Module Learning with Errors with General Distributions

Katharina Boudgoust
CNRS, Univ. Montpellier, LIRMM

Corentin Jeudy

Erkan Tairi

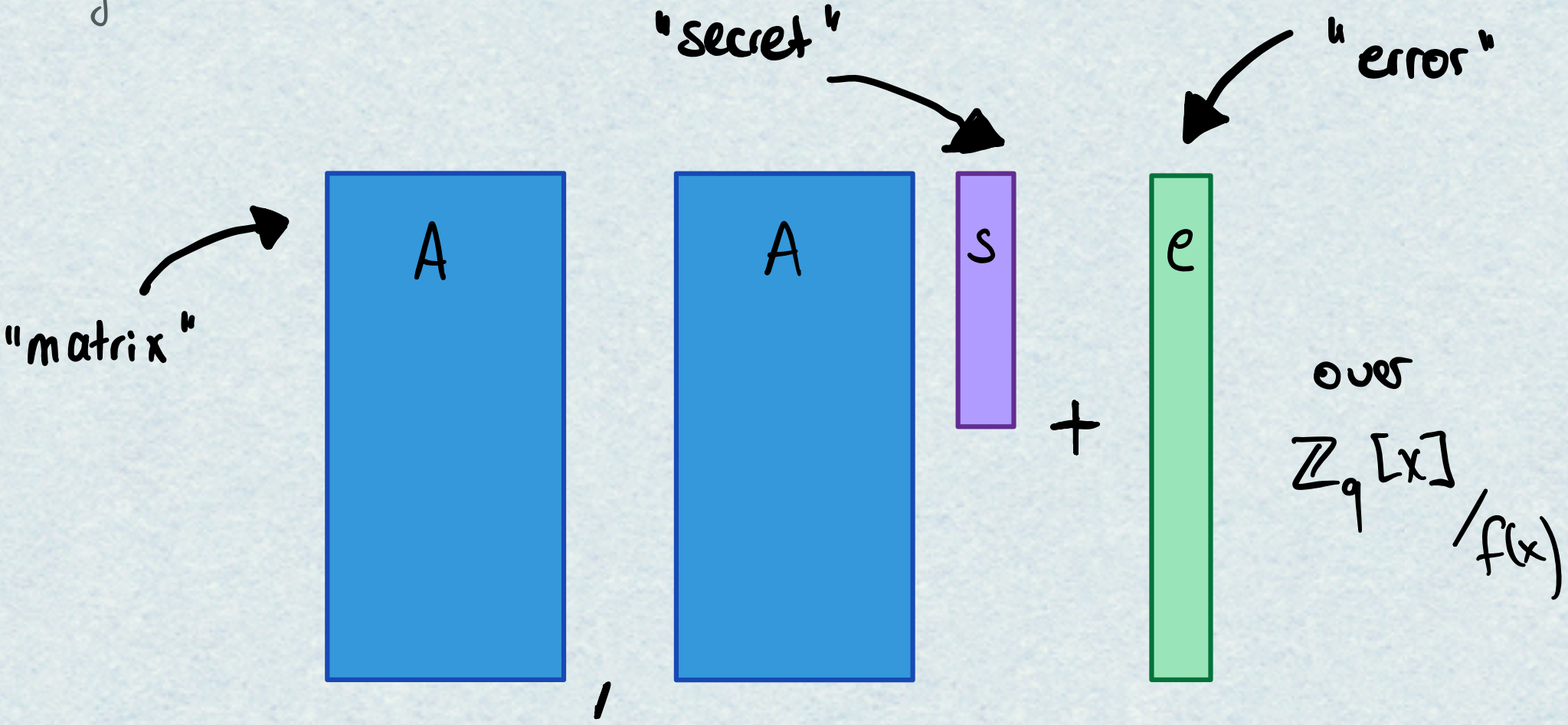
Weiqiang Wen

PKC'26

26.5.2026

Module Learning With Errors (M-LWE)

