The Hardness of LPN over Any **Integer Ring** and **Field** for **PCG Applications**

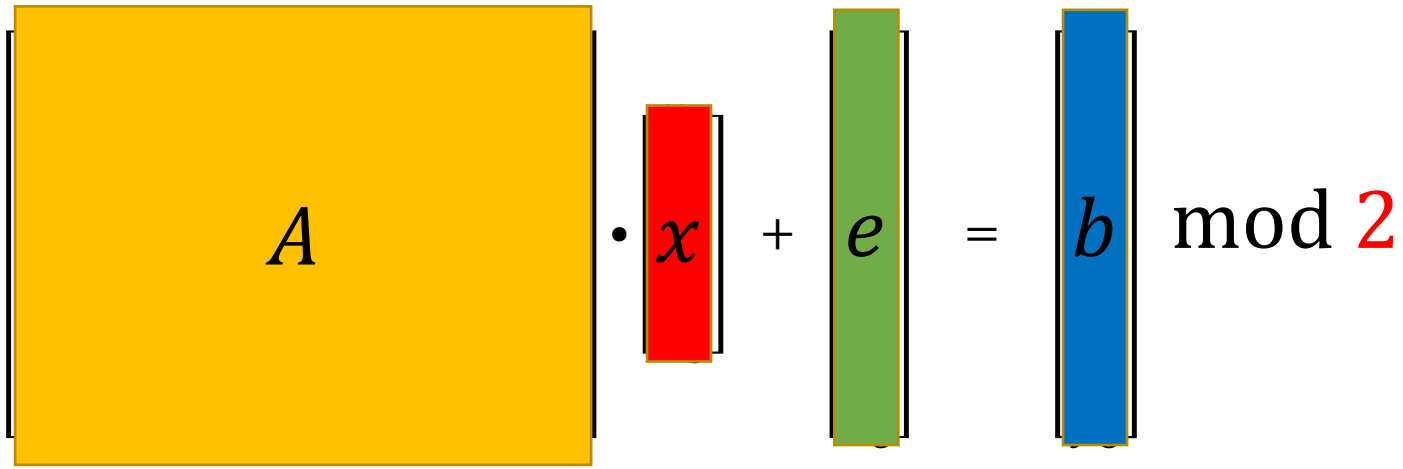
Hanlin Liu, Xiao Wang, Kang Yang, Yu Yu

State Key Laboratory of Cryptology

上海
期智研究院
SHANGHAI QI ZHI INSTITUTE

Learning Parity with Noise (LPN)

- $A \xleftarrow{\$} \mathbb{F}_2^{m \times n}, x \xleftarrow{\$} \mathbb{F}_2^n, e \leftarrow \mathrm{Ber}_{\mu}^m, b = Ax + e$



Search LPN
Given $(A, b = Ax + e)$,
figure out x

Learning Parity with Noise (LPN)

- $A \xleftarrow{\$} \mathbb{F}_2^{m \times n}, x \xleftarrow{\$} \mathbb{F}_2^n, e \leftarrow \mathrm{Ber}_{\mu}^m, b = Ax + e$

$\Pr[e_i = 1] = \mu$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \\ a_{61} & a_{62} & a_{63} & a_{64} & a_{65} \\ a_{71} & a_{72} & a_{73} & a_{74} & a_{75} \\ a_{81} & a_{82} & a_{83} & a_{84} & a_{85} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix} \bmod 2$$

Search LPN
Given $(A, b = Ax + e)$,
figure out x

Learning Parity with Noise (LPN)

- $A \xleftarrow{\$} \mathbb{F}_2^{m \times n}, x \xleftarrow{\$} \mathbb{F}_2^n, e \leftarrow \mathrm{Ber}_\mu^m, b = Ax + e$

$\Pr[e_i = 1] = \mu$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \\ a_{61} & a_{62} & a_{63} & a_{64} & a_{65} \\ a_{71} & a_{72} & a_{73} & a_{74} & a_{75} \\ a_{81} & a_{82} & a_{83} & a_{84} & a_{85} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix} \bmod 2$$

Search LPN
Given $(A, b = Ax + e)$,
figure out x

$\Leftrightarrow$ poly

Decisional LPN
Distinguish between
$(A, b = Ax + e)$ & $(A, z \xleftarrow{\$} \mathbb{F}_2^m)$

Learning Parity with Noise (LPN)

- $A \xleftarrow{\$} \mathbb{F}_2^{m \times n}, x \xleftarrow{\$} \mathbb{F}_2^n, e \leftarrow \mathrm{Ber}_\mu^m, b = Ax + e$

exact noise
regular noise

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \\ a_{61} & a_{62} & a_{63} & a_{64} & a_{65} \\ a_{71} & a_{72} & a_{73} & a_{74} & a_{75} \\ a_{81} & a_{82} & a_{83} & a_{84} & a_{85} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix}$$

mod q
mod 2^λ

Search LPN
Given $(A, b = Ax + e)$,
figure out x

$\Leftrightarrow$ poly

Decisional LPN
Distinguish between
$(A, b = Ax + e)$ & $(A, z \xleftarrow{\$} \mathbb{F}_2^m)$

LPN Variants Related with PCG

- Various noise distributions
  - Exact LPN: $e \xleftarrow{\$} \{e \mid e \in \mathbb{Z}_q^m \wedge \mathrm{HW}(e) = t\}$
  - Regular LPN: $e \xleftarrow{\$} \{(e_1, e_2, \cdots, e_t) \mid e_i \in \mathbb{Z}_q^{\frac{m}{t}} \wedge \mathrm{HW}(e_i) = 1\}$

LPN Variants Related with PCG

- Various noise distributions
  - Exact LPN: $e \xleftarrow{\$} \{e \mid e \in \mathbb{Z}_q^m \wedge \mathrm{HW}(e) = t\}$
  - Regular LPN: $e \xleftarrow{\$} \{(e_1, e_2, \cdots, e_t) \mid e_i \in \mathbb{Z}_q^{\frac{m}{t}} \wedge \mathrm{HW}(e_i) = 1\}$
- Various moduli

	Protocol	LPN type
[Boyle et al. CCS'19, Yang et al. CCS'22]	OT	$\mathbb{F}_2$
[Schoppmann et al. CCS'19]	VOLE	$\mathbb{F}_{2^{61}-1}$ and $\mathbb{Z}_{2^{64}}$
[Weng et al. S&P'21]	ZK	$\mathbb{F}_2$ and $\mathbb{F}_{2^{61}-1}$
[Franzese et al. CCS'21]	ZK	$\mathbb{F}_{2^{128}}$
[Rindal et al. Eurocrypt'21]	PSI	$\mathbb{F}_{2^{128}}$
[Baum et al. Crypto'21]	ZK	$\mathbb{F}_{2^{40}}$ and $\mathbb{F}_{2^{61}-1}$
[Baum et al. CCS'21]	ZK	$\mathbb{Z}_{2^{72}}$
[Baum et al. Crypto'22]	ZK	$\mathbb{Z}_{2^{104}}$

LPN Variants Related with PCG

- Various noise distributions
  - Exact LPN: $e \xleftarrow{\$} \{e \mid e \in \mathbb{Z}_q^m \wedge \mathrm{HW}(e) = t\}$
  - Regular LPN: $e \xleftarrow{\$} \{(e_1, e_2, \cdots, e_t) \mid e_i \in \mathbb{Z}_q^{\frac{m}{t}} \wedge \mathrm{HW}(e_i) = 1\}$
- Various moduli

How to estimate the hardness of these LPN variants?

