

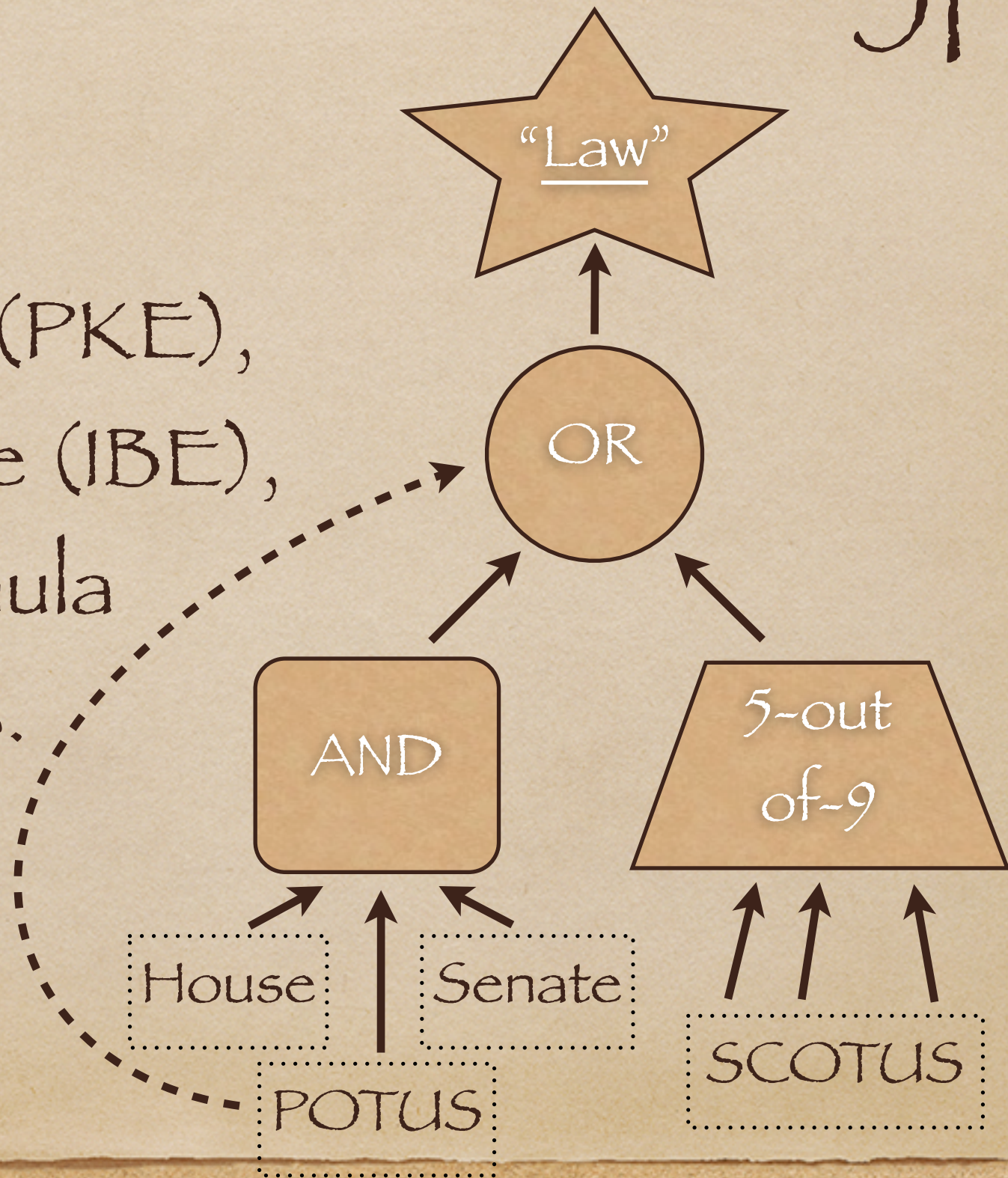
Attribute-Based
Encryption
from Lattices

Xavier Boyen

CRYPTO rump session - 2012/08/21

Attribute-based encryption

- ◆ Encrypt...
 - not to a key (PKE),
 - not to a name (IBE),
 - but to a formula on attributes.