Langlois, Stehlé DCC'15

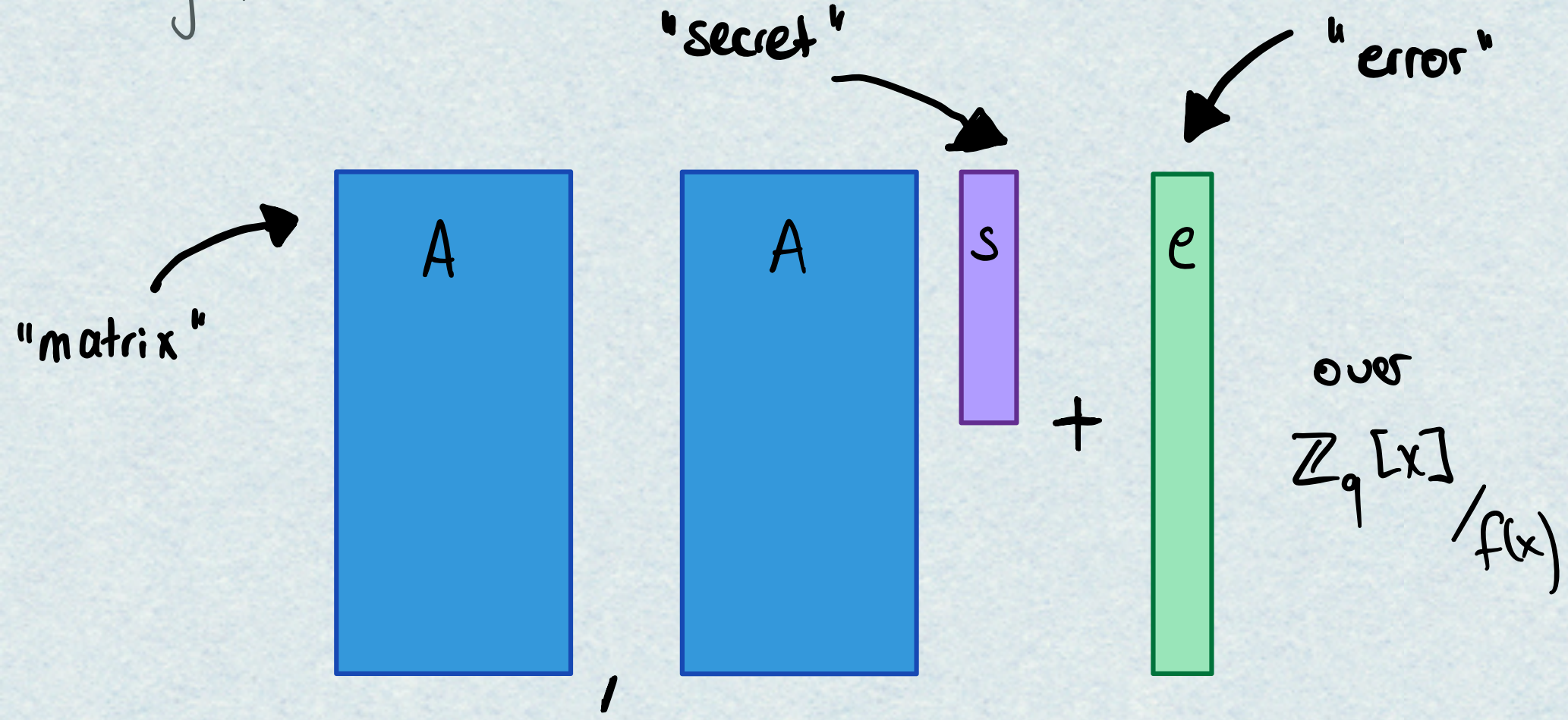


Search: Find s (or e)

Decision: Distinguish from (A, uniform)

Module Learning With Errors (M-LWE)

Roux-Langlois, Stehlé DCC'18



Choices:

* polynomial $f(x)$
* distribution of secret s
* distribution of error e
* distribution of matrix A

