ACISP 2022

Hybrid Dual and Meet-LWE Attack

BI Lei[1,2], LU Xianhui[1,2,3], LUO Junjie[4], WANG Kunpeng[1,2]

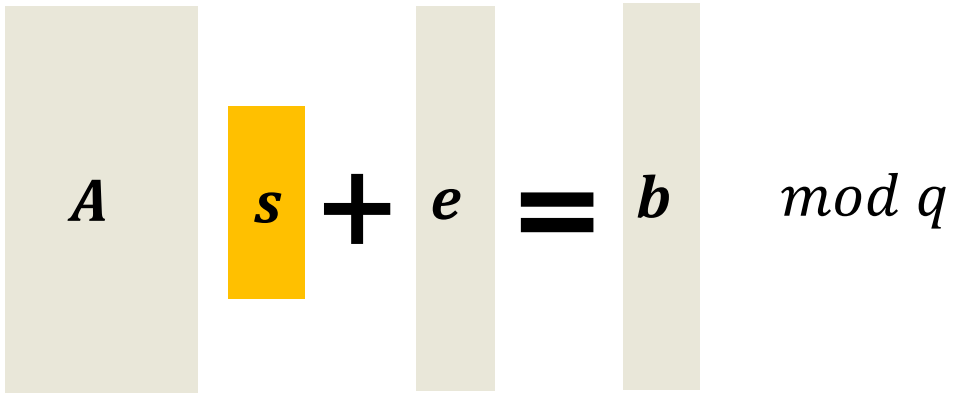
1. Institute of Information Engineering, CAS
2. School of Cyber Security, University of Chinese Academy of Sciences
3. State Key Laboratory of Cryptology
4. Beijing Jiaotong University

Outline

- **Background**
- **Recall hybrid dual attack and Meet-LWE attack**
- **Hybrid dual and Meet-LWE attack**
- **Concrete security estimation of FHE**
- **Conclusion**

Background

- **LWE (Learning with errors) problem** [Regev05]

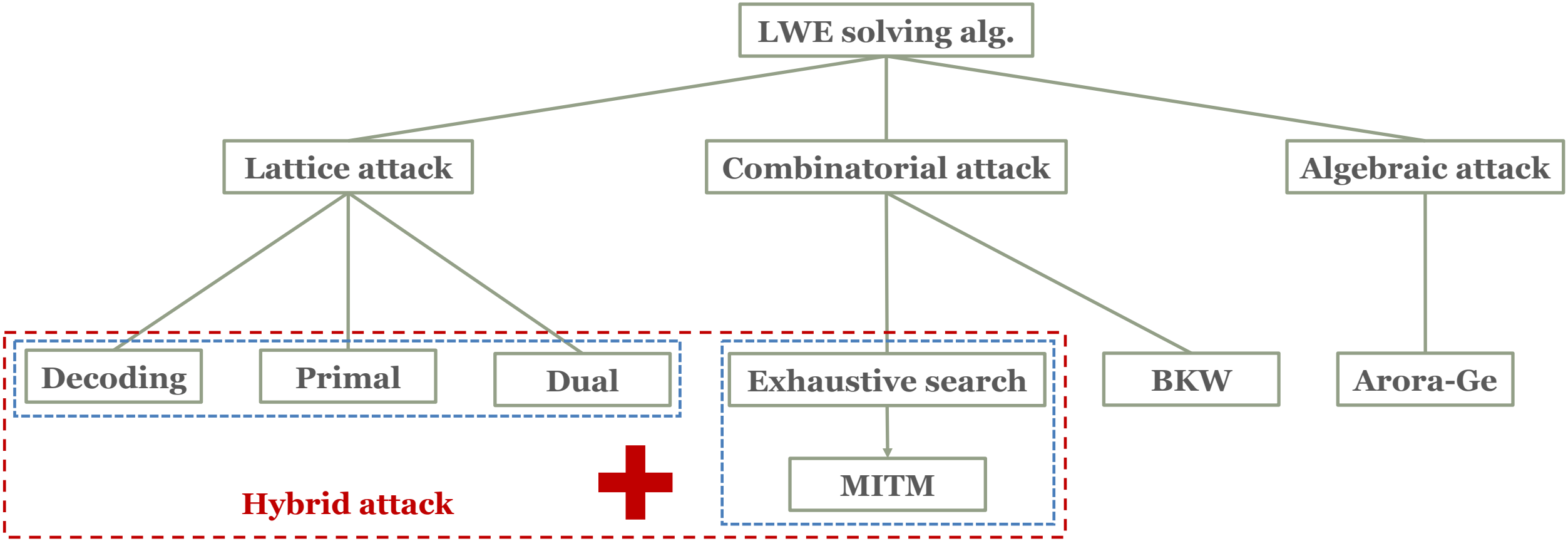


Given (A, b)

