Smoothing Out Binary Linear Codes and Worst-case Sub-exponential Hardness for LPN

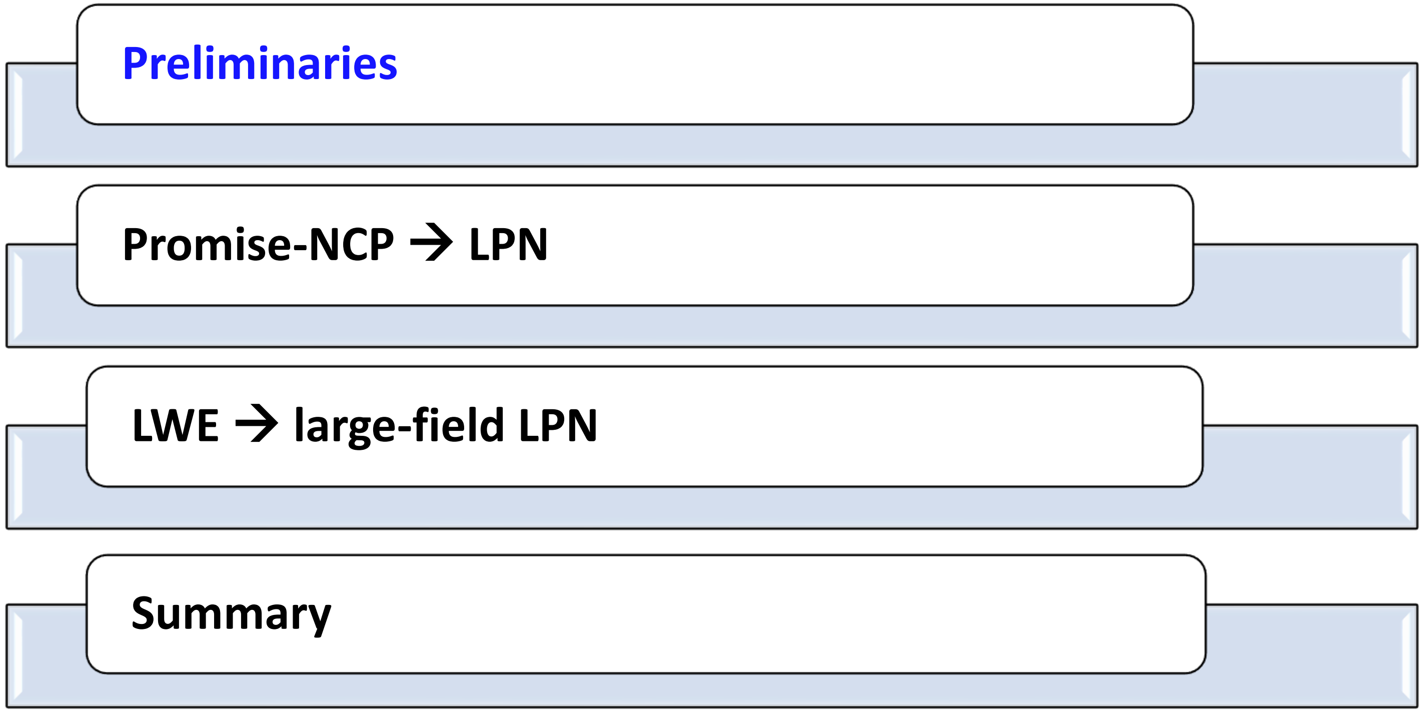
Yu Yu & Jiang Zhang

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

上海 期智研究院 SHANGHAI QI ZHI INSTITUTE

2021.08

Roadmap



Preliminaries

Promise-NCP → LPN

LWE → large-field LPN

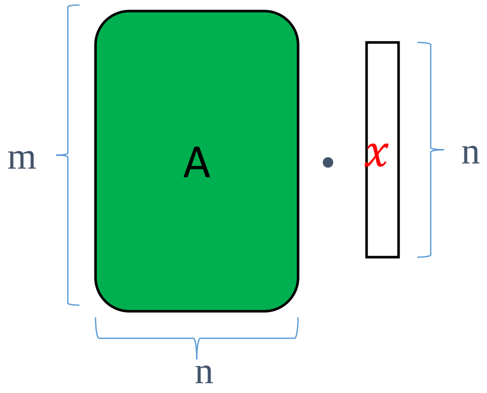
Summary

Binary Linear Codes

- **(n,m)- code**

  $\mathbb{F}_2^n \to \mathbb{F}_2^m$

  $x \;\mapsto\; A \cdot x$



- **(n,m,d)-code** minimum distance $d \overset{\text{def}}{=} \min_{x \neq 0} |\; Ax \;|$
- ***β*-balanced**

  minimum distance: $min_{x \neq 0} |\; Ax \;| \overset{\text{def}}{=} \left(\frac{1}{2} - \beta\right) m$

