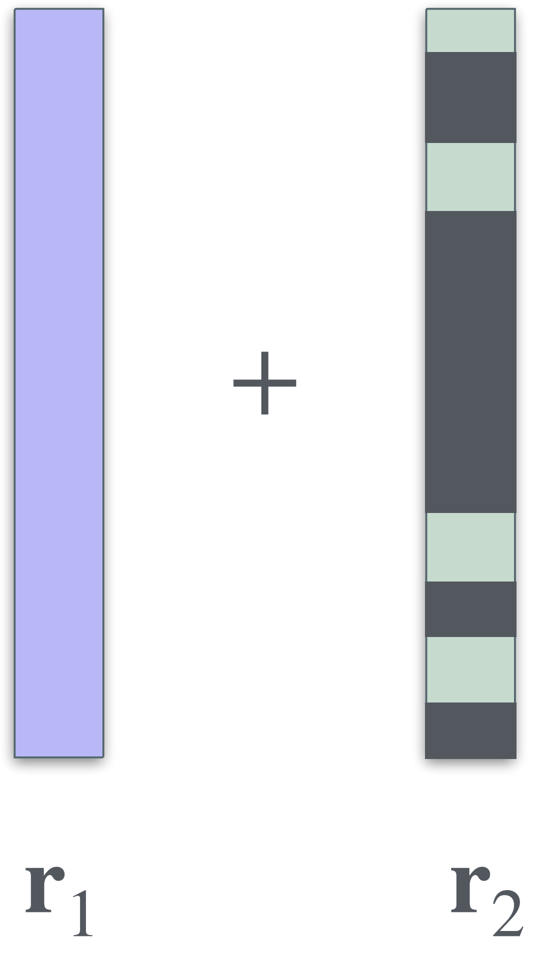
Bob

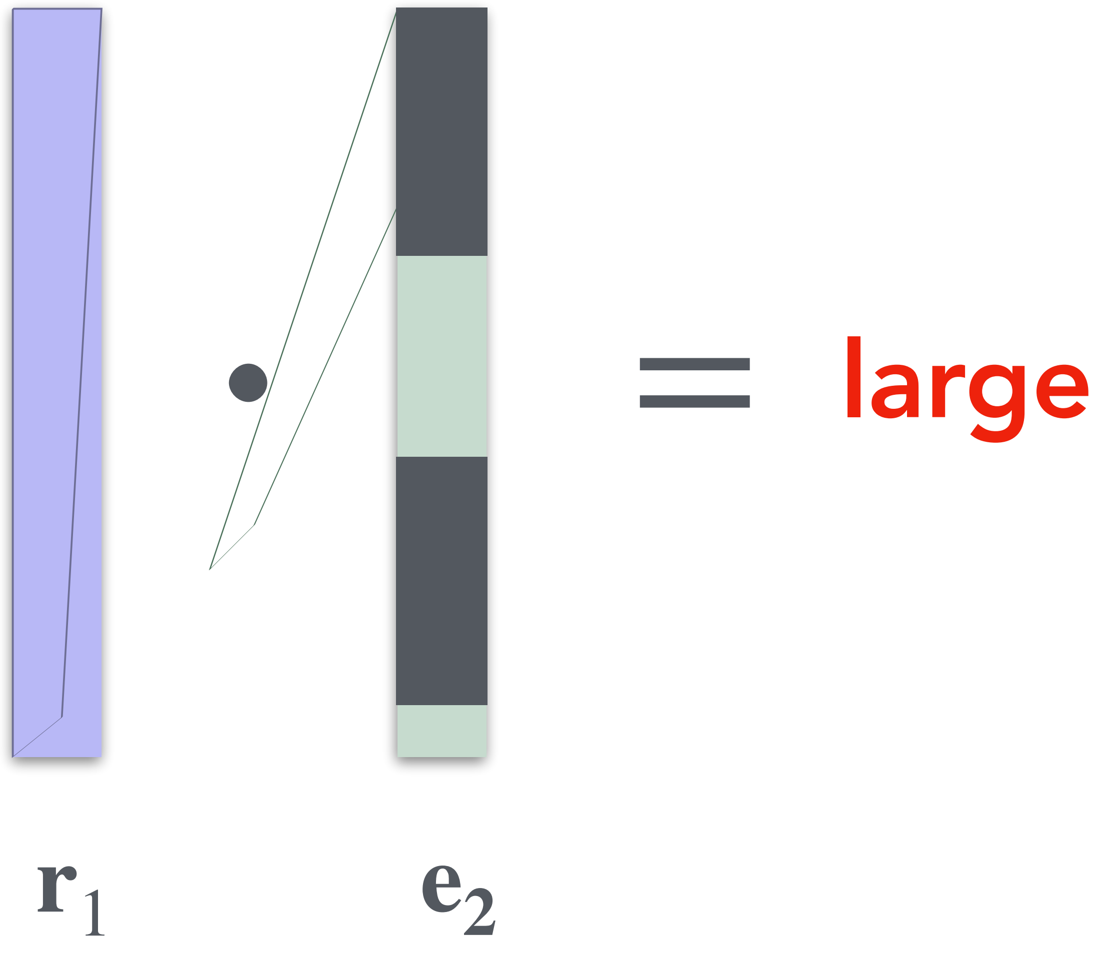
To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (**large**)

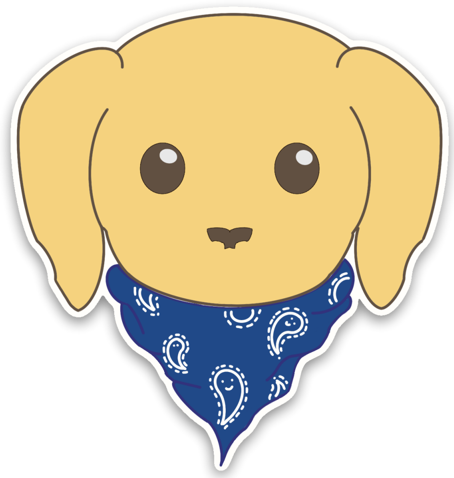
if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2 \leftarrow_\$ \mathscr{D}_{\text{error}}$