	Protocol	LPN type
[Boyle et al. CCS'19, Yang et al. CCS'22]	OT	$\mathbb{F}_2$
[Schoppmann et al. CCS'19]	VOLE	$\mathbb{F}_{2^{61}-1}$ and $\mathbb{Z}_{2^{64}}$
[Weng et al. S&P'21]	ZK	$\mathbb{F}_2$ and $\mathbb{F}_{2^{61}-1}$
[Franzese et al. CCS'21]	ZK	$\mathbb{F}_{2^{128}}$
[Rindal et al. Eurocrypt'21]	PSI	$\mathbb{F}_{2^{128}}$
[Baum et al. Crypto'21]	ZK	$\mathbb{F}_{2^{40}}$ and $\mathbb{F}_{2^{61}-1}$
[Baum et al. CCS'21]	ZK	$\mathbb{Z}_{2^{72}}$
[Baum et al. Crypto'22]	ZK	$\mathbb{Z}_{2^{104}}$

Roadmap

The Hardness of Regular LPN

The Hardness of LPN over $\mathbb{Z}_{2^\lambda}$

Concrete Analysis for LPN

The Hardness of Regular LPN

- [Feneuil, Joux and Rivain, Crypto 2022, adapted]
  - exact LPN with t-noise is (T, ϵ)-hard → regular LPN with t-noise is $(T, e^t \cdot \epsilon)$-hard

The Hardness of Regular LPN

- [Feneuil, Joux and Rivain, Crypto 2022, adapted]
  - exact LPN with t-noise is (T, ϵ)-hard → regular LPN with t-noise is $(T, e^t \cdot \epsilon)$-hard

- Lager penalty factor $p_t = e^t$
  - In PCG parameters $2n \leq m$, exact LPN with t-noise is $(\text{poly(n)}, \epsilon)$-hard, for $\epsilon > e^{-t}$
  - Then, regular LPN with t-noise is $(\text{poly(n)}, e^t \cdot \epsilon > 1)$-hard

The Hardness of Regular LPN

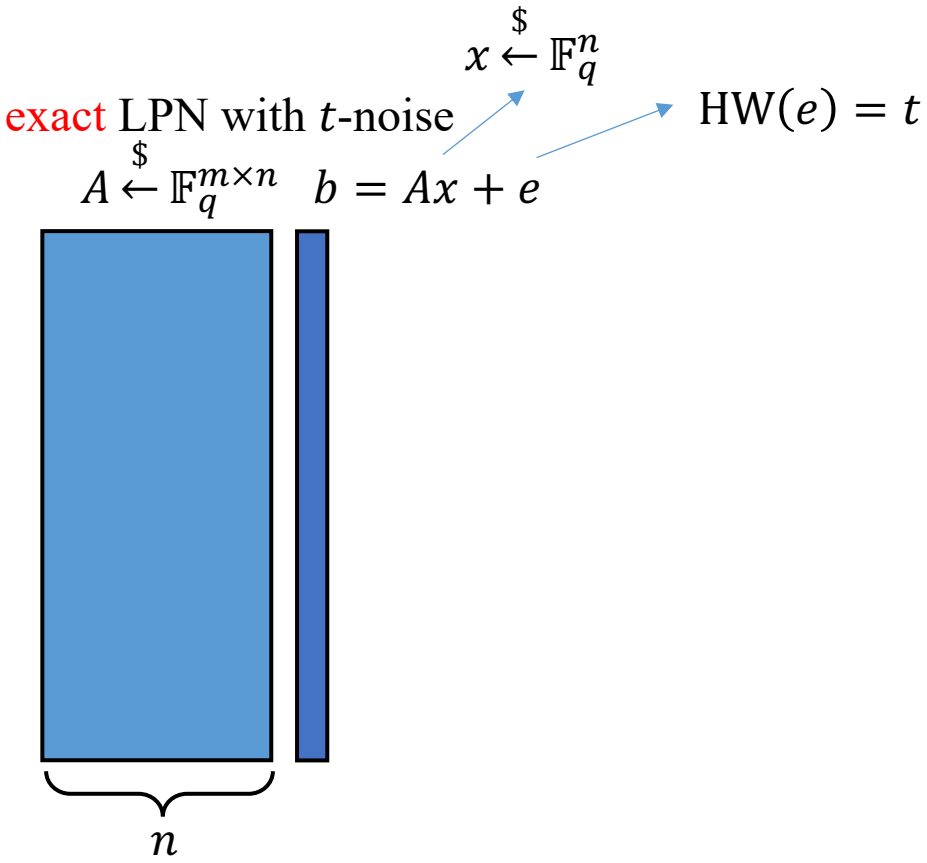
- [Feneuil, Joux and Rivain, Crypto 2022, adapted]
  - exact LPN with t-noise is (T, ϵ)-hard → regular LPN with t-noise is $(T, e^t \cdot \epsilon)$-hard

- Lager penalty factor $p_t = e^t$
  - In PCG parameters $2n \leq m$, exact LPN with t-noise is $(\text{poly(n)}, \epsilon)$-hard, for $\epsilon > e^{-t}$
  - Then, regular LPN with t-noise is $(\text{poly(n)}, e^t \cdot \epsilon > 1)$-hard

The Hardness of Regular LPN

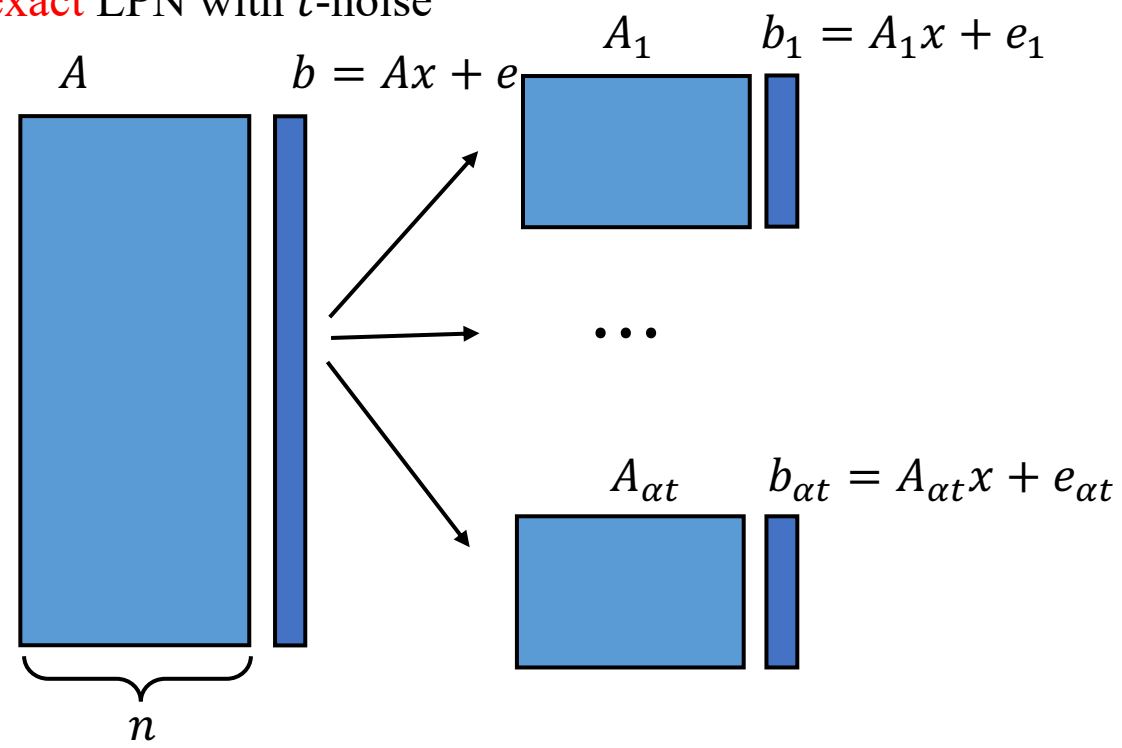
- [Feneuil, Joux and Rivain, Crypto 2022, adapted]
  - exact LPN with t-noise is (T, ϵ)-hard → regular LPN with t-noise is $(T, e^t \cdot \epsilon)$-hard
- Lager penalty factor $p_t = e^t$
  - In PCG parameters $2n \leq m$, exact LPN with t-noise is (poly(n), ϵ)-hard, for $\epsilon > e^{-t}$
  - Then, regular LPN with t-noise is (poly(n), $e^t \cdot \epsilon > 1$)-hard
- Our reduction: $p_t = 2^{\frac{t}{\alpha}}$
  - Additional parameter $\alpha \geq 2$
  - exact LPN with t-noise is (T, ϵ)-hard → regular LPN with αt-noise is $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard

(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise



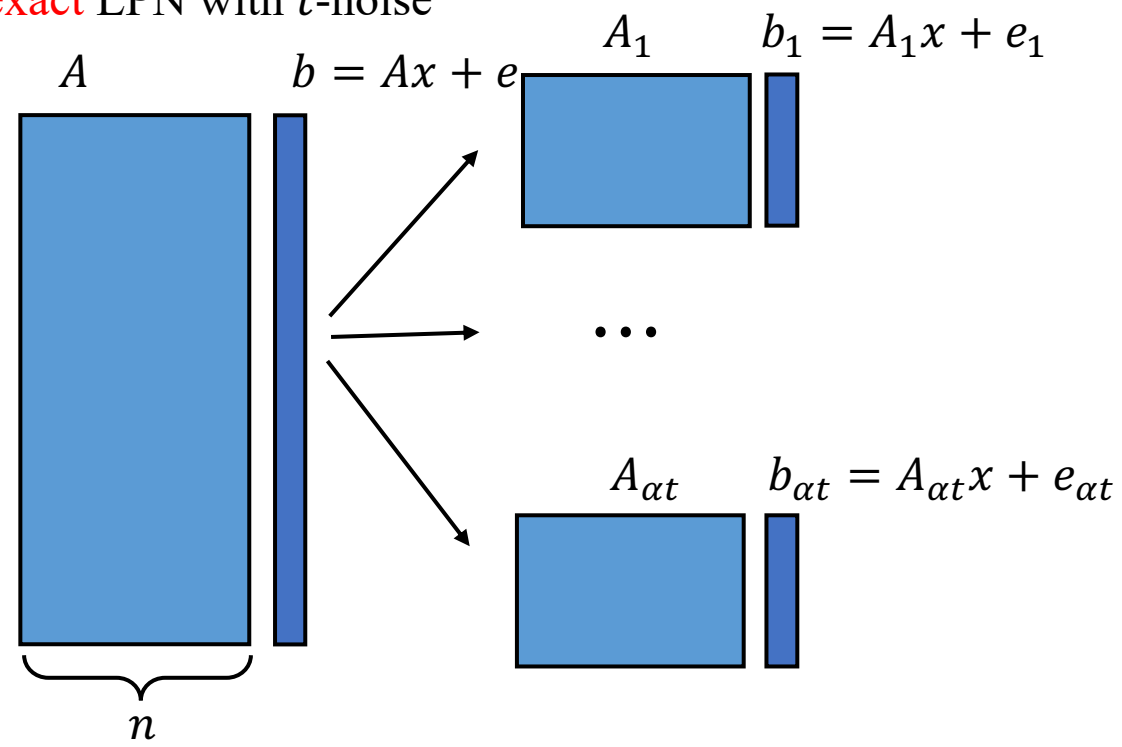
(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise

exact LPN with t-noise



(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise

exact LPN with t-noise



Q: why is penalty factor $p_t = 2^{\frac{t}{\alpha}}$?

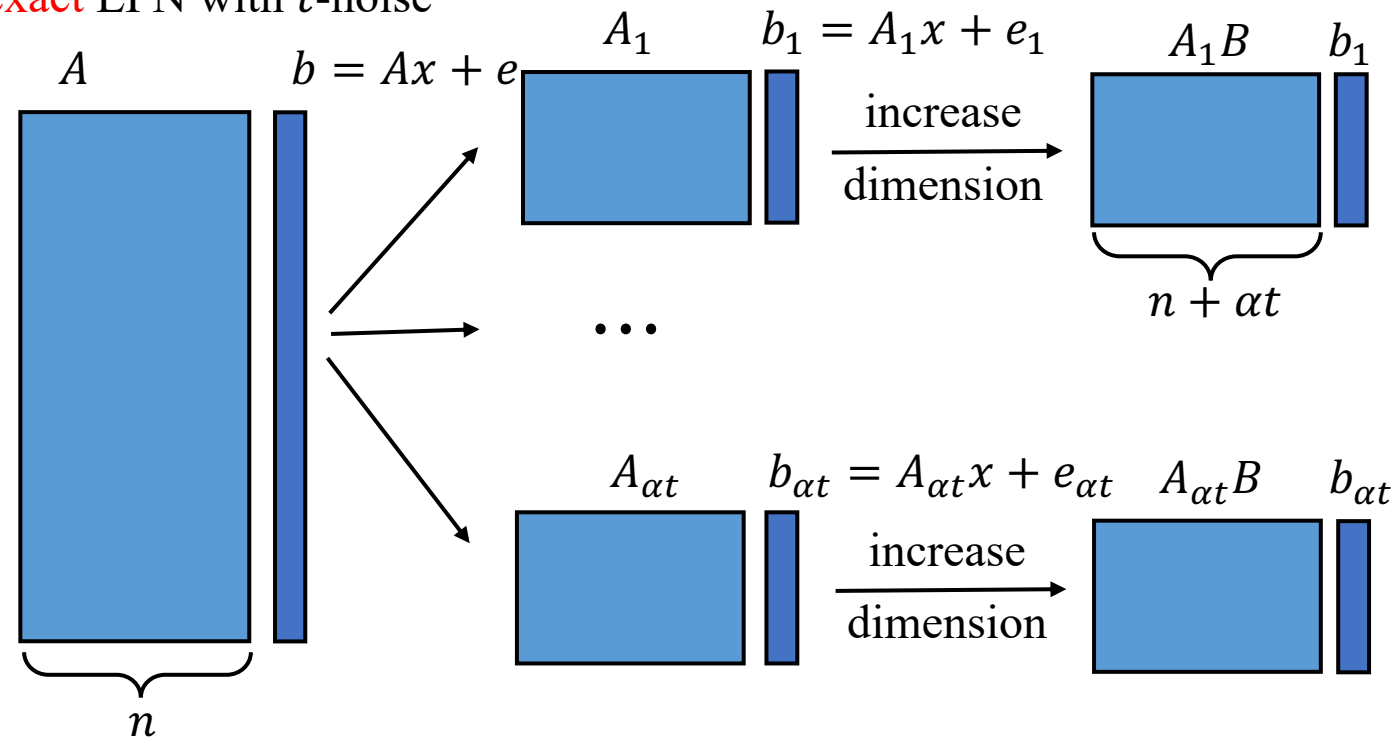
A: $\Pr[\mathrm{HW}(e_i) \leq 1, \forall i \in [\alpha t]\,] \approx 2^{-\frac{t}{\alpha}}$