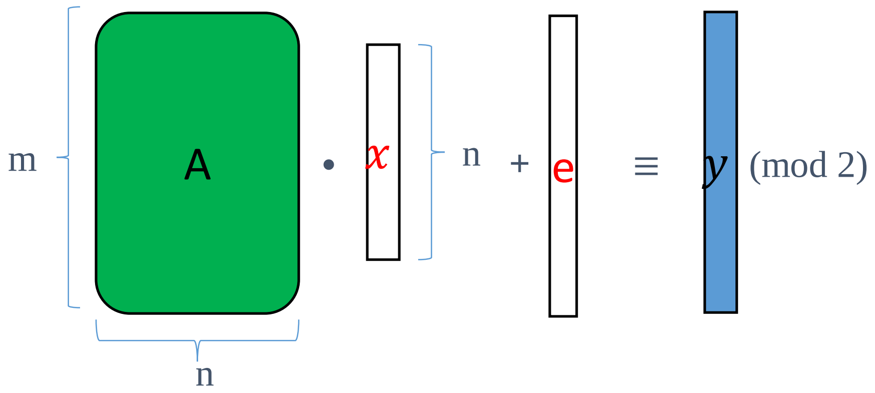
  maximum distance: $max_x \quad |\; Ax \;| \overset{\text{def}}{=} \left(\frac{1}{2} + \beta\right) m$
- **k-independent**

  every $k\times\, n$ submatrix of A has full rank

Decoding Linear Codes

- **The decoding problem**

  Find out x given $(A, y = Ax + e)$



- **LPN (Learning Parity with Noise)**

  $A \overset{\$}{\leftarrow} \mathbb{F}_2^{m\times n}, x \overset{\$}{\leftarrow} \mathbb{F}_2^n, e \sim \mathrm{Ber}_{\frac{w}{m}}^m$ $\quad (\mathrm{Exp}[|e|] = w)$

- **promise-NCP (Nearest Codeword Problem)**

  $A \in \mathbb{F}_2^{m\times n}, x \in \mathbb{F}_2^n, e \in \mathbb{F}_2^m$ with promise $|e| = w$

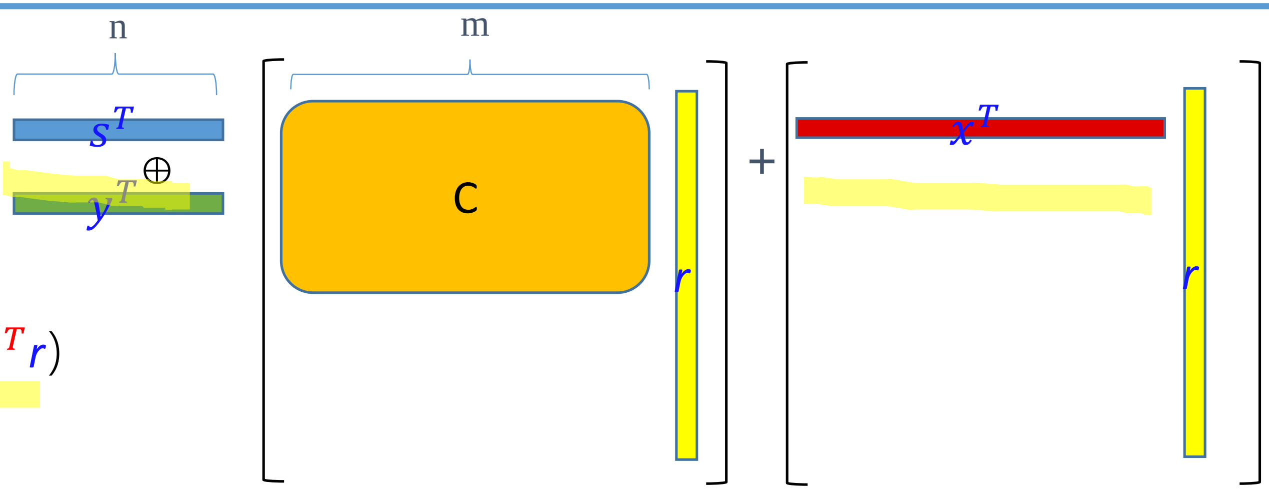
How hard is decoding linear code?