Not distinguishable from the case of $x = 0$

PKE from LW2E- Make use of asymmetry



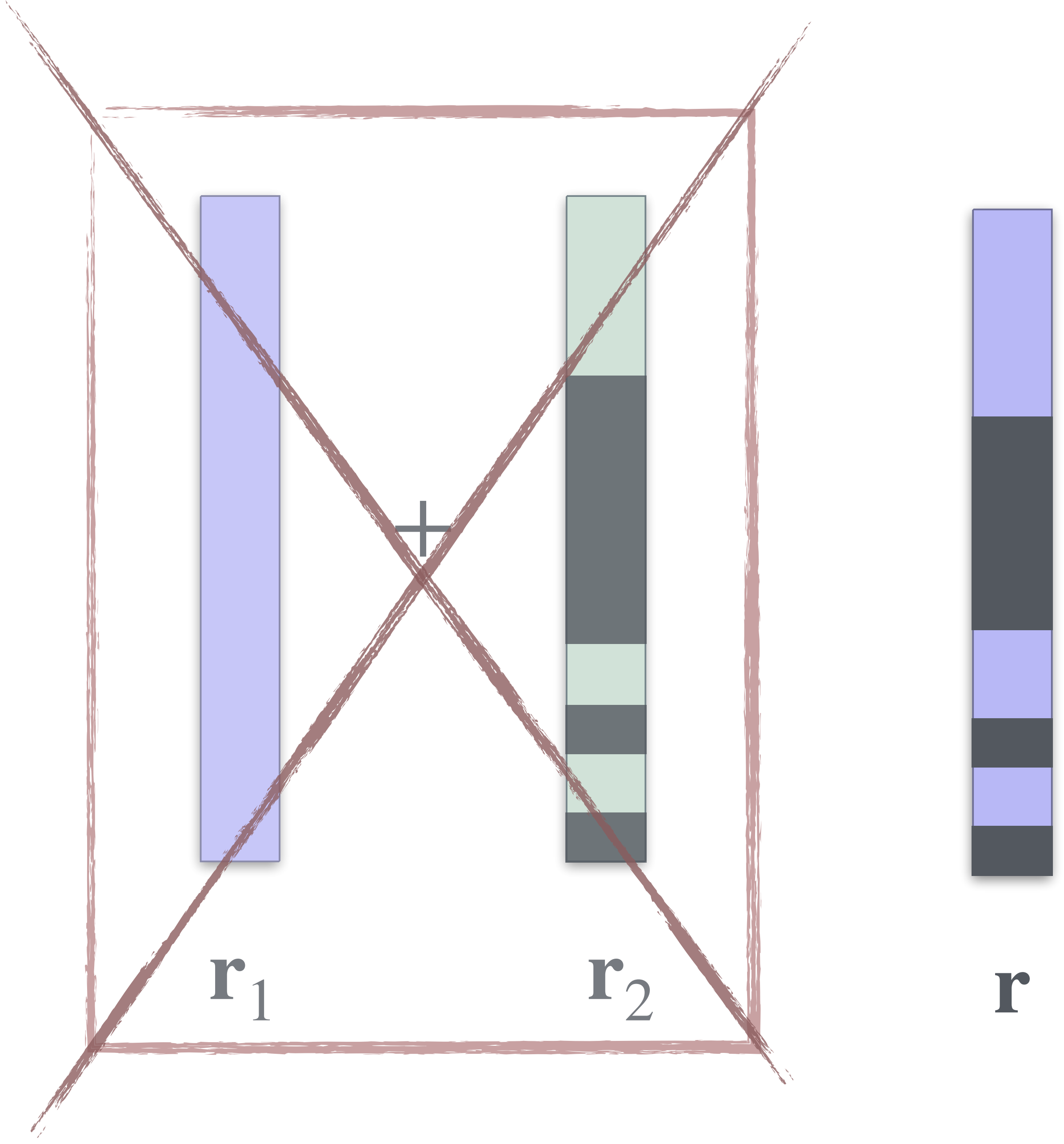
Bob

To decrypt, Bob computes:

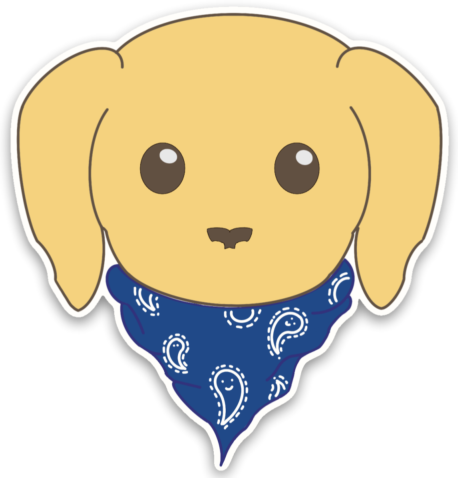
$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$