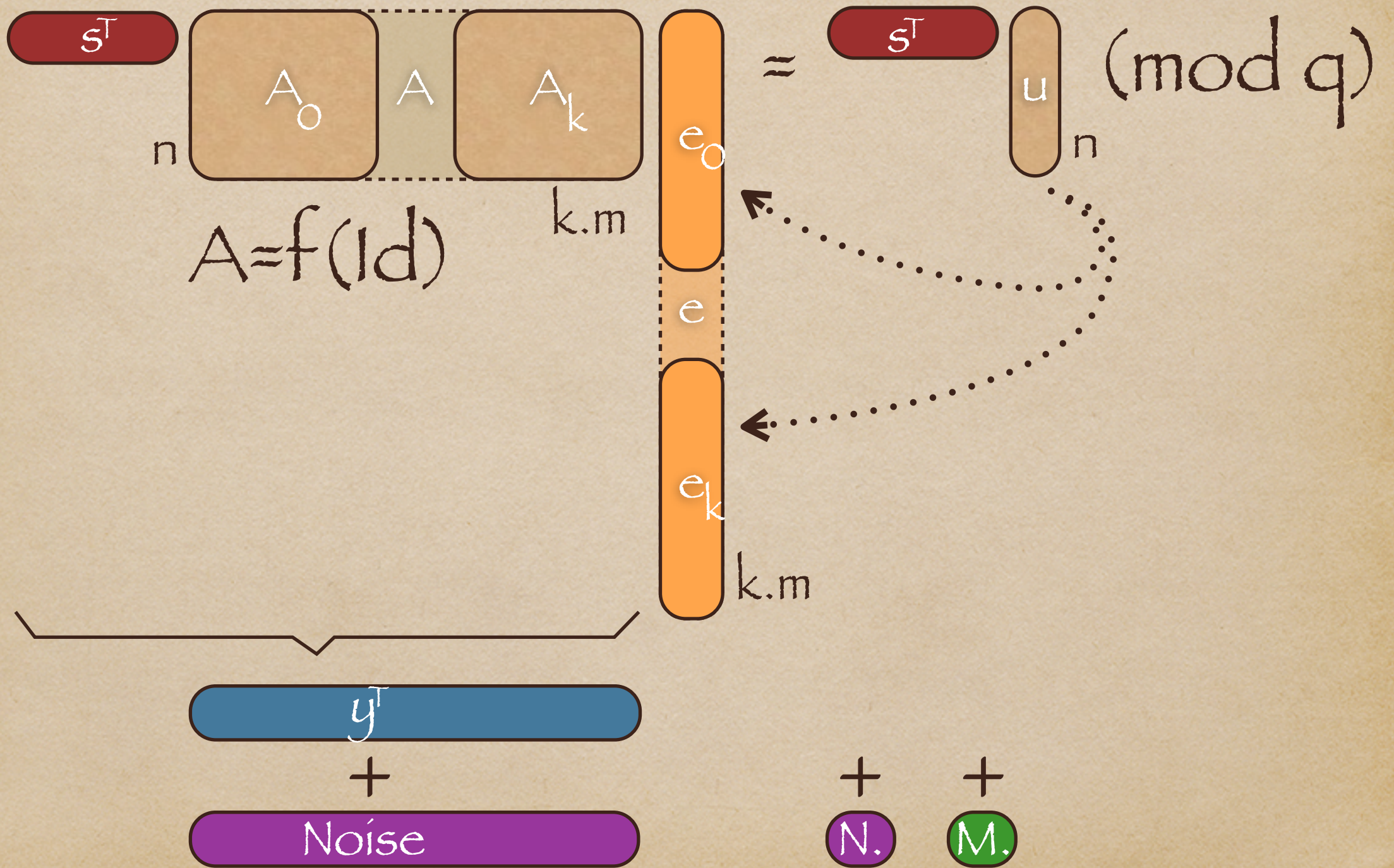
Regev's lattice PKE

$$\underbrace{\begin{matrix} \text{red box } s^T \text{ (size } n) \\ \text{brown box } A \text{ (size } n \times m) \\ \text{orange box } e \text{ (size } m) \end{matrix}}_{\text{encapsulation}} = \begin{matrix} \text{red box } s^T \text{ (size } n) \\ \text{brown box } u \text{ (size } n) \end{matrix} \pmod{q}$$