Problem	Best attack
Standard LPN $\frac{\boldsymbol{w}}{\boldsymbol{m}} =$ O(1)<0.5	$2^{O(n/\log n)}$ BKW03
High-noise Promise-NCP $w \geq \left(\frac{1}{2}+\epsilon\right)d$	NP-hard DMS03
Low-noise LPN/promise-NCP $\frac{\boldsymbol{w}}{\boldsymbol{m}} = \frac{\mathbf{1}}{\sqrt{n}}$	$poly(n,m) \cdot 2^{O\left(\frac{w}{m}n\right)} = 2^{O(\sqrt{n})}$
Extremely low-noise LPN/promise-NCP $\frac{\boldsymbol{w}}{\boldsymbol{m}} = \frac{(\log n)^2}{n}$	$poly(n,m) \cdot 2^{O\left(\frac{w}{m}n\right)} = n^{O(\log n)}$

[BKW03] Blum, A., Kalai, A., & Wasserman, H. (2003). Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM (JACM)*, *50*(4), 506-519.

NCP ⇒ LPN

- (transposed) NCP instance: $(C, s^TC + x^T)$
- an NCP instance ⇒ an LPN sample:



1. $r \leftarrow \mathrm{Sparse(m, d)}$, $y^T \overset{\$}{\leftarrow} \mathbb{F}_2^n$
2. $(Cr, (s^TC + x^T)r + y^TCr) \;=\; (Cr, \underbrace{(s^T + y^T)}_{\sim \mathrm{U}_n}Cr + x^Tr)$

Smoothing lemma [BLVW19] : For balanced code C and $r \leftarrow \boxed{\mathrm{Sparse(m, d)}}$

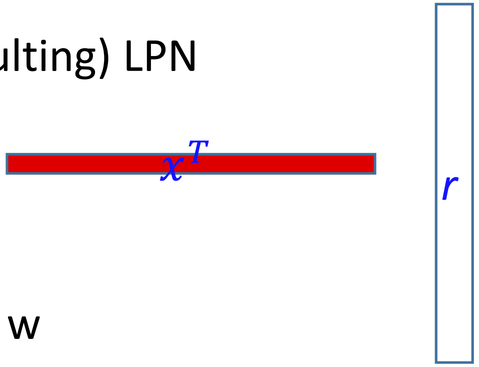
$$(\,Cr, x^Tr\,) \;\approx_s (\mathrm{U}_n\,, \mathrm{Ber}_\mu\,)$$

Proof. (binary) Fourier Transform [BLVW19] or linear distinguisher (Vazirani's XOR lemma) [This work]

[BLVW19] Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan, and Daniel Wichs. *Worst-case hardness for LPN and cryptographic hashing via code smoothing*. EUROCRYPT 2019

On the Sparse(m,d) Distribution of r

$x^T r$ becomes the noise of the (resulting) LPN

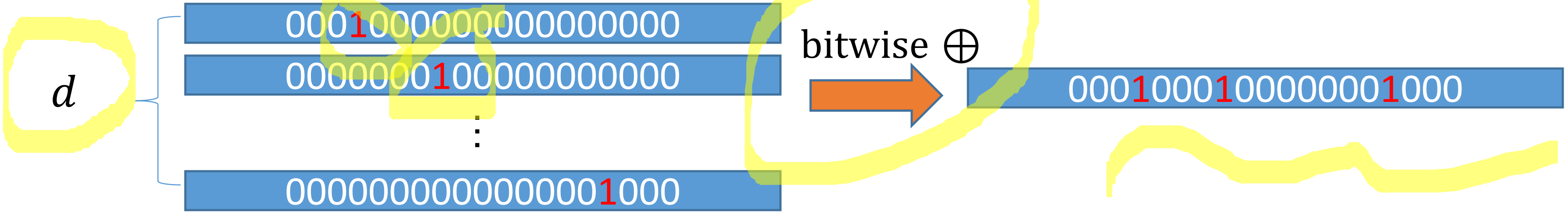


x^T: an m-bit error vector of weight w

$r \leftarrow \mathrm{Sparse}(\mathrm{m},\mathrm{d})$: the m-bit distribution of weight ≈d, entropy $\approx \log\binom{d}{m}$

LPN's noise rate $\mu = \Pr[x^T r = 1] = \frac{1}{2} - 2^{-\Theta\left(\frac{w}{m}d\right)}$

- **Option** 1: a uniform distribution over length-m-weight-d strings
- **Option** 2: [BLVW19] : the XOR of d length-m-weight-1 strings



- **Option** 3: [This work]: the m-fold Bernoulli distribution of rate $\frac{\mathrm{d}}{\mathrm{m}}$,denoted by $\mathrm{Ber}^{m}_{\frac{d}{m}}$

The main result of [BLVW19]