PKE from LW2E- Make use of asymmetry



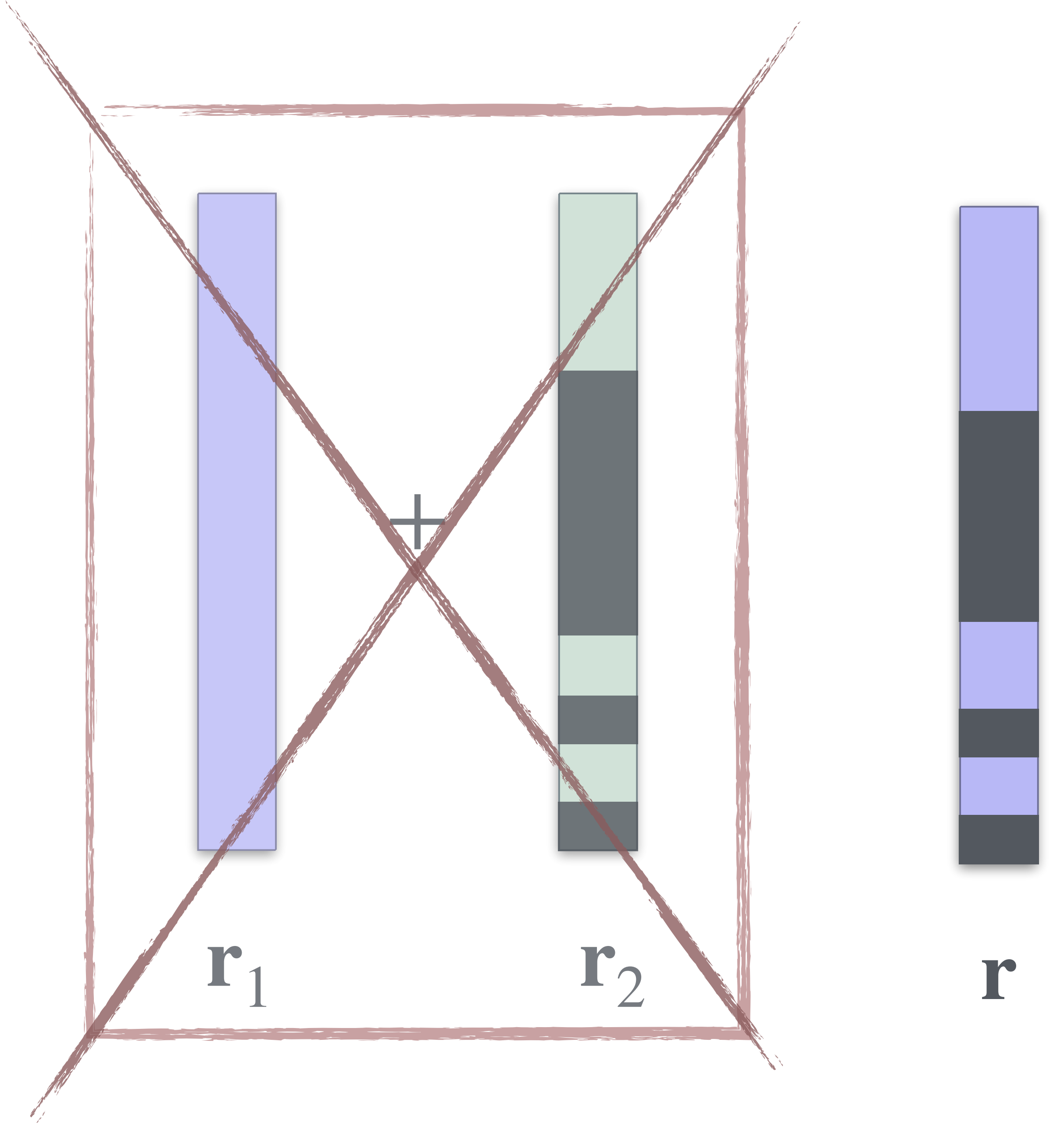
Bob

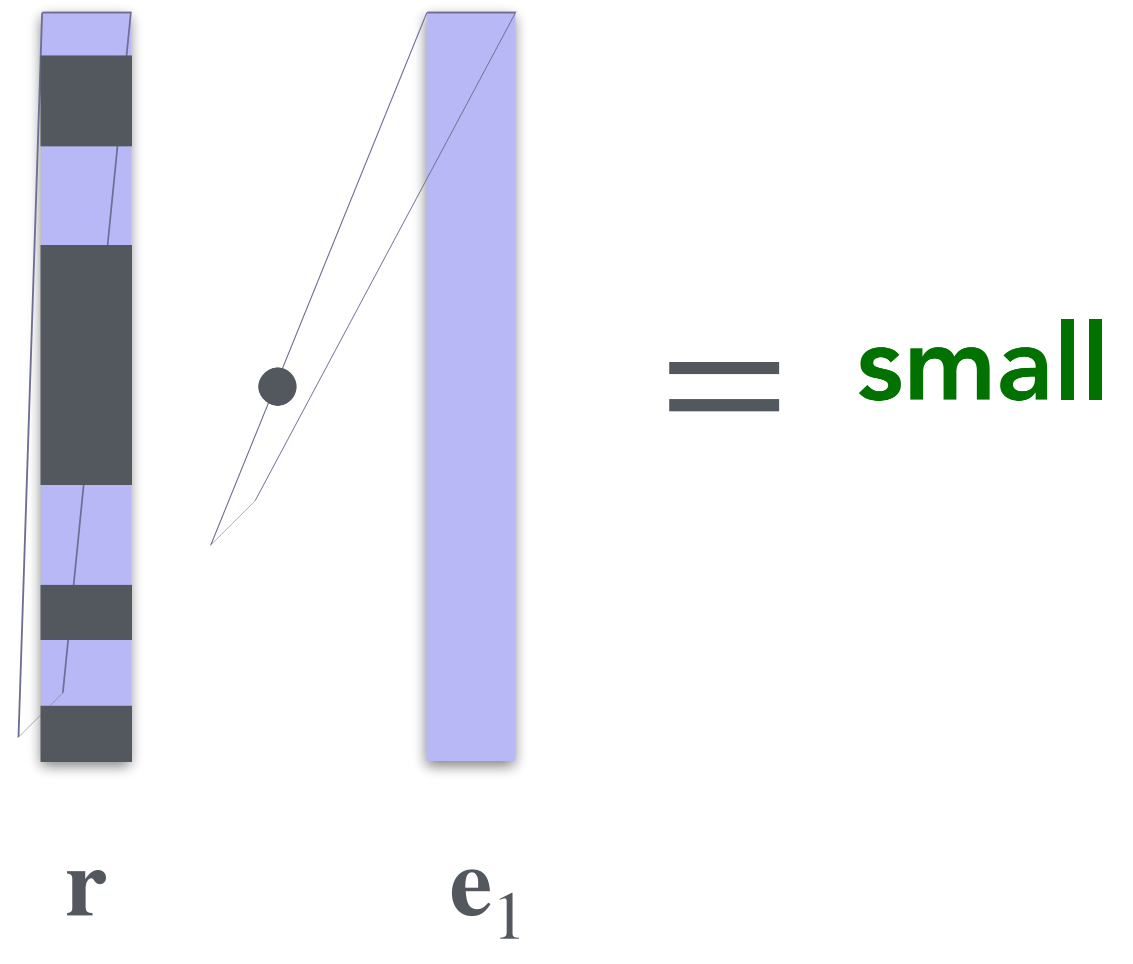
To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