(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise

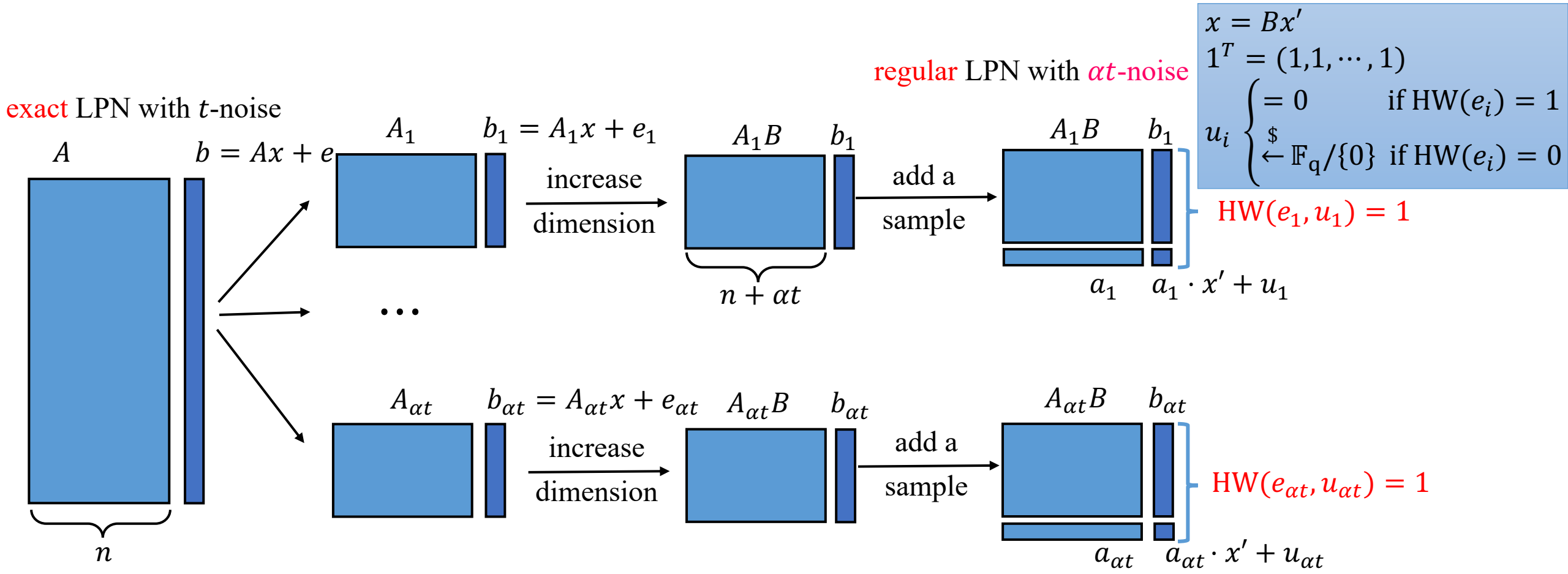
$A_i B x' = A_i x$, for each $i \in [\alpha t]$

$x = Bx'$

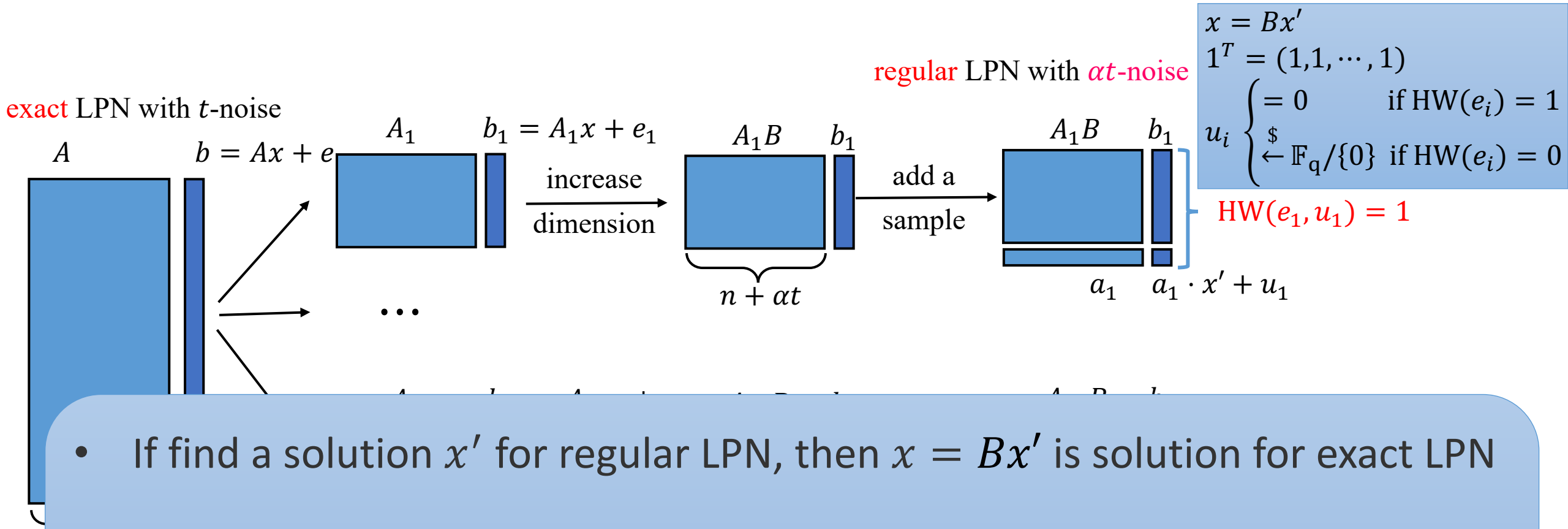
exact LPN with t-noise



(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise

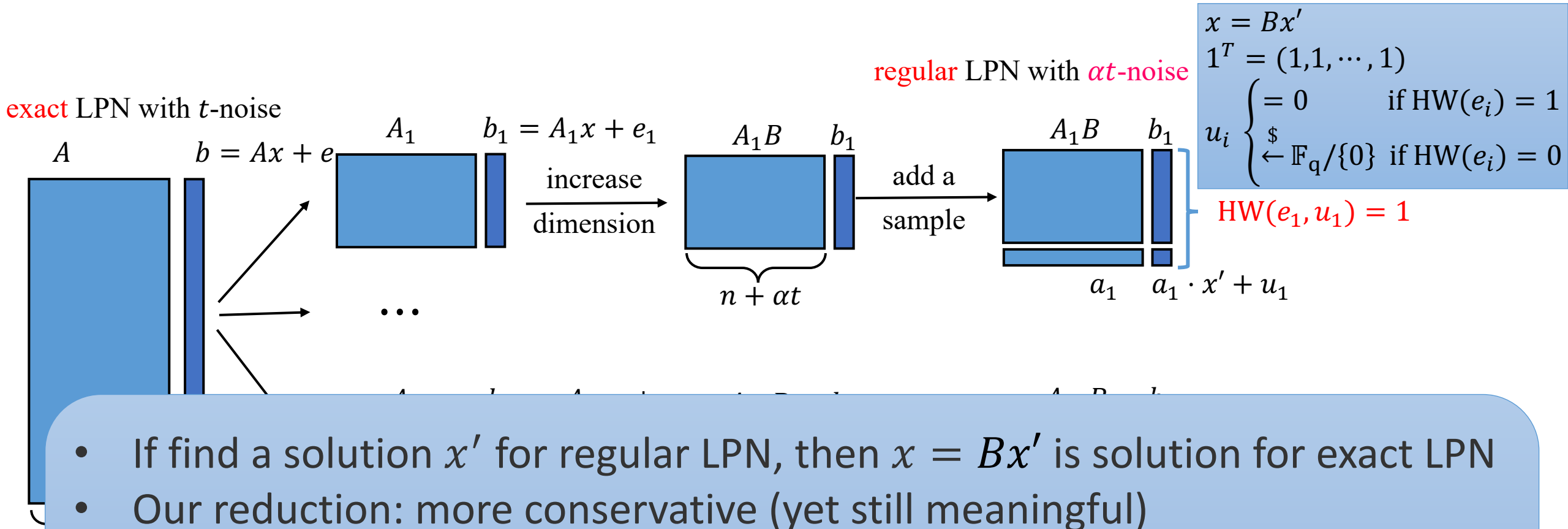


(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise



- If find a solution x' for regular LPN, then $x = Bx'$ is solution for exact LPN