Smoothing lemma [BLVW19] : For any β −balanced code C, any x^T of weight w, and $r \leftarrow \mathrm{Sparse(m, d)}$

$$\text{Stat-Dist}\left(\;(Cr,\, x^T r) \;,\; (\mathrm{U}_n \,,\, \mathrm{Ber}_\mu) \;\right) \leq \; 2^{\frac{n}{2}} \left(2\frac{w}{m} + \beta\right)^d$$

where

- NCP’s noise rate: $\frac{w}{m} = \frac{\lambda \cdot \log n}{n}$ with $\lambda = \omega(1)$ (known attacks of complexity $n^{O(\lambda)}$)
- LPN’s noise rate: $\mu = \frac{1}{2} - 2^{-\Theta\left(\frac{w}{m}d\right)}$
- Gilbert–Varshamov bound: $\beta = O(\sqrt{\frac{n}{m}})$
- Entropy condition: $d = \Omega(n/\log n)$

Theorem [BLVW19] : Assumption: promise-NCP of noise $\frac{w}{m} = \frac{\lambda \cdot \log n}{n}$ is $n^{O(\lambda)}$$-\mathrm{wc}-\mathrm{hard}$,

Conclusion: LPN of noise $\frac{1}{2} - 2^{-\Theta(\lambda)}$ is $n^{O(\lambda)}$$-\mathrm{ac}-\mathrm{hard}$

The range of λ : $\omega(1) \leq \lambda \leq O(\log n)$

Corollary $(\lambda = \log n\,)$ **:** LPN of noise $\frac{1}{2} - \frac{1}{\mathrm{poly(n)}}$ is $n^{O(\log n)}$ -ac-hard

Roadmap

Preliminaries

Promise-NCP → LPN

LWE → large-field LPN

Summary

(Non-constructive) existential analysis

Smoothing lemma : ∃ code C of portion $\left(1-2^{w\log m-\frac{n}{2}}\right)$: for any x^T of weight w, and $r \leftarrow \mathrm{Sparse(m,d)}$

$$\text{Stat-Dist}\left(\ (Cr,\ x^T r)\ ,\ \ (\mathrm{U}_n, x^T r) \ \right) \le 2^{-\Omega(n)}$$

where entropy H(r)=log $\binom{d}{m} \approx d\log\frac{m}{d} = \Omega(n)$, $x^T r \sim \mathrm{Ber}_\mu$ with $\mu = \frac{1}{2} - 2^{-\Theta\left(\frac{w}{m}d\right)}$

Proof.

Leftover Hash Lemma

Markov's inequality

Union bound

for $C \sim \mathrm{U}_{n\times m}$ Stat-Dist$\left(\ (Cr,\ x^T r)\ ,\ \ (\mathrm{U}_n, x^T r) \ \right) \le 2^{-n}$

for any x^T : ∃ ($\le 2^{-\frac{n}{2}}$)-fraction of bad C s.t. Stat-Dist$\left(\ (Cr,\ x^T r)\ ,\ \ (\mathrm{U}_n, x^T r) \ \right) > 2^{-\frac{n}{2}}$

for all length-m-weight-w x^T : bad C's of fraction $\le \binom{w}{m} \cdot 2^{-\frac{n}{2}} = 2^{w\log\frac{m}{w}-\frac{n}{2}}$

To Prove Constant-Noise LPN:

1. LPN's noise: $\mu = \frac{1}{2} - 2^{-\Theta\left(\frac{w}{m}d\right)} = \Theta(1) \quad \Leftrightarrow \quad \frac{w}{m}d = \Theta(1)$
2. Entropy: $d\log\frac{m}{d} = \Omega(n)$

bad C's fraction $\binom{w}{m} \cdot 2^{-\frac{n}{2}} = 2^{\underbrace{w\log\frac{m}{w}}_{}-\frac{n}{2}}$ >> 1 (useless!)

$$\underset{\text{Eq.1}}{=} \Omega\left(\frac{m}{d}\log d\right) \underset{\text{Eq.2}}{=} 2^{\Omega(n/d)}\log d = n^{\omega(1)}$$

Not possible unless the above inequalities (esp. the union bound) can be circumvented

Observation

- Easy-to-prove: $Cr \approx_s \mathrm{U}_n$
- Much worse: $\forall |x^T| = w$: $(Cr, x^T r) \approx_s (U_n, x^T r)$

Observation:

For $r \leftarrow \mathrm{Ber}_{\frac{d}{m}}^m$ (important: r is coordinate-wise independent),

$$\text{Stat−Dist}(\,(Cr, x^T r)\;,(U_n, x^T r)\,) \le \frac{\text{Stat−Dist}(cr, \mathrm{U}_n)}{\left(1-\frac{2d}{m}\right)^w} \approx \frac{\text{Stat−Dist}(cr, \mathrm{U}_n)}{(1-2\mu)}$$

μ : LPN’s noise

- **almost** tight (w.r.t. $r \leftarrow \mathrm{Ber}_{\frac{d}{m}}^m$)
- Suffices to bound Stat−Dist(Cr, U_n) for a specific (balanced/independent) code C

proof omitted…

Main result I

Theorem. Assume NCP for balanced/independent code is (T,ϵ)-wc-hard,

Then, $\mathrm{LPN}_{n,\mu,q}$ is $\left(T - O(nmq), \epsilon + \frac{q\cdot 2^{-\Omega(d)}}{1-2\mu}\right)$-ac-hard for $\mu = \frac{1}{2} - 2^{-\Theta\left(\frac{w}{m}d\right)}$ and $d\log\left(\frac{m}{d}\right) = \Theta(n)$.