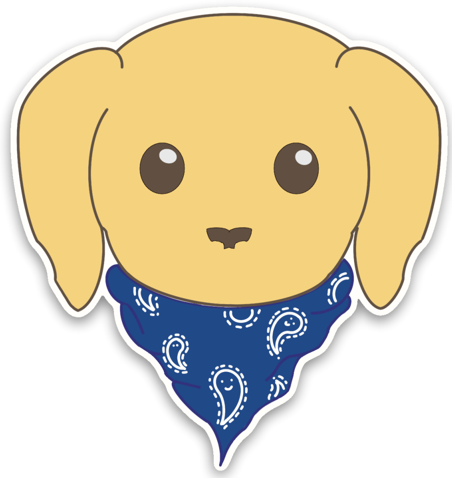
if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$





PKE from LW2E- Make use of asymmetry



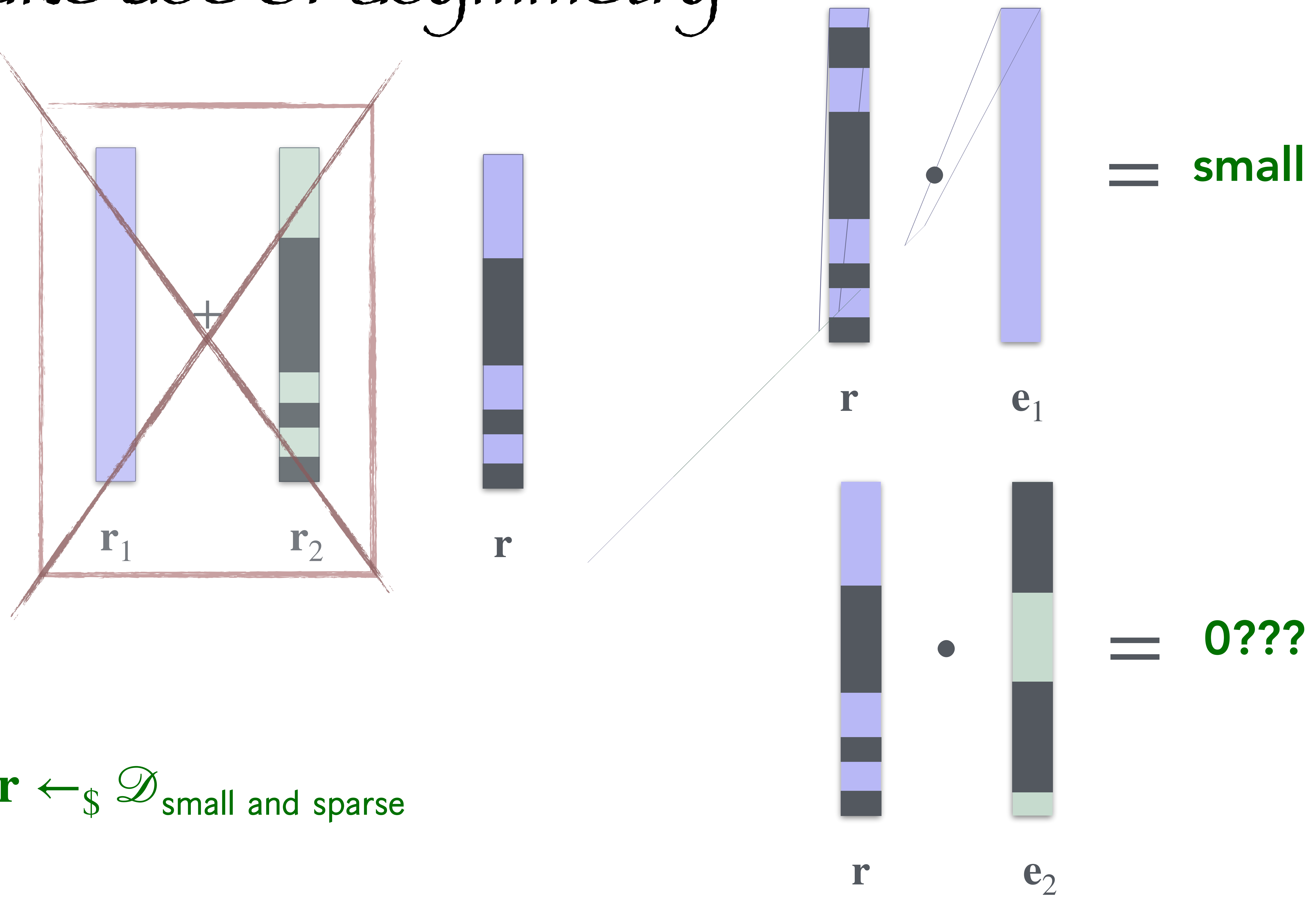
Bob

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (**large**)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$



PKE from LW2E- Make use of asymmetry

Assume for simplicity: $m = O(n)$.

$n^{-\gamma}$ sparse $n^{-\delta}$ sparse

PKE from LW2E- Make use of asymmetry

Assume for simplicity: $m = O(n)$.