(T, ϵ)-hard exact LPN with t-noise → $(T, 2^{\frac{t}{\alpha}} \cdot \epsilon)$-hard regular LPN with αt-noise



- If find a solution x' for regular LPN, then $x = Bx'$ is solution for exact LPN
- Our reduction: more conservative (yet still meaningful)
  - Noise's weight $t \rightarrow \alpha t$
  - Dimension $n \rightarrow n + \alpha t$
  - Reasonable, regular noise leaks αt bits

Roadmap

The Hardness of Regular LPN

The Hardness of LPN over $\mathbb{Z}_{2^\lambda}$

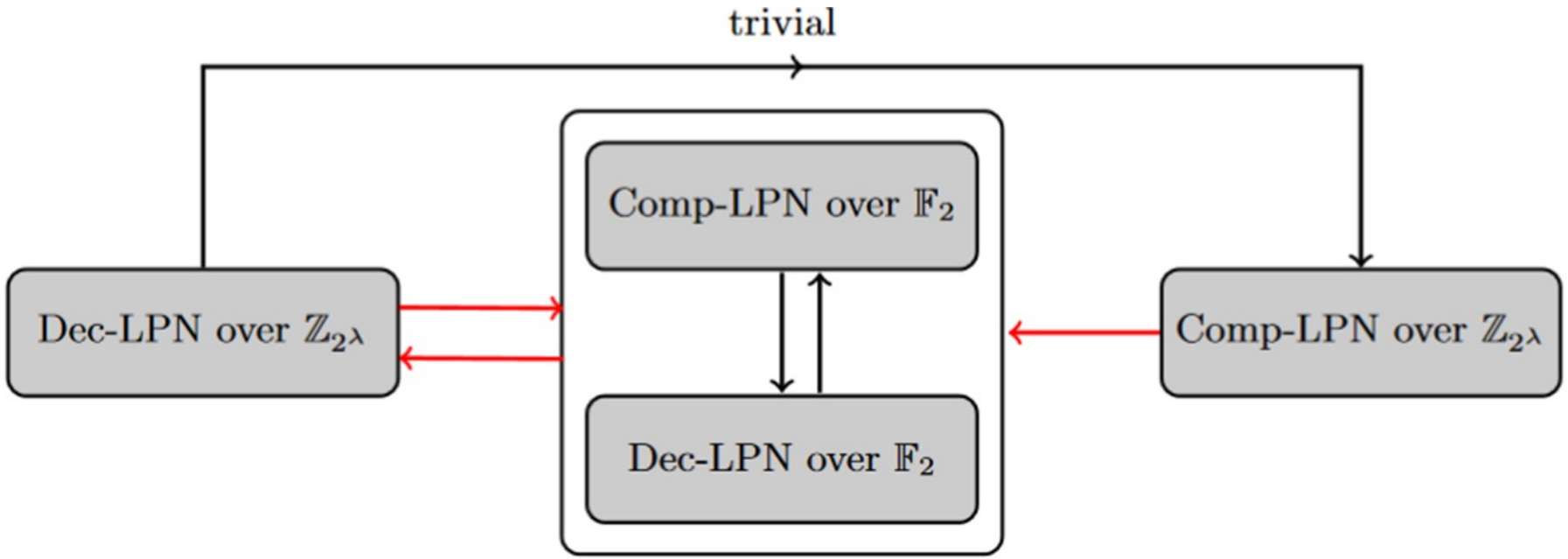
Concrete Analysis for LPN

The Hardness of LPN over $\mathbb{Z}_{2^\lambda}$

- Some prior works assume that LPN with t-noise over $\mathbb{Z}_{2^\lambda} \approx$ LPN with t-noise over $\mathbb{F}_2$

The Hardness of LPN over $\mathbb{Z}_{2^\lambda}$

- Some prior works assume that LPN with t-noise over $\mathbb{Z}_{2^\lambda} \approx$ LPN with t-noise over $\mathbb{F}_2$
- Our reductions:
  - LPN with t-noise over $\mathbb{Z}_{2^\lambda} \rightarrow$ LPN with $t/2$-noise over $\mathbb{F}_2$
  - Dec-LPN with t-noise over $\mathbb{F}_2 \rightarrow$ Dec-LPN with λt-noise over $\mathbb{Z}_{2^\lambda}$

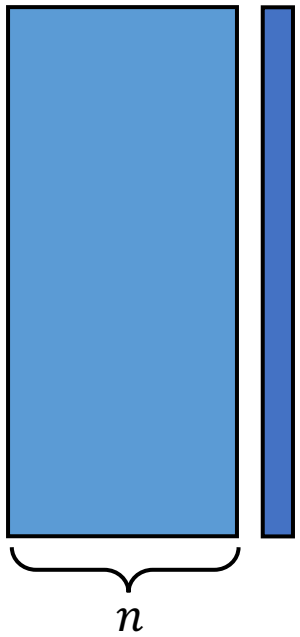


LPN with t-noise over $\mathbb{Z}_{2^\lambda}$ → LPN with $t/2$-noise over $\mathbb{F}_2$

$e \in \mathbb{Z}_{2^\lambda}^m$
$\mathrm{HW}(e) = t$

LPN with t-noise over $\mathbb{Z}_{2^\lambda}$

$b = Ax + e \bmod 2^\lambda$

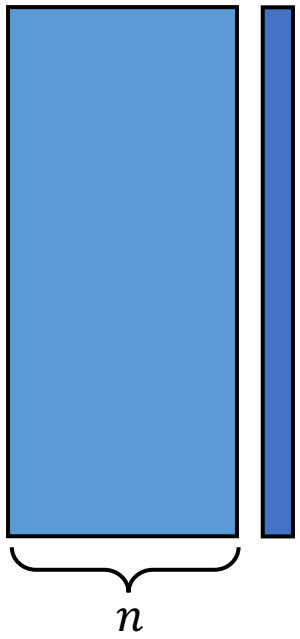


LPN with t-noise over $\mathbb{Z}_{2^\lambda}$ → LPN with $t/2$-noise over $\mathbb{F}_2$