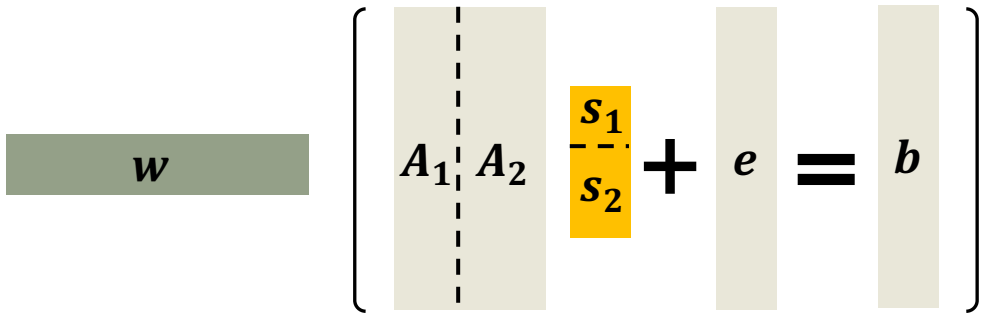
- **Search-version : find** s
- **Decision-version : LWE or Uniform dist. ?**

Background

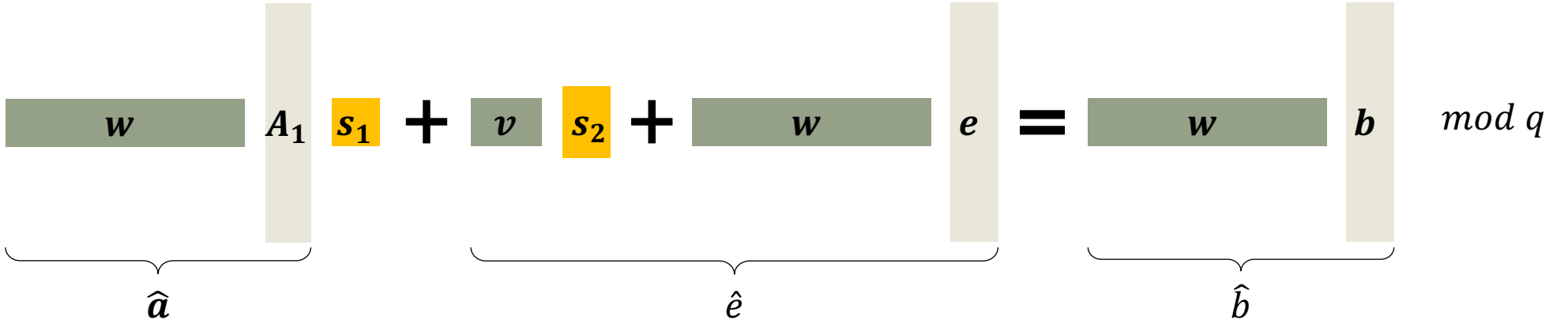
- LWE solving algorithms



Recall Hybrid Dual Attack



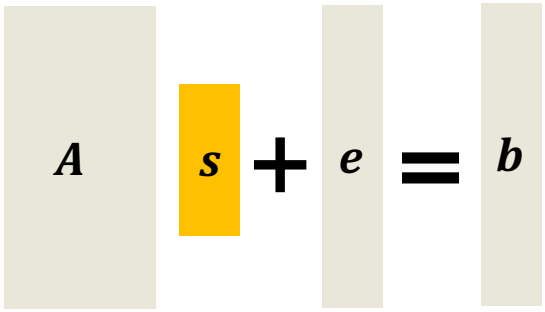
$$(\boldsymbol{w}, \boldsymbol{v}) \leftarrow \Lambda^{\perp}(\boldsymbol{A_2}) = \{(\boldsymbol{w}, \boldsymbol{v}) | \boldsymbol{w}\boldsymbol{A_2} = \boldsymbol{v} \bmod q\}$$