$n^{-\gamma}$ sparse

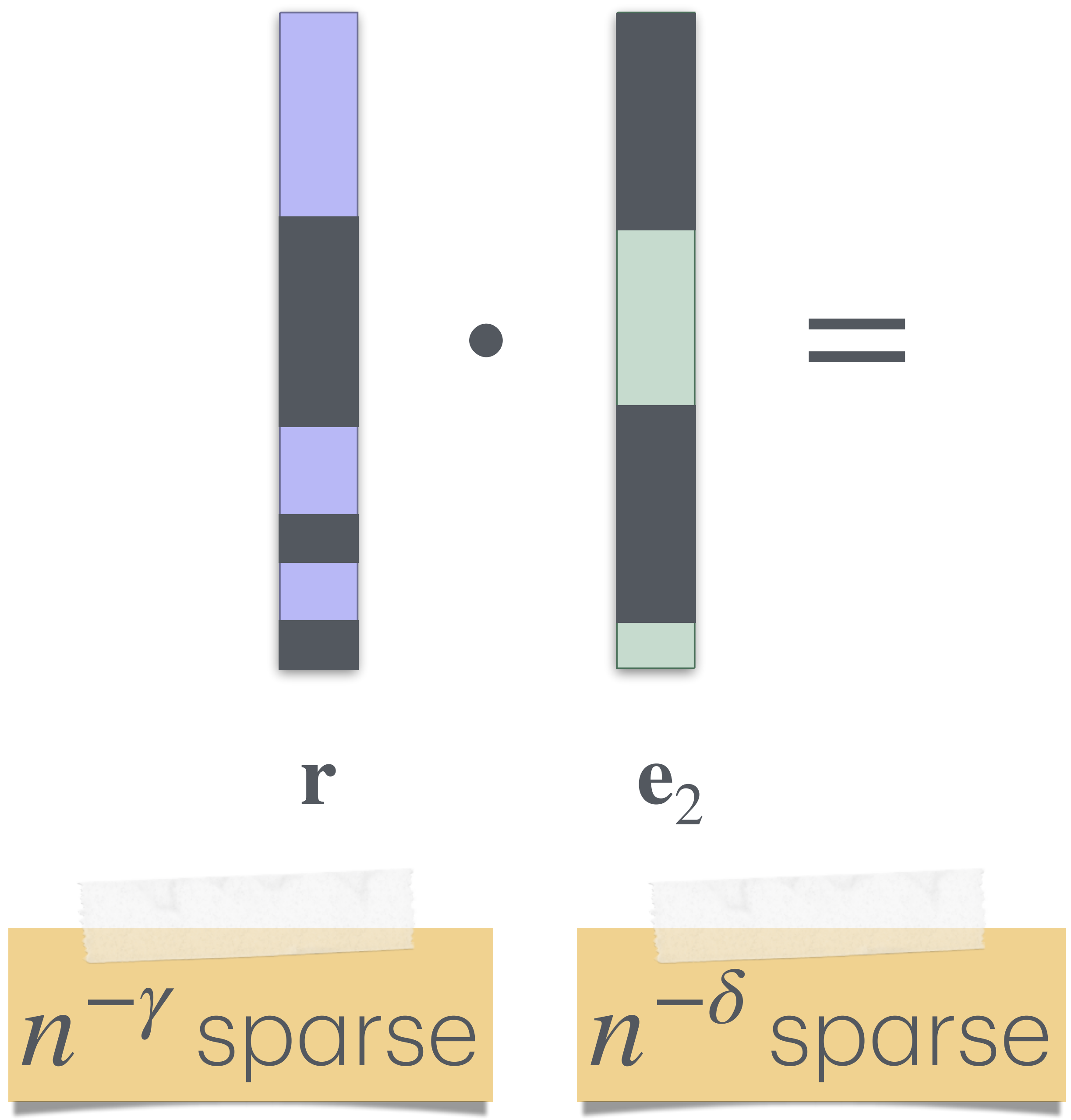
$n^{-\delta}$ sparse

Probability of being 0 is roughly $(1 - n^{-\delta})^{mn^{-\gamma}} \approx e^{-n^{1-\gamma-\delta}}$.

For correctness, want this to be non-negligible, i.e. $\gamma + \delta \geq 1$.

PKE from LW2E- Make use of asymmetry

Assume for simplicity: $m = O(n)$.



Probability of being 0 is roughly $(1 - n^{-\delta})^{mn^{-\gamma}} \approx e^{-n^{1-\gamma-\delta}}$.

For correctness, want this to be non-negligible, i.e. $\gamma + \delta \geq 1$.

Pick $\gamma < 0.5$ and $\delta \geq 0.5$

PKE from LW2E- Summary

Assume for simplicity: $m = O(n)$.

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e_1} + \mathbf{e_2}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^m$$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

$\mathbf{e_2}$ is $n^{-\delta}$ sparse and $\mathbf{r}$ is $n^{-\gamma}$ sparse

$\gamma < 0.5$ **and** $\delta \geq 0.5$

PKE from LW2E

What about security?

PKE from LW2E

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

PKE from LW2E

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by ?

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 0$

PKE from LW2E

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Leftover Hash Lemma?

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 0$

PKE from LW2E

Recall: $m = O(n)$.

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$

Can we apply the Leftover Hash Lemma (LHL)?

PKE from LW2E

Recall: $m = O(n)$.

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$

Can we apply the Leftover Hash Lemma (LHL)?

Amount of entropy in r: $\log \left(\binom{m}{mn^{-\gamma}} B^{mn^{-\gamma}} \right)$ bits $\approx \tilde{O}(n^{1-\gamma})$ bits

PKE from LW2E

Recall: $m = O(n)$.

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$

Can we apply the Leftover Hash Lemma (LHL)?

Amount of entropy in r: $\log \left(\binom{m}{mn^{-\gamma}} B^{mn^{-\gamma}} \right)$ bits $\approx \tilde{O}(n^{1-\gamma})$ bits

LHL needs the entropy to be greater than $n \log q$.

PKE from LW2E

Recall: $m = O(n)$.

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$

Can we apply the Leftover Hash Lemma (LHL)?

Amount of entropy in r: $\log \left(\binom{m}{mn^{-\gamma}} B^{mn^{-\gamma}} \right)$ bits $\approx \tilde{O}(n^{1-\gamma})$ bits

LHL needs the entropy to be greater than $n \log q$.

No known setting of m, δ, γ such that correctness holds and security holds via LW2E + LHL.

PKE from LW2E

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by ?

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 0$

PKE from LW2E

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

A computational assumption?