Corollary 1 ([BLVW19]-like). Assume promise-NCP of noise $\frac{w}{m} = \frac{\lambda\cdot\log n}{n}$ is $n^{O(\lambda)}$–wc–hard,
Then, LPN of noise $\frac{1}{2} - 2^{-\Theta(\lambda)}$ is $n^{O(\lambda)}$–ac–hard for any $\omega(1) \le \lambda \le O(\log n)$

Proof. Set $\frac{w}{m} = \frac{\lambda\cdot\log n}{n}$, $d = O\left(\frac{n}{\log n}\right)$, $m = n^{1+\epsilon}$

$\mathrm{m} = n^{1+\epsilon}$	Noise rate of LPN [BLVW19]	Noise rate of LPN (Corollary 1)
$m = n^{1.2}$	$\mu = \frac{1}{2} - n^{-14}$	$\mu = \frac{1}{2} - n^{-58}$
$m = n^{2}$	$\mu = \frac{1}{2} - n^{-3}$	$\mu = \frac{1}{2} - n^{-12}$
$m = n^{3}$	$\mu = \frac{1}{2} - n^{-3}$	$\mu = \frac{1}{2} - n^{-6}$
$m = n^{9}$	$\mu = \frac{1}{2} - n^{-3}$	$\mu = \frac{1}{2} - n^{-1.4}$
$m = n^{10}$	$\mu = \frac{1}{2} - n^{-3}$	$\mu = \frac{1}{2} - n^{-1.3}$
$m = n^{100}$	$\mu = \frac{1}{2} - n^{-3}$	$\mu = \frac{1}{2} - n^{-0.1}$

[BLVW19] 's smoothing lemma:

$$2^{\frac{n}{2}}\left(2\frac{w}{m} + 2\sqrt{\frac{n}{m}}\right)^{d}$$

Main result II

Theorem. Assume NCP for balanced/independent code is (T,ϵ)-wc-hard.

Then, $\mathrm{LPN}_{n,\mu,q}$ is $(T-O(nmq), \epsilon+\frac{q\cdot 2^{-\Omega(d)}}{1-2\mu})$-ac-hard for $\mu=\frac{1}{2}-2^{-\Theta\left(\frac{w}{m}d\right)}$ and $d\log(\frac{m}{d})=\Theta(n)$.

Corollary 2. Sub-exponential hardness for standard LPN!

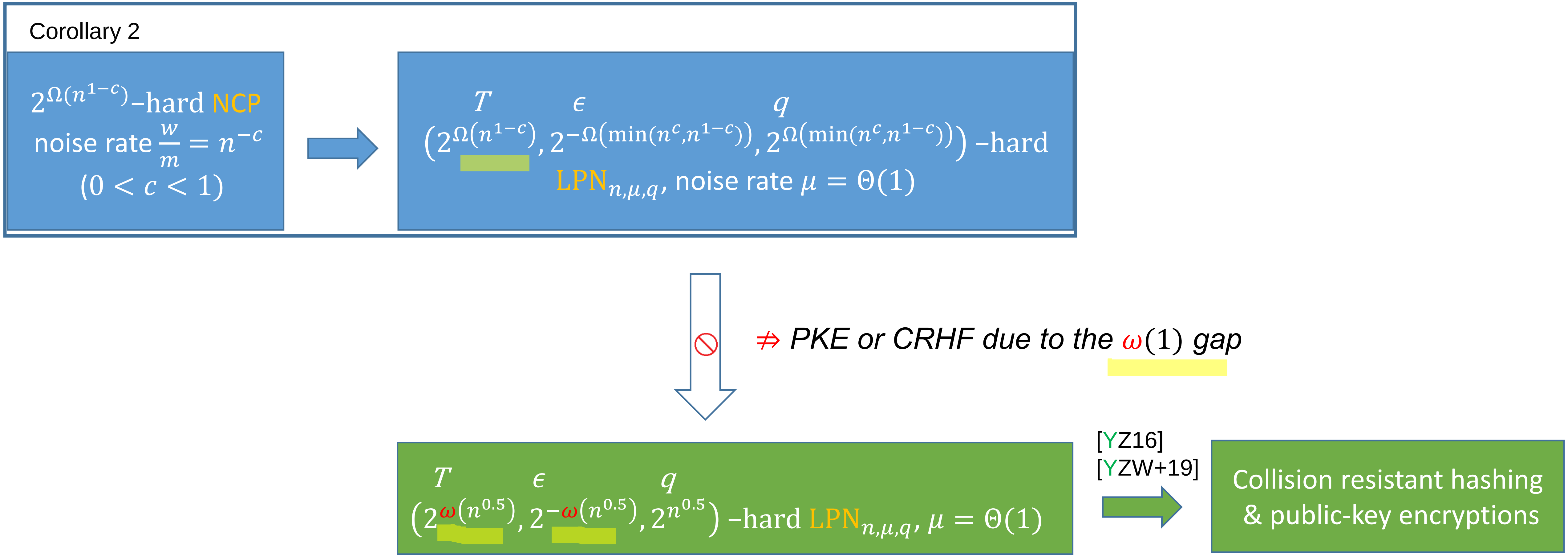
Assume NCP of noise $\frac{w}{m}=n^{-c}$ is $2^{\Omega(n^{1-c})}$–wc–hard (optimal up to a constant), Then,