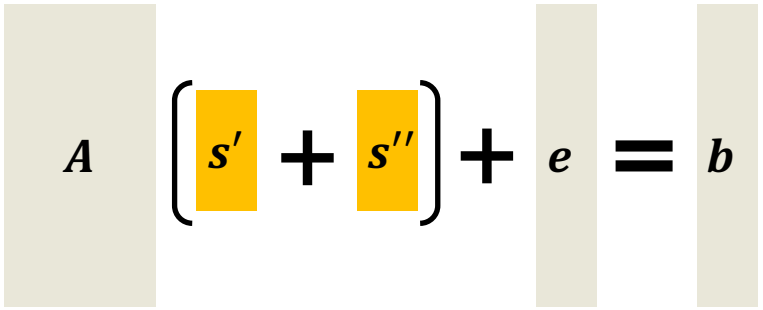


Guess s_1 — **hypothesis test on $\hat{b} - < \hat{a}, s_1 > mod\ q$** → { **modular Gaussian ⇔ Correct** ; **uniform** }

Recall Meet-LWE Attack

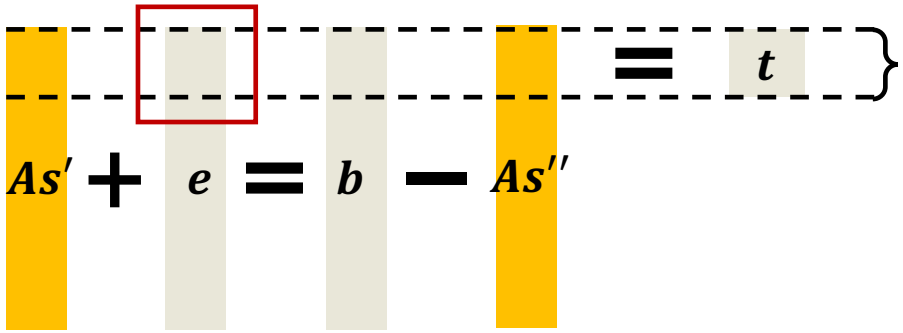
- **Meet-LWE attack on sparse ternary LWE** [May21]





- $\boldsymbol{s} \in \mathcal{T}^{\boldsymbol{n}}(w)$ and $\boldsymbol{s}', \boldsymbol{s}'' \in \mathcal{T}^{\boldsymbol{n}}\left(\frac{w}{2}\right)$
- $\#(\text{representation}) := R = \binom{w}{\frac{w}{2}}$

- $L_1 = \left\{\boldsymbol{s}' \in \mathcal{T}^{\boldsymbol{n}}\left(\frac{w}{2}\right) \middle| \pi_k(\boldsymbol{A}\boldsymbol{s}' + \boldsymbol{e}) = \boldsymbol{t}\right\}$
- $L_2 = \left\{\boldsymbol{s}'' \in \mathcal{T}^{\boldsymbol{n}}\left(\frac{w}{2}\right) \middle| \pi_k(\boldsymbol{b} - \boldsymbol{A}\boldsymbol{s}'') = \boldsymbol{t}\right\}$



$k = \lfloor \log_q R \rceil$

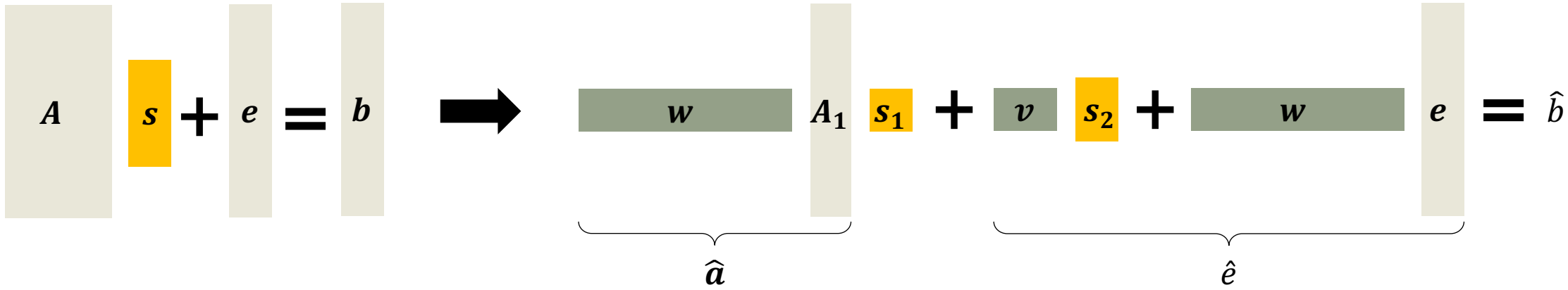
Recall Meet-LWE Attack

- **Meet-LWE attack on sparse ternary LWE** [May21]