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 0$

PKE from LW2E + helper assumption

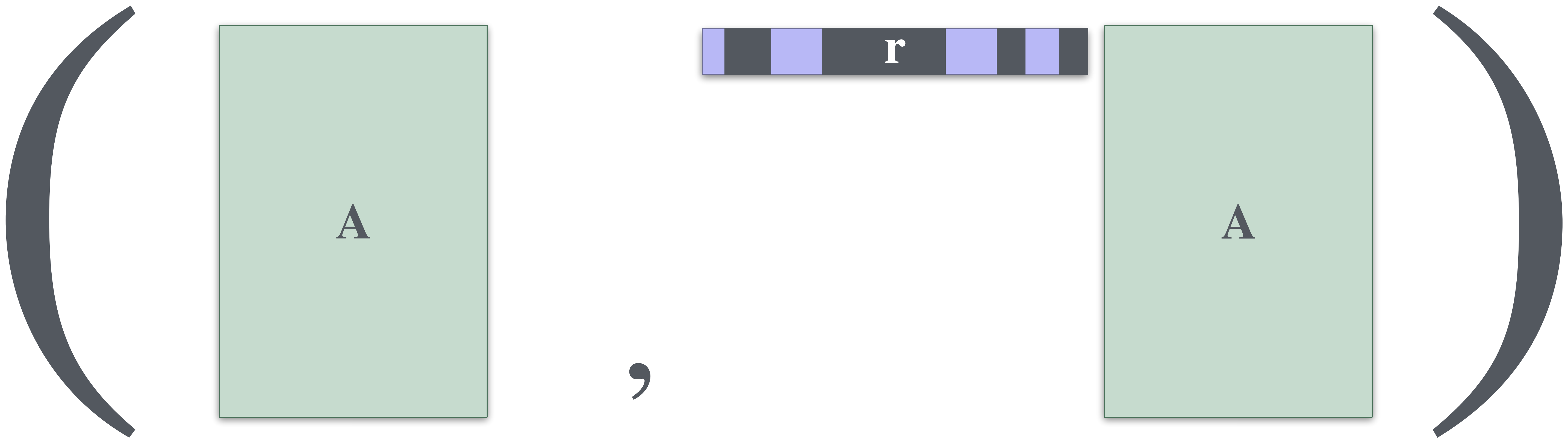
$(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

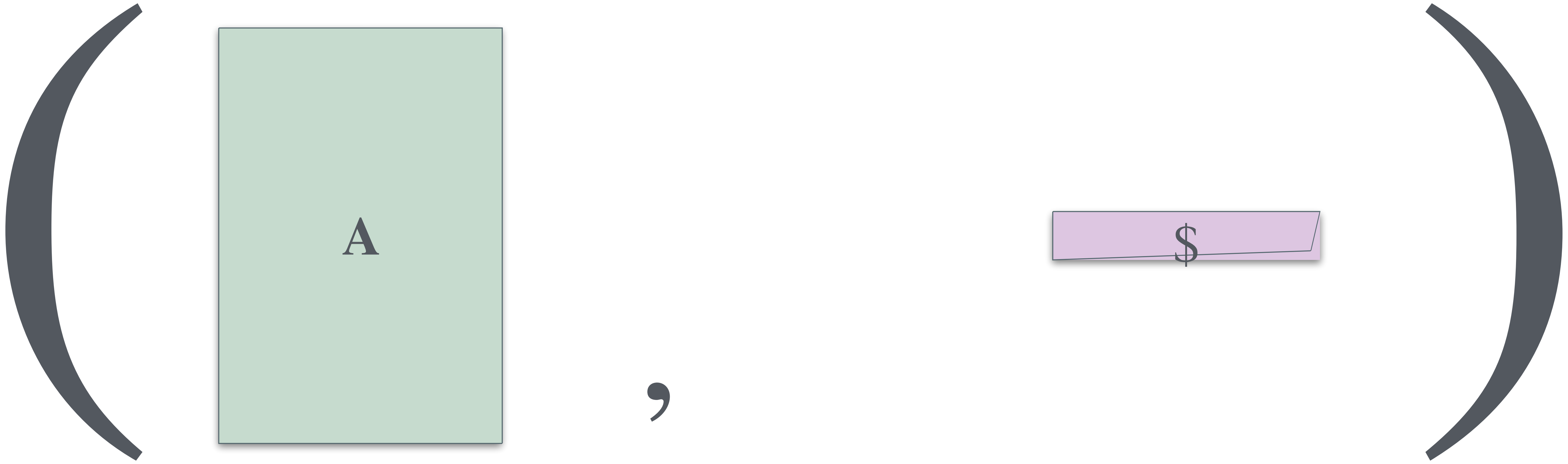
A computational assumption?

$(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$.

PKE from LW2E + helper assumption



is computationally indistinguishable from



$(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

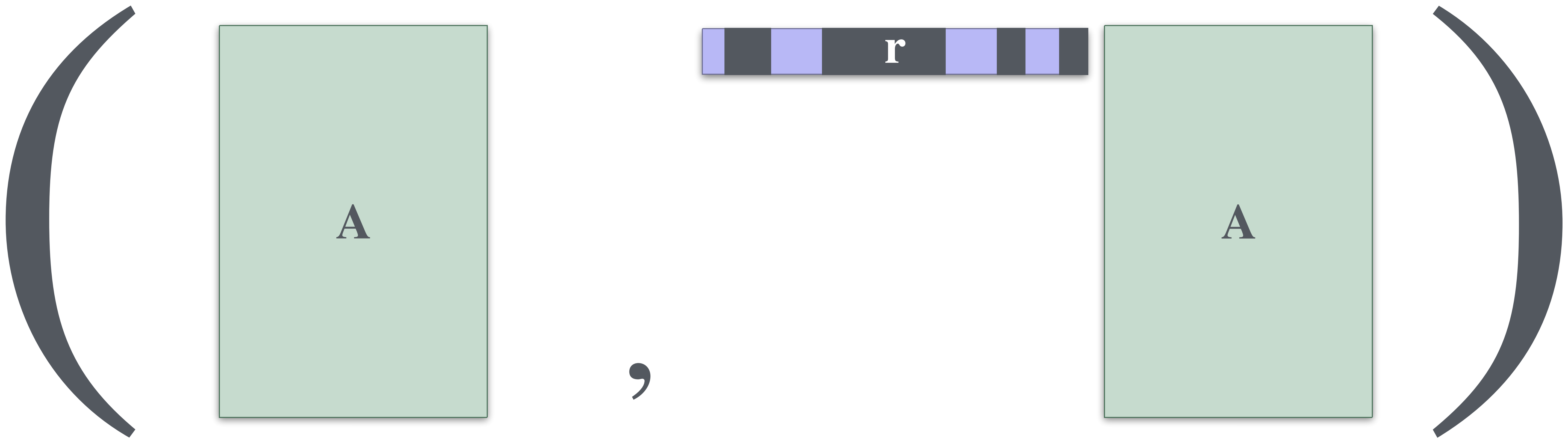
where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

A computational assumption?