- case $0<c\le\frac{1}{2}$: $\mathrm{LPN}_{n,\mu,q}\left(2^{\Omega(n^{1-c})}, 2^{-\Omega(n^{c})}\right)$ –ac–hard for constant $0<\ \mu<\frac{1}{2}$ and $q=2^{O(n^{c})}$
- case $\frac{1}{2}<c<1$: $\mathrm{LPN}_{n,\mu,q}\left(2^{\Omega(n^{1-c})}, 2^{-\Omega(n^{1-c})}\right)$ –ac–hard for constant $0<\ \mu<\frac{1}{2}$ and $q=2^{O(n^{1-c})}$

Proof. Set $\frac{w}{m}=n^{-c}, d=O(n^{c}), \mu=\Theta(1),\ \ \epsilon+\frac{q\cdot 2^{-\Omega(d)}}{1-2\mu}=2^{-\Omega(n^{1-c})}+2^{-\Omega(n^{c})}$

Applications (Unsuccessful Attempt I)

Base collision resistant hashing / public-key encryption on the worst-hardness of NCP ?



Corollary 2

$2^{\Omega(n^{1-c})}$–hard NCP
noise rate $\frac{w}{m} = n^{-c}$
$(0 < c < 1)$

$\left(\overset{T}{2^{\Omega(n^{1-c})}}, \overset{\epsilon}{2^{-\Omega(\min(n^c,n^{1-c}))}}, \overset{q}{2^{\Omega(\min(n^c,n^{1-c}))}}\right)$ –hard $\mathrm{LPN}_{n,\mu,q}$, noise rate $\mu = \Theta(1)$