} flexible usage BUT non-trivial security analysis

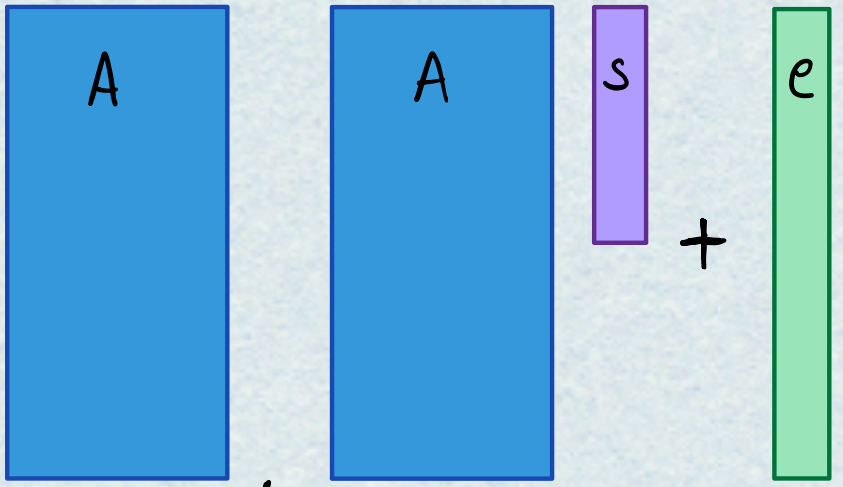
Standard Module Learning With Errors

Short Independent Vectors Problem
in ANY module lattice

quantum: Roux-Langlois, Stehlé JCC'15

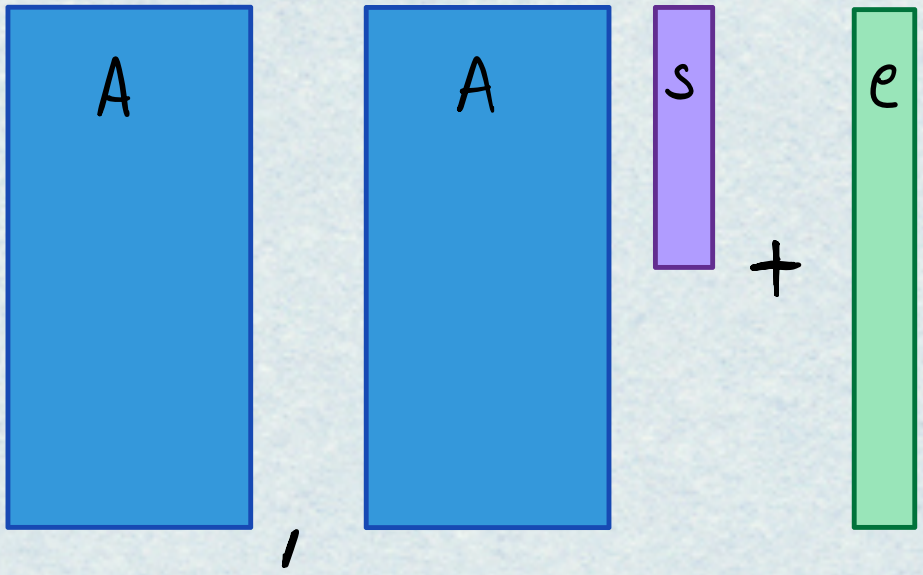
classical: Boudgoust, Jeudy Roux-Langlois, Wen Asiacrypt'20

* cyclotomic polynomial $f(x)$
* s uniform over $\mathbb{Z}_q[x]/f(x)$
* e discrete Gaussian
* A uniform over $\mathbb{Z}_q[x]/f(x)$



Variants of M-LWE

Module Learning With Errors Variants



* distribution of s: any as long as enough min-entropy

Brakerski, Döttling TCC '20
Boudgoust, Jeudy, Roux-Langlois, Wen Indocrypt '22
Lin, Wang, Zhuang, Wang TCS '24

Question: Can we show something similar for the distribution of e?

Our Results Part 1:

Search M-LWE with noise distribution $\mathcal{D}$ is as hard as standard M-LWE as long as:

1. samples of $\mathcal{D}$ are short
2. $\mathcal{D}$ has sufficient min-entropy
3. not too many samples are provided