- **compute** $k = \lfloor \log_q R \rceil$ **and fix a** $\boldsymbol{t} \xleftarrow{\$} \mathbb{Z}_q^k$
- **For each** $\pi_k(\boldsymbol{e}) \in \mathcal{T}^k$ **do**
  - **construct** $L_1 = \left\{ \left(\boldsymbol{s}' \in \mathcal{T}^{\boldsymbol{n}} \left(\frac{w}{2} \right), h(\boldsymbol{A}\boldsymbol{s}' + \boldsymbol{e}) \right) \middle| \pi_k(\boldsymbol{A}\boldsymbol{s}' + \boldsymbol{e}) = \boldsymbol{t} \right\}$
  - **construct** $L_2 = \left\{ \left(\boldsymbol{s}'' \in \mathcal{T}^{\boldsymbol{n}} \left(\frac{w}{2} \right), h(\boldsymbol{b} - \boldsymbol{A}\boldsymbol{s}'') \right) \middle| \pi_k(\boldsymbol{b} - \boldsymbol{A}\boldsymbol{s}'') = \boldsymbol{t} \right\}$
- **For all matched** $(\boldsymbol{s}', \cdot)$ **and** $(\boldsymbol{s}'', \cdot)$ **in the 2nd component do**
  - **if** $\boldsymbol{s} = \boldsymbol{s}' + \boldsymbol{s}'' \in \mathcal{T}^n(w)$ **and** $\boldsymbol{A}\boldsymbol{s} - \boldsymbol{b} \in \mathcal{T}^k$ **then**
    - **return** $\boldsymbol{s}$

Hybrid Dual and Meet-LWE Attack

- Use Meet-LWE attack to accelerate guessing s_1



- Dual attack makes a **trade-off** between the dim of secret and the norm of error

Technical problems

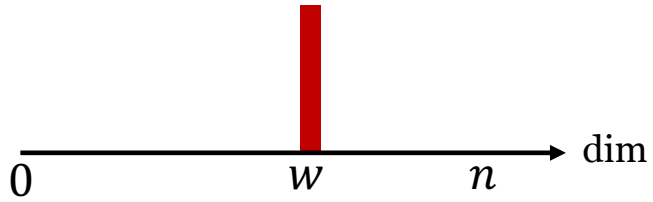
1. **secret** : hamming weight fixed → unknown
2. **error** : ternary → large

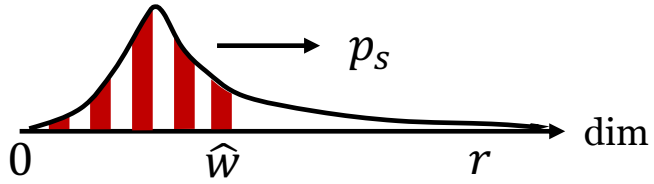
Hybrid Dual and Meet-LWE Attack

- **Problem 1 --- unknown hamming weight of the secret**

$$s = s' + s'' \quad \Rightarrow \quad s_1 = s' + s''$$

$$\mathcal{T}^n(w) \leftarrow \mathcal{T}^n\left(\frac{w}{2}\right) \qquad \sum_{h=0}^{w} \mathcal{T}^r(h) \leftarrow \mathcal{T}^r\left(\frac{\hat{w}}{2}\right)$$