$e \in \mathbb{Z}_{2^\lambda}^m$
$\mathrm{HW}(e) = t$

LPN with t-noise over $\mathbb{Z}_{2^\lambda}$

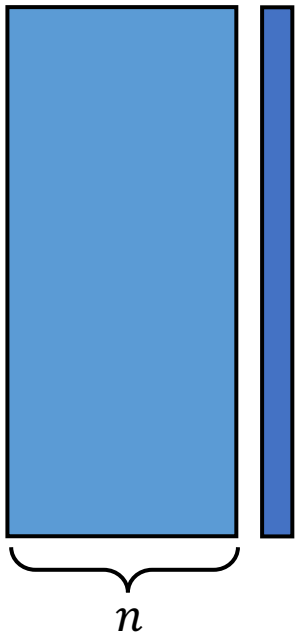
A $\quad b = Ax + e \bmod 2^\lambda$



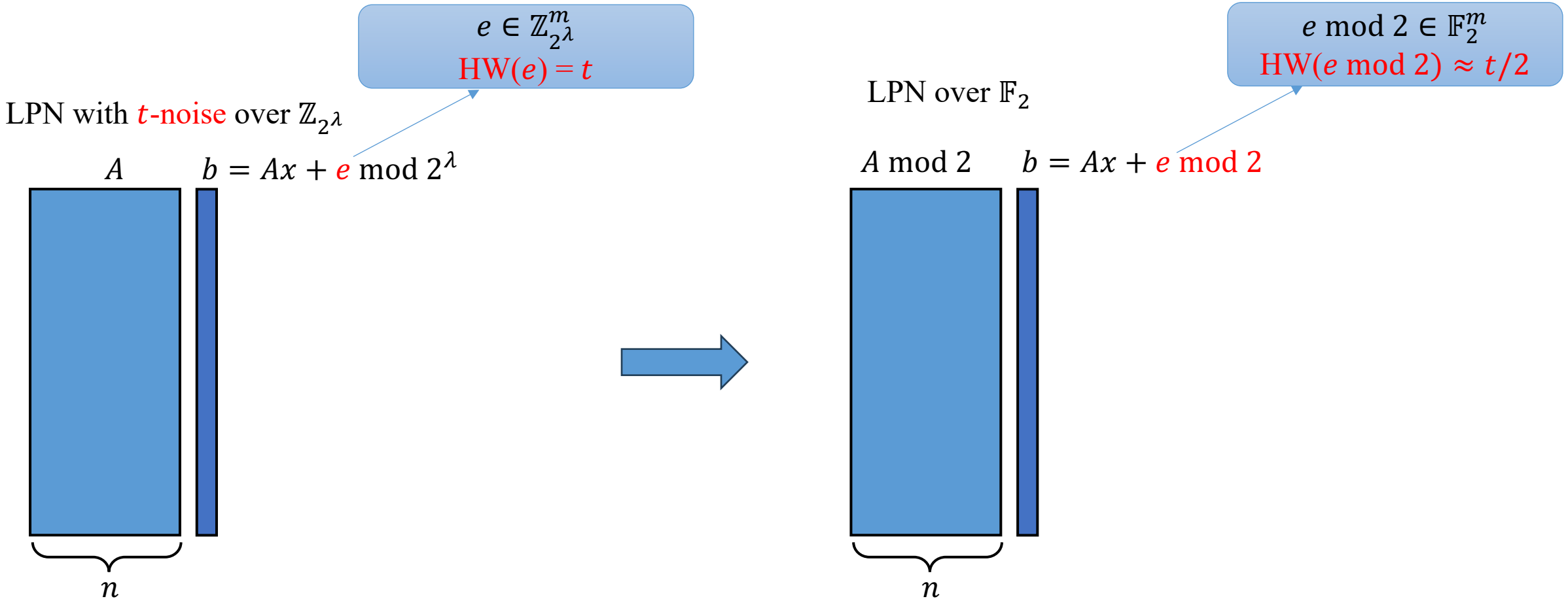
$e \bmod 2 \in \mathbb{F}_2^m$
$\mathrm{HW}(e \bmod 2) \approx t/2$

LPN over $\mathbb{F}_2$

$A \bmod 2$ $\quad b = Ax + e \bmod 2$



LPN with t-noise over $\mathbb{Z}_{2^\lambda}$ → LPN with $t/2$-noise over $\mathbb{F}_2$



Countermeasure [Baum et al. Crypto'22]

- (non-standard) noise $e \xleftarrow{\$} \{e \mid e \in \mathbb{Z}_{2^\lambda}^m \wedge \mathrm{HW}(e) = t \wedge \mathrm{HW}(e \bmod 2) = t\}$

Dec-LPN over $\mathbb{F}_2$ with $e \leftarrow \mathrm{Ber}_\mu^m \rightarrow$ Dec-LPN over $\mathbb{Z}_{2^\lambda}$ with $e \leftarrow \mathrm{IndBer}_\mu^m(\lambda)$

- Bit-decomposition function: for $a \in \mathbb{Z}_{2^\lambda}^n$, $(a_0, a_1, \cdots, a_{\lambda-1}) = \mathrm{decom}(a)$
  - $a_i \in \{0,1\}^n$
  - $\sum_{i=0}^{\lambda-1}(2^i \cdot a_i) = a$

Dec-LPN over $\mathbb{F}_2$ with $e \leftarrow \mathrm{Ber}_\mu^m$ $\rightarrow$ Dec-LPN over $\mathbb{Z}_{2^\lambda}$ with $e \leftarrow \mathrm{IndBer}_\mu^m(\lambda)$

- Bit-decomposition function: for $a \in \mathbb{Z}_{2^\lambda}^n$, $(a_0, a_1, \cdots, a_{\lambda-1}) = \mathrm{decom}(a)$
  - $a_i \in \{0,1\}^n$
  - $\sum_{i=0}^{\lambda-1}(2^i \cdot a_i) = a$

- Bit-wise independent Bernoulli: $e \leftarrow \mathrm{IndBer}_\mu(\lambda)$
  - $(e_0, e_1, \cdots, e_{\lambda-1}) = \mathrm{decom}(e)$
    - $\Pr[e_i = 1] = \mu$
    - $\Pr[e_i = 0] = 1 - \mu$

Dec-LPN over $\mathbb{F}_2$ with $e \leftarrow \mathrm{Ber}_{\mu}^{m}$ $\rightarrow$ Dec-LPN over $\mathbb{Z}_{2^\lambda}$ with $e \leftarrow \mathrm{IndBer}_{\mu}^{m}(\lambda)$

- Given input $\left(A \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^{m \times n}, b = Ax + e\right)$, where $x \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^{n}$ and $e \leftarrow \mathrm{IndBer}_{\mu}^{m}(\lambda)$

Dec-LPN over $\mathbb{F}_2$ with $e \leftarrow \mathrm{Ber}_{\mu}^{m}$ $\rightarrow$ Dec-LPN over $\mathbb{Z}_{2^\lambda}$ with $e \leftarrow \mathrm{IndBer}_{\mu}^{m}(\lambda)$

- Given input $\left(A \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^{m \times n}, b = Ax + e\right)$, where $x \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^{n}$ and $e \leftarrow \mathrm{IndBer}_{\mu}^{m}(\lambda)$
- $(b_0, b_1, \cdots, b_{\lambda-1}) \coloneqq \mathrm{decom}(b)$

Dec-LPN over $\mathbb{F}_2$ with $e \leftarrow \mathrm{Ber}_\mu^m$ → Dec-LPN over $\mathbb{Z}_{2^\lambda}$ with $e \leftarrow \mathrm{IndBer}_\mu^m(\lambda)$