Application: sparse ternary error distribution

Module Learning With Errors in Hermite Normal Form

Applebaum, Cash, Peikert, Sahai Crypto'09

s follows the same distribution as e

- both are short
- relevant for efficiency

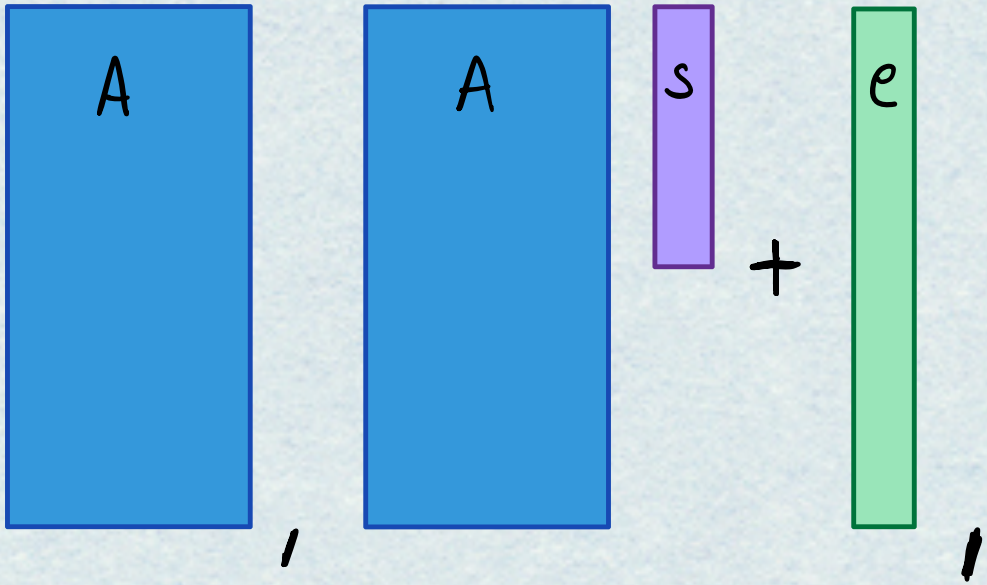
Our Results Part 2:

Search M-LWE with secret-noise distr. D is as hard as standard M-LWE as long as:

1. samples of D are short
2. D has sufficient min-entropy
3. not too many, but still enough samples are provided

We address a subtlety if the coefficients of $\binom{s}{e} \leftarrow D$ are correlated.

Module Learning With Errors Leaky Variants



$f(s,e)$

leakage function f

* within reductions
* leverage constructions

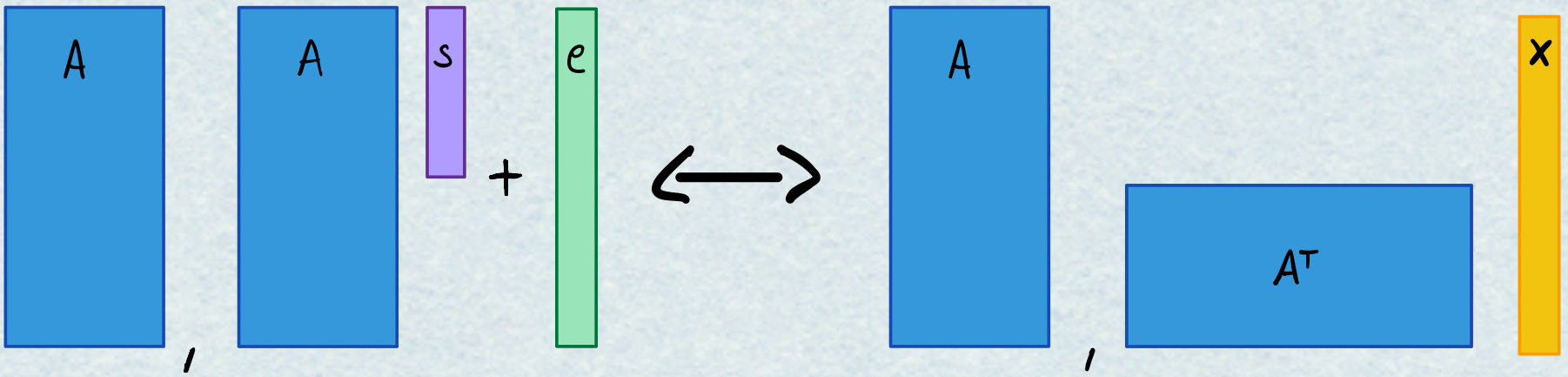
Our Results Part 3:

Search M-LWE with secret-noise distr. $\mathcal{D}$ and leakage $f(s,e)$ is as hard as standard M-LWE as long as:

1. samples of $\mathcal{D}$ are short
2. $\mathcal{D}$ has sufficient min-entropy conditioned on leakage f
3. not too many, but still enough samples are provided

Detailed Analysis for
* exact & approximate linear fct's
* some quadratic function
* some non-algebraic function