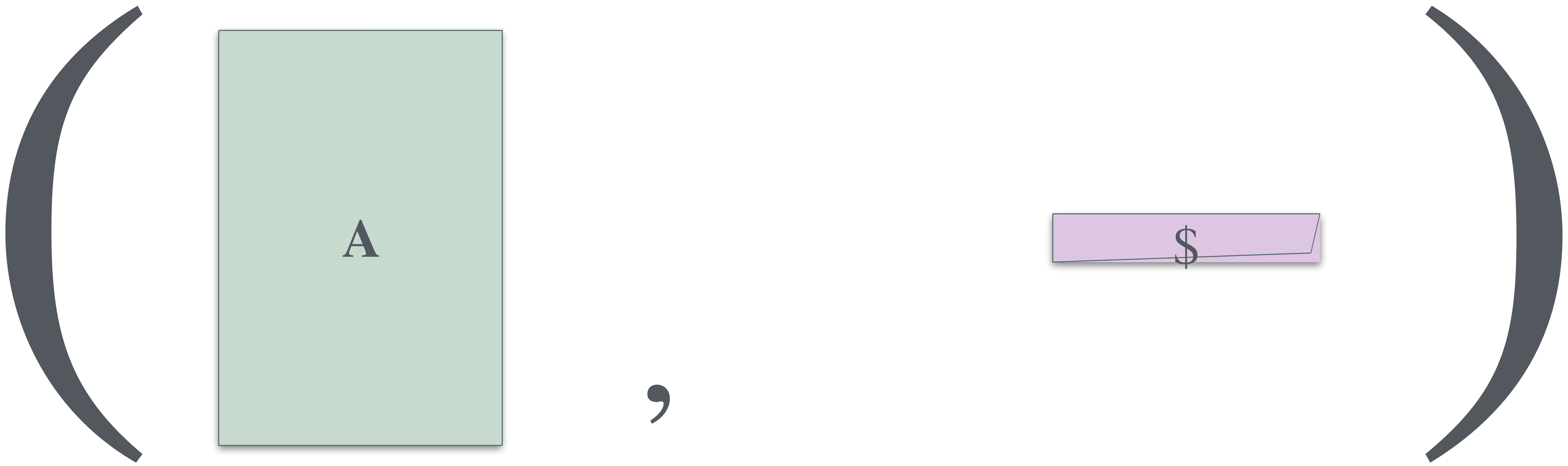
$(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$.

A computational version of LHL.

PKE from LW2E + ISSIS



is computationally indistinguishable from



$(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

A computational assumption?

$(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$.

A computational version of LHL.

Inhomogeneous Short and Sparse Integer Solution (ISSIS) problem

PKE from LW2E + ISSIS

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by ISSIS

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 1$

Adversary's view when $x = 0$

PKE from LW2E + ISSIS

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

by LW2E

Intuitively harder than both LWE and LPN.

: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by ISSIS

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 0$

PKE from LW2E + ISSIS

$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

Adversary's view when $x = 1$

by LW2E

Intuitively harder than both LWE and LPN.

: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small and sparse}}$.

by ISSIS

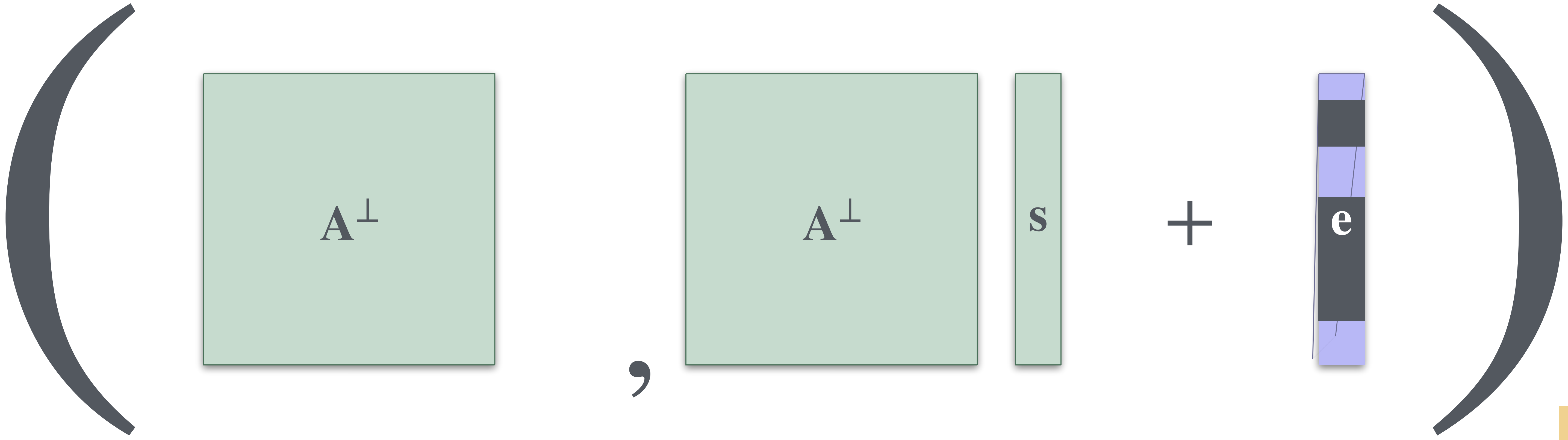
How does its hardness relate to LWE and LPN?