⇏ *PKE or CRHF due to the* $\omega(1)$ *gap*

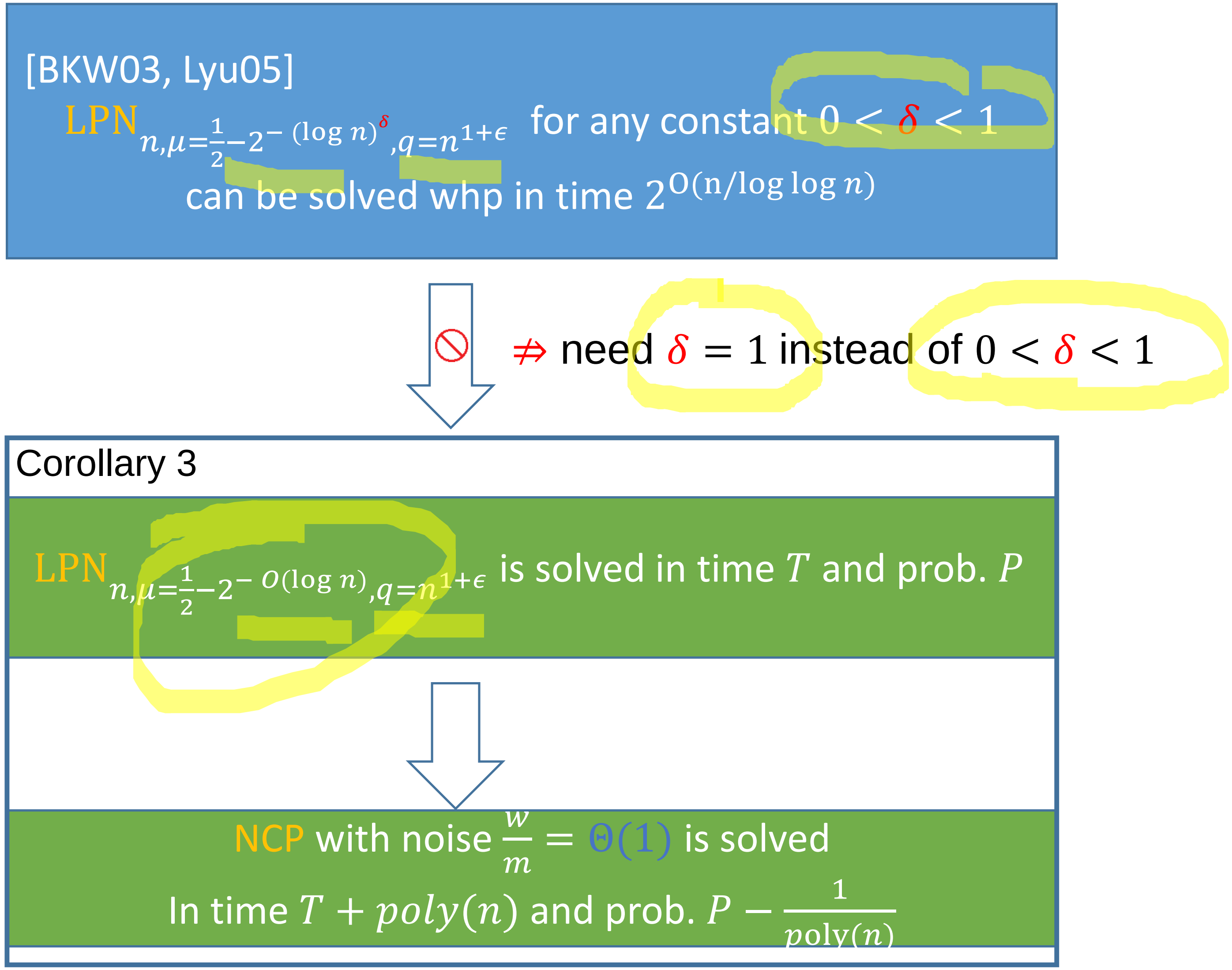
$\left(\overset{T}{2^{\omega(n^{0.5})}}, \overset{\epsilon}{2^{-\omega(n^{0.5})}}, \overset{q}{2^{n^{0.5}}}\right)$ –hard $\mathrm{LPN}_{n,\mu,q}$, $\mu = \Theta(1)$

[YZ16]
[YZW+19]

Collision resistant hashing & public-key encryptions

Applications (Unsuccessful Attempt II)

A sub-exponential algorithm for worst-case constant-noise NCP (based on BKW) ?



[BKW03, Lyu05]

$\mathrm{LPN}_{n,\mu=\frac{1}{2}-2^{-(\log n)^{\delta}},q=n^{1+\epsilon}}$ for any constant $0 < \delta < 1$