Proof Strategy for general error distribution



M-LWE M-Knap

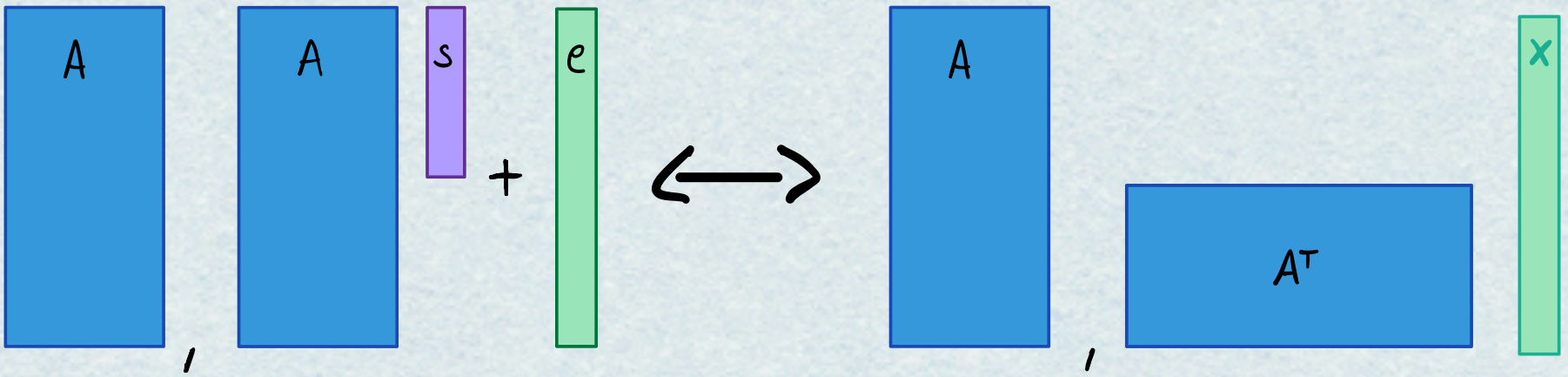
Function family $f_A(x) = A^T x$

Closely follows proofs for bounded uniform error

LWE: Micciancio & Peikert Crypto'13

M-LWE: Boudgoust, Jeudy, Roux-Langlois, Wen JoC'23

Proof Strategy for general error distribution



M-LWE

M-Knap

Function family $f_A(x) = A^T x$

Second preimage resistant → $(f_A)_A$ one-way ⇐⇒ search M-Knap is hard

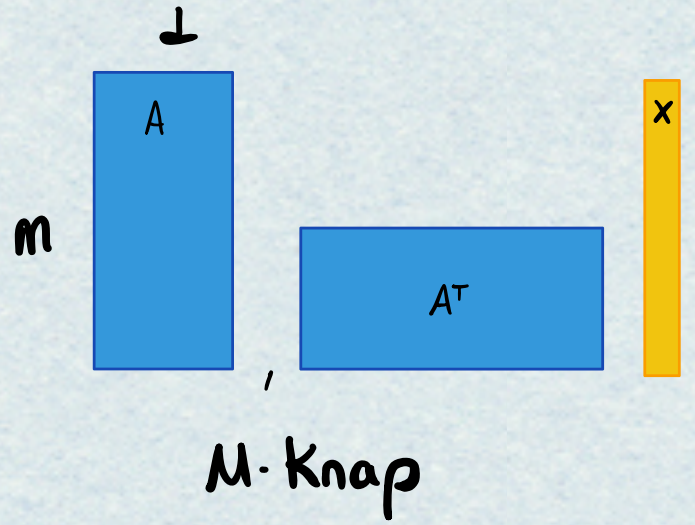
uninvertible →

Second-Preimage Resistance of M-Knap

Given $(A, x \leftarrow D)$

find $x' \neq x$ s.t. $A^T x = A^T x'$

$\epsilon \; Supp(D) = S$



$$\sum_{x' \in S \setminus \{x\}} \mathbb{P}_A \left[A^T(x - x') = 0 \right]$$

uniformly distributed over the ideal

$$\leq \left(|S| - 1 \right) \cdot \frac{Bound^d}{|R_q|^d}$$

loose

$$I = \langle x_1 - x_1', \ldots, x_m - x_m' \rangle$$

$$N(I) \leq Bound$$

Wrapping-UP:

Search M-LWE with secret-noise distr. $\mathcal{D}$

and leakage $f(s,e)$

is as hard as standard M-LWE

as long as:

1. samples of $\mathcal{D}$ are short
2. $\mathcal{D}$ has sufficient min-entropy conditioned on leakage f
3. not too many, but still enough samples are provided

Limitations:

* practical parameters not covered
* only search variant

Wrapping-UP:

Thanks !

Search M-LWE with secret-noise distr. $\mathcal{D}$

and leakage $f(s,e)$

is as hard as standard M-LWE

as long as:

1. samples of $\mathcal{D}$ are short
2. $\mathcal{D}$ has sufficient min-entropy conditioned on leakage f
3. not too many, but still enough samples are provided

Limitations:

* practical parameters not covered
* only search variant