rid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

Adversary's view when $x = 0$

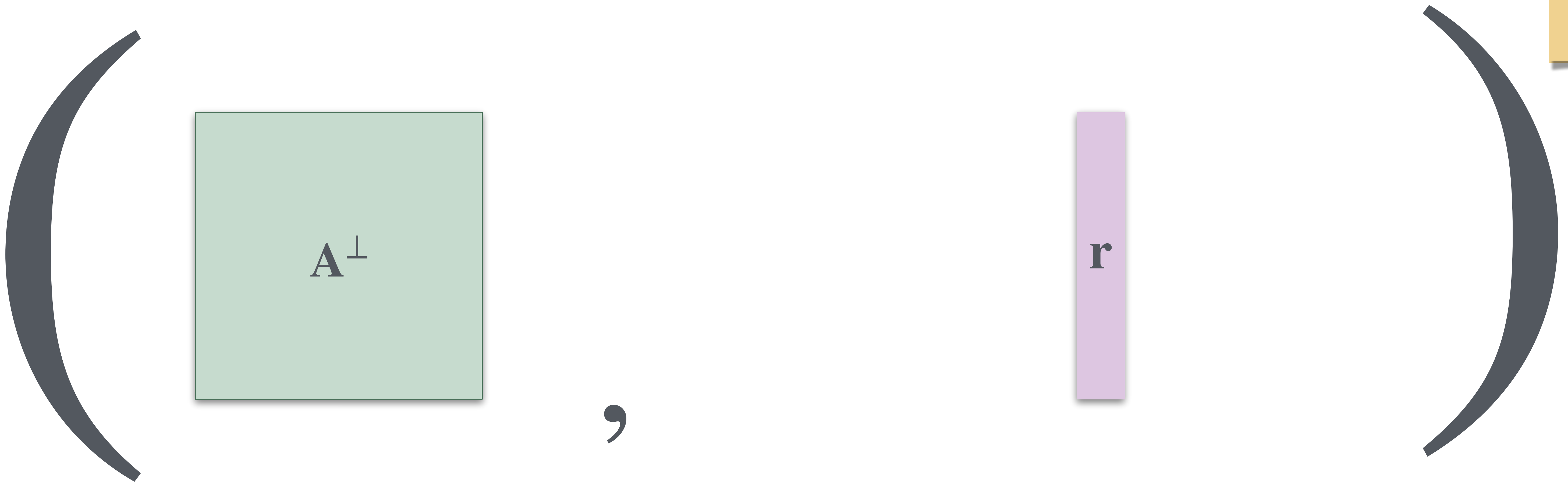
Learning with Short and Sparse Errors (LWSSE)

The matrix is near-square $\mathbb{F}_q^{(m-n)\times m}$.

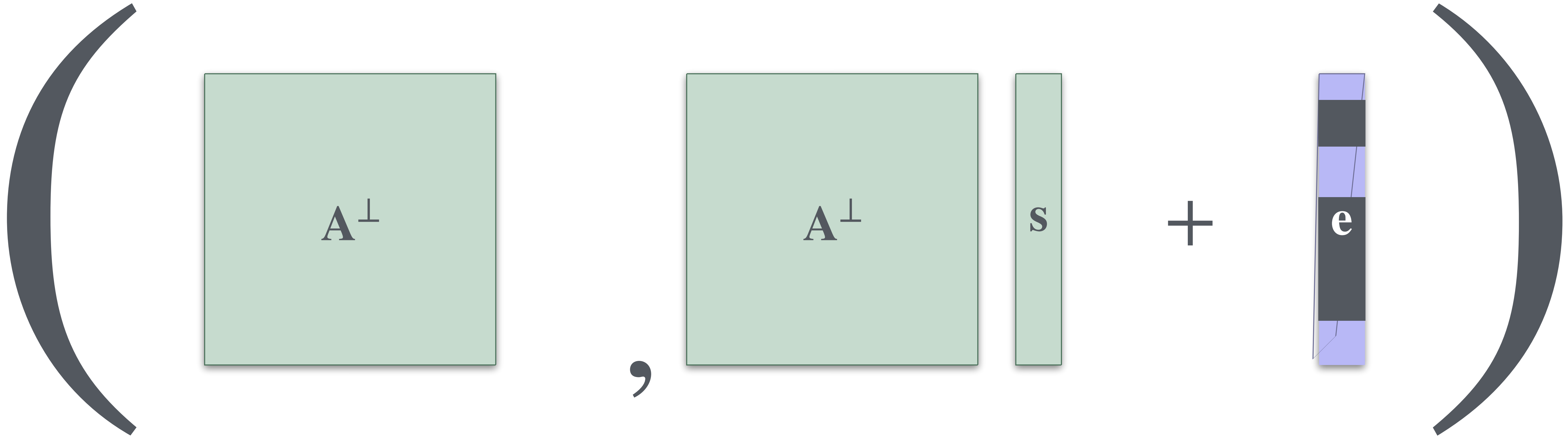


is computationally indistinguishable from

Dual and equivalent to ISSIS.



Relation to LPN



- LWSSE reduces to LPN with the same sparsity

Recall we crucially use ISSIS with sparsity $n^{-\gamma}, \gamma < 0.5$

Relation to lattice problems

Can we separate ISSIS from LWE or approx CVP?

Relation to lattice problems

Can we separate ISSIS from LWE or approx CVP?

No.

In general, it is not known how to obtain formal separations between assumptions without proving $P \neq NP$.

What can we show?

Relation to lattice problems

Parameter Setting for ISSIS: #dimensions after compression n, Secret dim. $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.

Relation to lattice problems

Parameter Setting for ISSIS: #dimensions after compression n, Secret dim. $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.

Standard reduction ideas to lattice problems fail with these parameters

Relation to lattice problems

Parameter Setting for ISSIS: #dimensions after compression n, Secret dim. $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.

Standard reduction ideas to lattice problems fail with these parameters

- These parameters are in the total SIS regime, thus, exponentially many SIS solutions expected to exist.

Relation to lattice problems

Parameter Setting for ISSIS: #dimensions after compression n, Secret dim. $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.

Standard reduction ideas to lattice problems fail with these parameters

- These parameters are in the total SIS regime, thus, exponentially many SIS solutions expected to exist.
- There are too many short vectors that are not sparse. An approximate BDD or CVP oracle is blind to sparseness.

Main Result

We introduce the Learning with Two Errors (LW2E) assumption and the Inhomogeneous Short and Sparse Integer Solution (ISSIS) assumption.

We give evidence that LW2E and ISSIS—in a range of parameters that imply public-key encryption (PKE)—remain secure even if LWE and Alekhnovich LPN are (quantum) broken.

Informal main result: There exists PKE assuming the hardness of LW2E and ISSIS in parameter regimes such that neither are potentially lattice problems and potentially stronger than Alekhnovich's LPN.

Open Problems

- Use ISSIS and LW2E to build advanced primitives.

Open Problems

- Use ISSIS and LW2E to build advanced primitives.
- Develop rich cryptanalysis for LW2E and ISSIS.

Open Problems

- Use ISSIS and LW2E to build advanced primitives.
- Develop rich cryptanalysis for LW2E and ISSIS.
- Construct PKE or other primitives from LW2E alone.
  - Propose another assumption that is potentially harder than both LWE and LPN, and can imply PKE without additional helper assumption.

Thank You!