- Given input $\left(A \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^{m\times n}, b = Ax + e\right)$, where $x \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^n$ and $e \leftarrow \mathrm{IndBer}_\mu^m(\lambda)$
- $(b_0, b_1, \cdots, b_{\lambda-1}) \coloneqq \mathrm{decom}(b)$
- Define the hybrid distributions $H_0, \cdots, H_\lambda$

$$H_0 = (A, u_0, \cdots, u_{i-1}, u_i, u_{i+1}, \cdots, u_{\lambda-1})$$
$$\vdots$$
$$H_i = (A, b_0, \cdots, b_{i-1}, u_i, u_{i+1}, \cdots, u_{\lambda-1})$$
$$H_{i+1} = (A, b_0, \cdots, b_{i-1}, b_i, u_{i+1}, \cdots, u_{\lambda-1})$$
$$\vdots$$
$$H_\lambda = (A, b_0, \cdots, b_{i-1}, b_i, b_{i+1}, \cdots, b_{\lambda-1})$$

where each $u_i \xleftarrow{\$} \{0,1\}^m$

Dec-LPN over $\mathbb{F}_2$ with $e \leftarrow \mathrm{Ber}_\mu^m$ → Dec-LPN over $\mathbb{Z}_{2^\lambda}$ with $e \leftarrow \mathrm{IndBer}_\mu^m(\lambda)$

- Given input $\left(A \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^{m\times n}, b = Ax + e\right)$, where $x \xleftarrow{\$} \mathbb{Z}_{2^\lambda}^n$ and $e \leftarrow \mathrm{IndBer}_\mu^m(\lambda)$
- $(b_0, b_1, \cdots, b_{\lambda-1}) \coloneqq \mathrm{decom}(b)$

Dec-LPN over $\mathbb{F}_2$ → $H_i \approx H_{i+1}$

- Define the hybrid distributions $H_0, \cdots, H_\lambda$

$$H_0 = (A, u_0, \cdots, u_{i-1}, u_i, u_{i+1}, \cdots, u_{\lambda-1})$$
$$\vdots$$
$$H_i = (A, b_0, \cdots, b_{i-1}, u_i, u_{i+1}, \cdots, u_{\lambda-1})$$
$$H_{i+1} = (A, b_0, \cdots, b_{i-1}, b_i, u_{i+1}, \cdots, u_{\lambda-1})$$
$$\vdots$$
$$H_\lambda = (A, b_0, \cdots, b_{i-1}, b_i, b_{i+1}, \cdots, b_{\lambda-1})$$