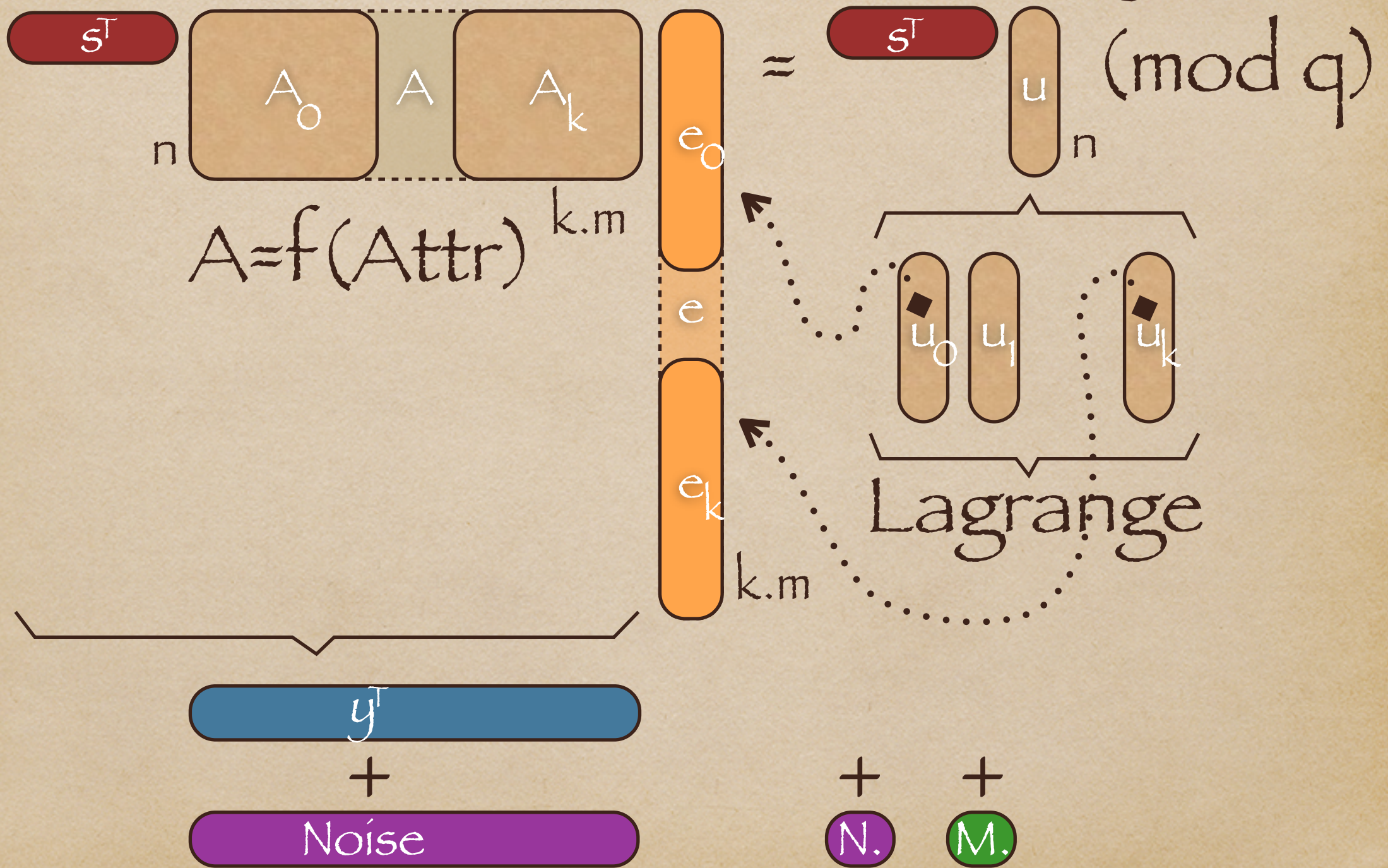
$$\underbrace{\begin{matrix} \text{blue box } y^T \text{ (size } m) \\ \text{purple box } \text{Noise} \text{ (size } m) \end{matrix}}_{\text{decapsulation}} + \begin{matrix} \text{purple box } N. \\ \text{green box } M. \end{matrix}$$