can be solved whp in time $2^{O(n/\log\log n)}$

⊘ $\not\Rightarrow$ need $\delta = 1$ instead of $0 < \delta < 1$

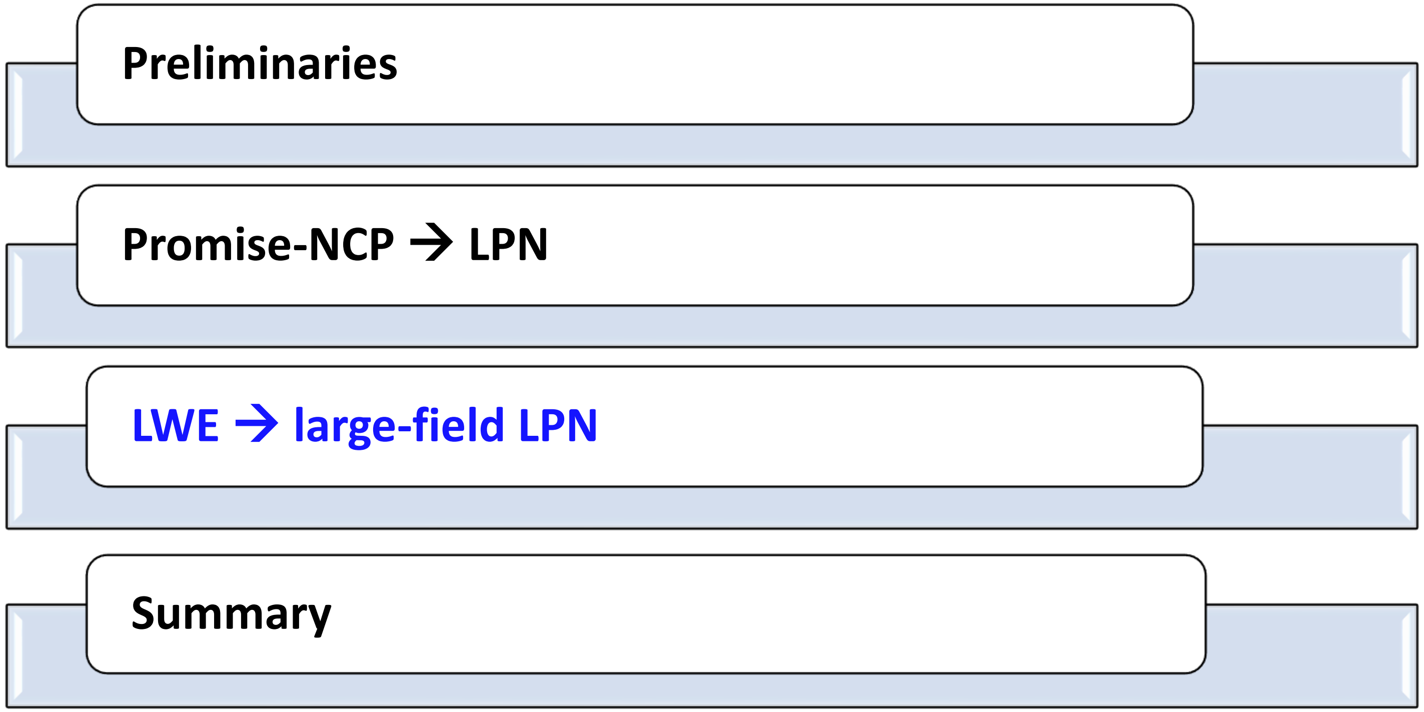
Corollary 3

$\mathrm{LPN}_{n,\mu=\frac{1}{2}-2^{-O(\log n)},q=n^{1+\epsilon}}$ is solved in time T and prob. P

NCP with noise $\frac{w}{m} = \Theta(1)$ is solved

In time $T + poly(n)$ and prob. $P - \frac{1}{\mathrm{poly}(n)}$

Roadmap



- **Preliminaries**
- **Promise-NCP → LPN**
- **LWE → large-field LPN**
- **Summary**

LWE ⇒ LPN over $\mathbb{F}_p$

- **Large-field LPN**

$$a \overset{\$}{\leftarrow} \mathbb{F}_p^n,\ x \overset{\$}{\leftarrow} \mathbb{F}_p^n,\ e \sim \mathrm{Ber}_{r,p} \begin{cases} \blacklozenge\ \text{Prob.}\, r: \quad e \overset{\$}{\leftarrow} \mathbb{F}_p^n \\ \blacklozenge\ \text{Prob.}\, 1-r: e := 0 \end{cases}$$

- **LWE (Learning with Errors)**

$$a \overset{\$}{\leftarrow} \mathbb{F}_p^n,\ x \overset{\$}{\leftarrow} \mathbb{F}_p^n,\ e \sim \mathcal{D}_{\mathbb{Z},\alpha p}$$

Theorem. $\mathrm{LWE}_{n,p,\alpha=\omega(\log n)} \Rightarrow \mathrm{LPN}_{n,p,r=1-\Omega(\frac{1}{\alpha p})}$

Proof.

$$(a, \langle a, s\rangle + e) \xrightarrow{m \overset{\$}{\leftarrow} \mathbb{F}_p \backslash \{0\}} (ma, \langle ma, s\rangle + me)$$

$$\begin{cases} \blacklozenge e \neq 0:\ (ma, me) \overset{\$}{\leftarrow} \mathbb{F}_p^n \times (\mathbb{F}_p \backslash \{0\}) \\ \blacklozenge e = 0: \quad (ma, me) \overset{\$}{\leftarrow} \mathbb{F}_p^n \times \{0\} \end{cases}$$

$me \sim \mathrm{Ber}_{r,p}$ *with* $\Pr[me = 0] = \Omega(\frac{1}{\alpha p})$

Roadmap

Preliminaries

Promise-NCP → LPN

LWE → large-field LPN

Summary

Summary

- Worst-case to average-case reduction for LPN
  - LWE → large-field LPN (noise $\frac{1}{\sqrt{n}}$-close-to-uniform)
  - Promise-NCP (on balanced/independent code) → LPN
    1. Extremely-low-noise promise-NCP → high-noise LPN w. quasi-poly hardness
    2. Low-noise NCP w. almost optimal hardness → constant-noise LPN w. subexp hardness

- Open problems:

1. Promise-NCP (on any (n,m,d)-code) → LPN
2. PKE/CRH from worst-case hardness for decoding binary linear codes
3. More efficient reductions between LWE and LPN

Thanks for your attention

E-mail: yuyuathk@gmail.com