where each $u_i \xleftarrow{\$} \{0,1\}^m$

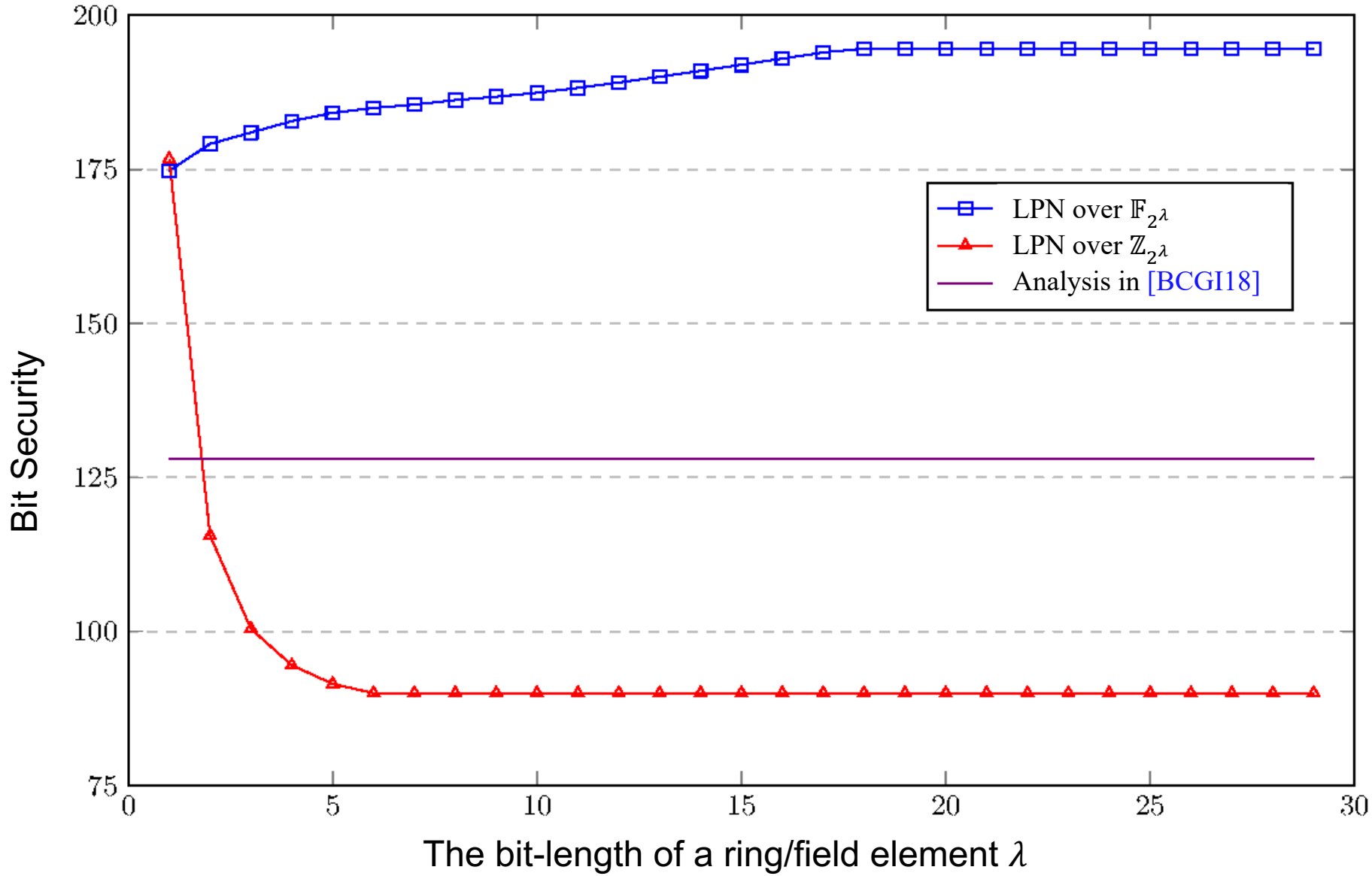
Roadmap

The Hardness of Regular LPN

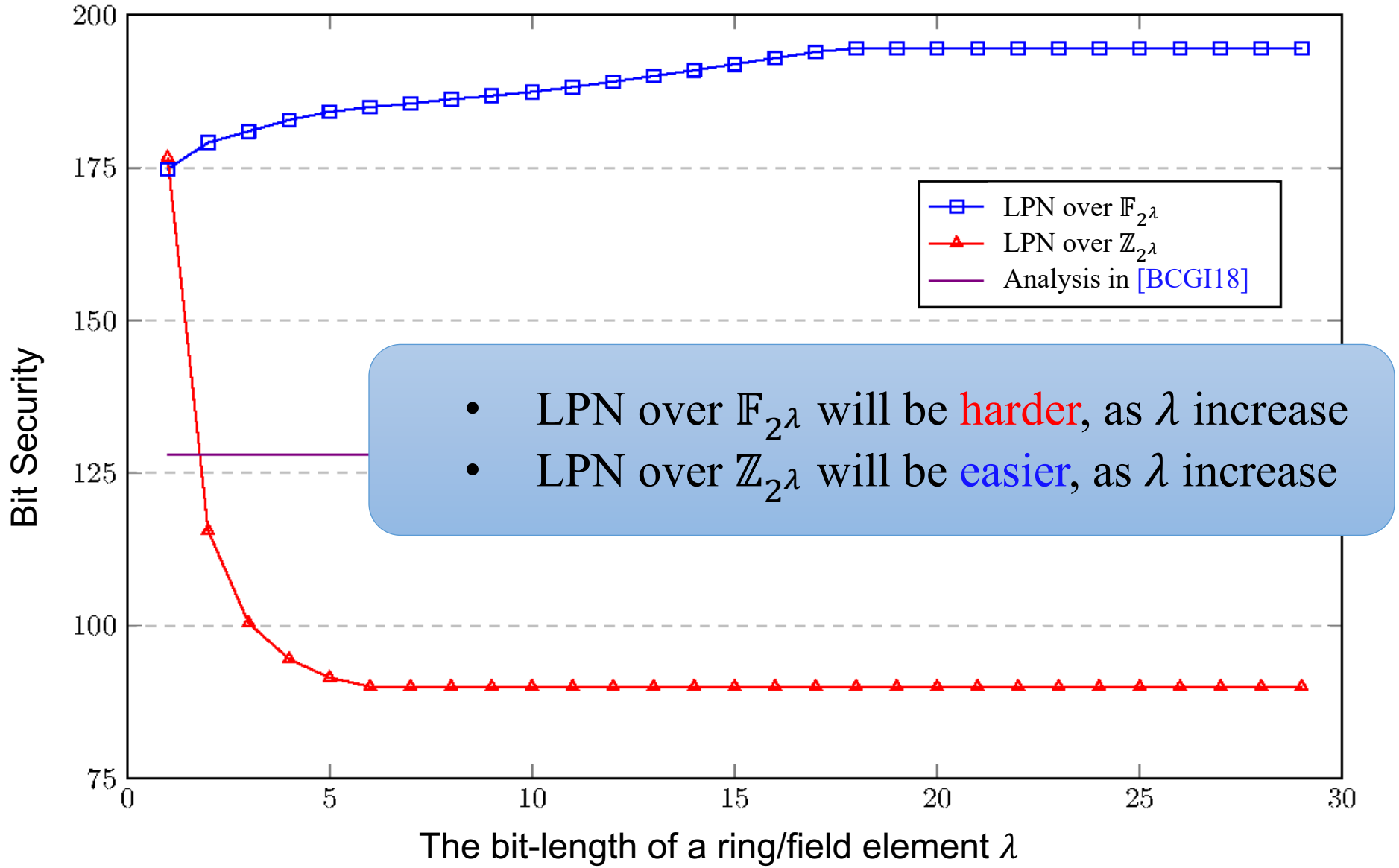
The Hardness of LPN over $\mathbb{Z}_{2^\lambda}$

Concrete Analysis for LPN

Concrete Analysis for LPN



Concrete Analysis for LPN



Concrete Analysis for LPN in PCG Parameter

Regular LPN over $\mathbb{F}$			$(\log\|\mathbb{F}\| = 128)$					$(\log\|\mathbb{F}\| = 1)$				
N	k	t	Gauss	SD	SD 2.0	ISD	AGB	Gauss	SD	SD 2.0	ISD	AGB
2^{10}	652	57	111	184	184	111	111	106	183	108	90	101
2^{12}	1589	98	100	151	151	100	107	96	146	130	80	103
2^{14}	3482	198	101	149	149	101	110	97	143	136	83	106
2^{16}	7391	389	103	147	147	103	111	99	141	138	87	108
2^{18}	15336	760	105	146	146	105	107	101	140	138	92	104
2^{20}	32771	1419	107	145	145	107	102	104	139	139	97	98
2^{22}	67440	2735	108	144	144	108	104	106	138	138	101	103

Gauss **Pooled Gauss [EKM17]**

SD **Statistical decoding algorithm [DT17, Zic17]**

SD 2.0 **Lower bound of SD 2.0 [CDMT22] adapted to the low-noise setting**

ISD **Information set decoding [Ste88, Dum91, MMT11, BJMM12]**

AGB **The recent algebraic approach [BØ23] only for regular LPN**

Concrete Analysis for LPN in PCG Parameter

Regular LPN over $\mathbb{F}$			$(\log\|\mathbb{F}\| = 128)$					$(\log\|\mathbb{F}\| = 1)$				
N	k	t	Gauss	SD	SD 2.0	ISD	AGB	Gauss	SD	SD 2.0	ISD	AGB
2^{10}	652	57	111	184	184	111	111	106	183	108	90	101
2^{12}	1589	98	100	151	151	100	107	96	146	130	80	103
2^{14}	3482	198	101	149	149	101	110	97	143	136	83	106
2^{16}	7391	389	103	147	147	103	111	99	141	138	87	108
2^{18}	15336	760	105	146	146	105	107	101	140	138	92	104
2^{20}	32771	1419	107	145	145	107	102	104	139	139	97	98
2^{22}	67440	2735	108	144	144	108	104	106	138	138	101	103

Gauss Pooled Gauss [EKM17]

SD Statistical decoding algorithm

SD 2.0 Lower bound of SD 2.0 [CDMT22] adapted to the low-noise setting

ISD Information set decoding [Ste88, Dum91, MMT11, BJMM12]

AGB The recent algebraic approach [BØ23] only for regular LPN

For exact LPN, ISD is the best.
For regular LPN, both ISD and AGB are best.

Concrete Analysis for LPN in PCG Parameter

Regular LPN over $\mathbb{F}$			$(\log\|\mathbb{F}\| = 128)$					$(\log\|\mathbb{F}\| = 1)$				
N	k	t	Gauss	SD	SD 2.0	ISD	AGB	Gauss	SD	SD 2.0	ISD	AGB
2^{10}	652	57	111	184	184	111	111	106	183	108	90	101
2^{12}	1589	98	100	151	151	100	107	96	146	130	80	103
2^{14}	3482	198	101	149	149	101	110	97	143	136	83	106
2^{16}	7391	389	103	147	147	103	111	99	141	138	87	108
2^{18}	15336	760	105	146	146	105	107	101	140	138	92	104
2^{20}	32771	1419	107	145	145	107	102	104	139	139	97	98
2^{22}	67440	2735	108	144	144	108	104	106	138	138	101	103

Gauss Pooled Gauss [EKM17]

SD Statistical decoding algorithm [DT17, Zic17]

SD 2.0 Lower bound of SD 2.0 [CDMT22] adapted to the low-noise setting

ISD Information set decoding [Ste88, Dum91, MMT11, BJMM12]

AGB The recent algebraic approach [BØ23] only for regular LPN

Regular LPN is easier to attack.

Two Ways to Enhance Regular-LPN Security

- Increasing the noise weight t
- Increasing the dimension k

Two Ways to Enhance Regular-LPN Security

- Increasing the noise weight t
- **Increasing the dimension k** ✓
  - The Bootstrapping-iteration technique [Yang et al. CCS2020]

Comparison of dimensions between exact-LPN and regular-LPN for 128-bit security

#Samples	Weight	Dimension for $\log\|\mathbb{F}\| = 128$		Dimension for $\log\|\mathbb{F}\| = 1$	
		Exact-LPN	Regular-LPN	Exact-LPN	Regular-LPN
2^{12}	172	1321	1377(+4.2%)	1549	1657(+7.0%)
2^{14}	338	2895	2909(+0.5%)	3373	3655(+8.3%)
2^{16}	667	6005	6091(+1.4%)	6956	7560(+8.7%)
2^{18}	1312	12160	14796(+21.7%)	13898	15996(+15.1%)
2^{20}	2467	25346	30978(+22.2%)	28289	33354(+17.9%)
2^{22}	4788	50854	75396(+48.3%)	55408	80074(+44.5%)

Thanks for Listening!