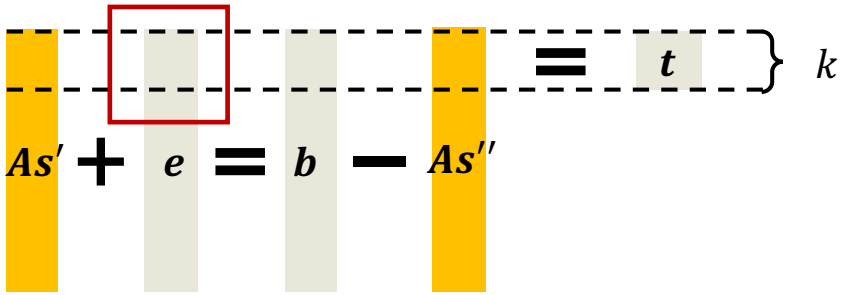


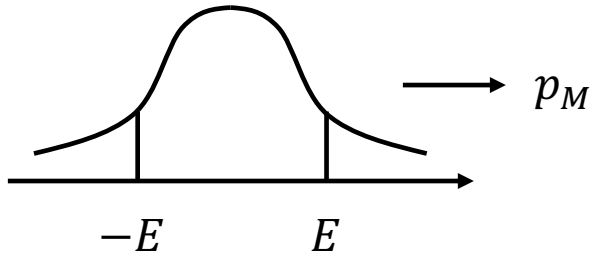


Hybrid Dual and Meet-LWE Attack

- **Problem 2 --- large error**

  - **Enumerate** $\{-E, \dots, E\}$ **instead of** $\{-1,0,1\}$





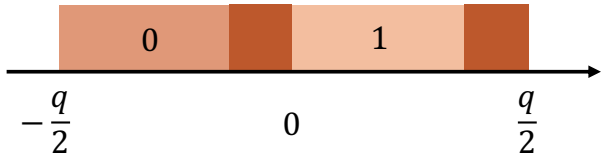
Hybrid Dual and Meet-LWE Attack

- **Problem 2 --- large error**

$$\hat{e} = \boldsymbol{v}\ \boldsymbol{s_2} + \boldsymbol{w}\ \boldsymbol{e} \sim \mathcal{G}_\rho \gg e$$

- **Define a new hash function**

$$h(\boldsymbol{x_i}) = \begin{cases} 0, \boldsymbol{x_i} \in \left[-\frac{q}{2}, -E\right) \\ 1, \boldsymbol{x_i} \in \left[0, \frac{q}{2} - E\right) \\ 0{,}1, \boldsymbol{x_i} = [-E, 0) \cup \left[\frac{q}{2} - E, \frac{q}{2}\right) \end{cases}$$



$$\#(\text{addresses for each element}) = 2^{\frac{2E+1}{q} \cdot M}$$

Concrete Security Estimation of FHE

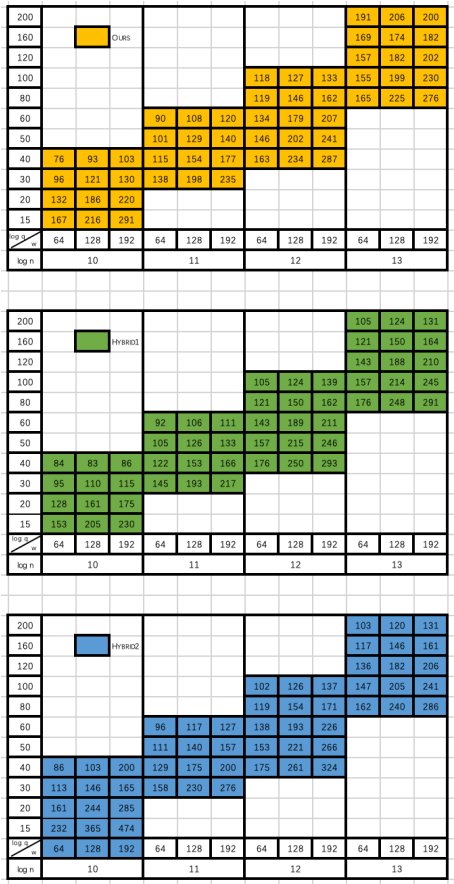
- **Improvements up to 16 bits**

200										103	120	131
160										117	146	161
120										136	182	202
100							102	124	133	147	199	230
80							119	146	162	162	225	276
60				90	106	111	134	179	207			
50				101	126	133	146	202	241			
40	76	83	86	115	153	166	163	234	287			
30	95	110	115	138	193	217						
20	128	161	175									
15	153	205	230									
log q / w	64	128	192	64	128	192	64	128	192	64	128	192
log n	10			11			12			13		

OURS

HYBRID1

HYBRID2



- HYBRID1 [BLLWZ22] Hybrid dual attack on LWE with arbitrary secrets. Cybersecurity 2022.
- HYBRID2 [CHHS19] A hybrid of dual and meet-in-the-middle attack on sparse and ternary secret LWE. IEEE Access 2019.

Conclusion

- **Summary**
  - **Use Meet-LWE to accelerate guessing in hybrid dual attack**
  - **Improve the estimation of the concrete security of FHE up to 16 bits**

- **Future work**
  - **Remove enumerating $\hat{e}$**
  - **Replace the hash function**

Thanks!