- ◆ PK: random (A, u) SK: small $e : A \cdot e = u \pmod{q}$
- ◆ Encrypt: pick s , output: $y = s^T A + \text{noise}$
 $x = M \cdot [q/2] + s^T A + \text{noise}$
- ◆ Decrypt: $x - y^T e = 0 + M \cdot [q/2] + \text{epsilon}$

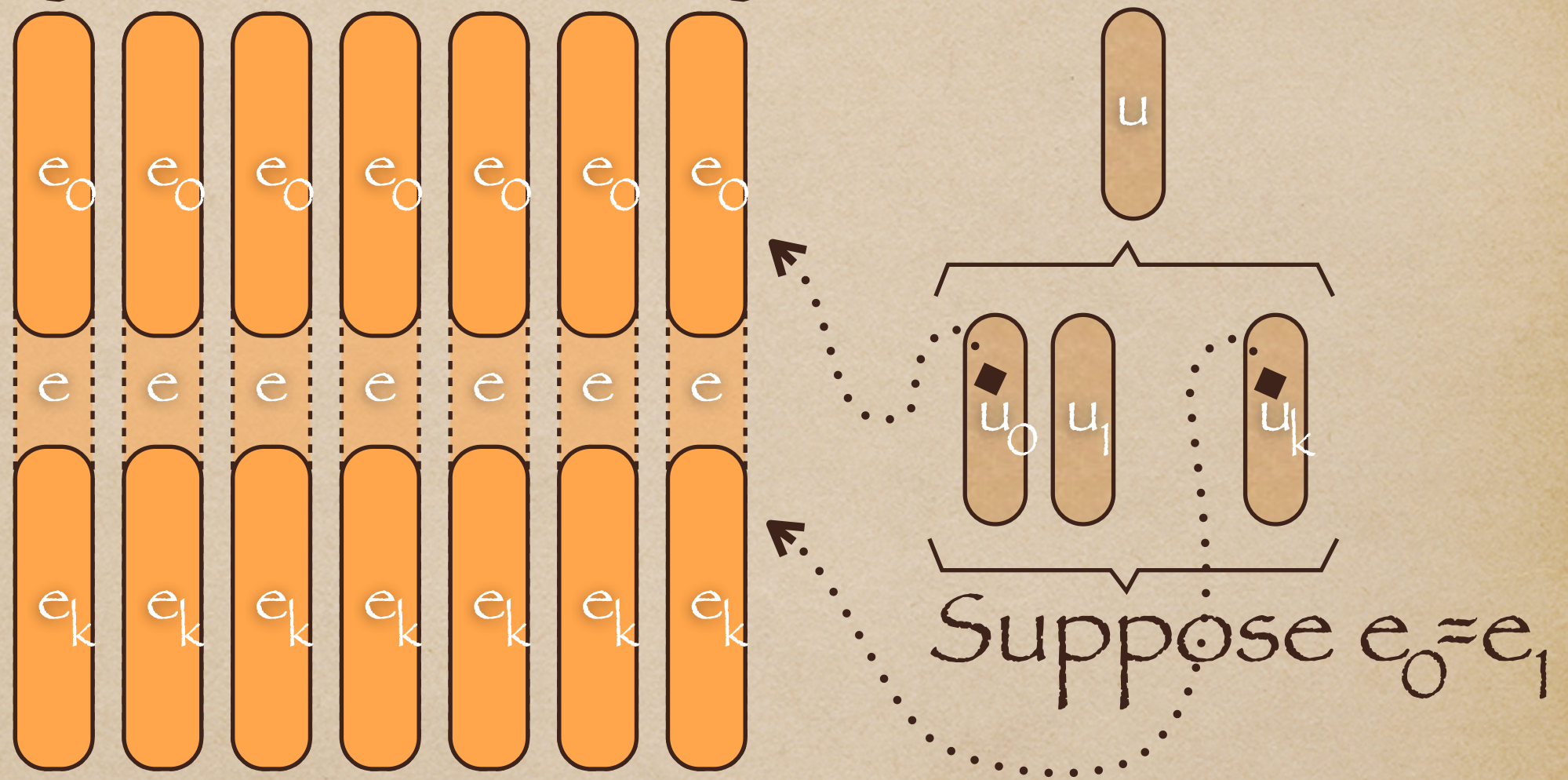
AB&CHKP's lattice IBE



ABVW's lattice FuzzyIBE



Beyond Fuzzy? Danger!



Not independent;
there be Rogue Basis!

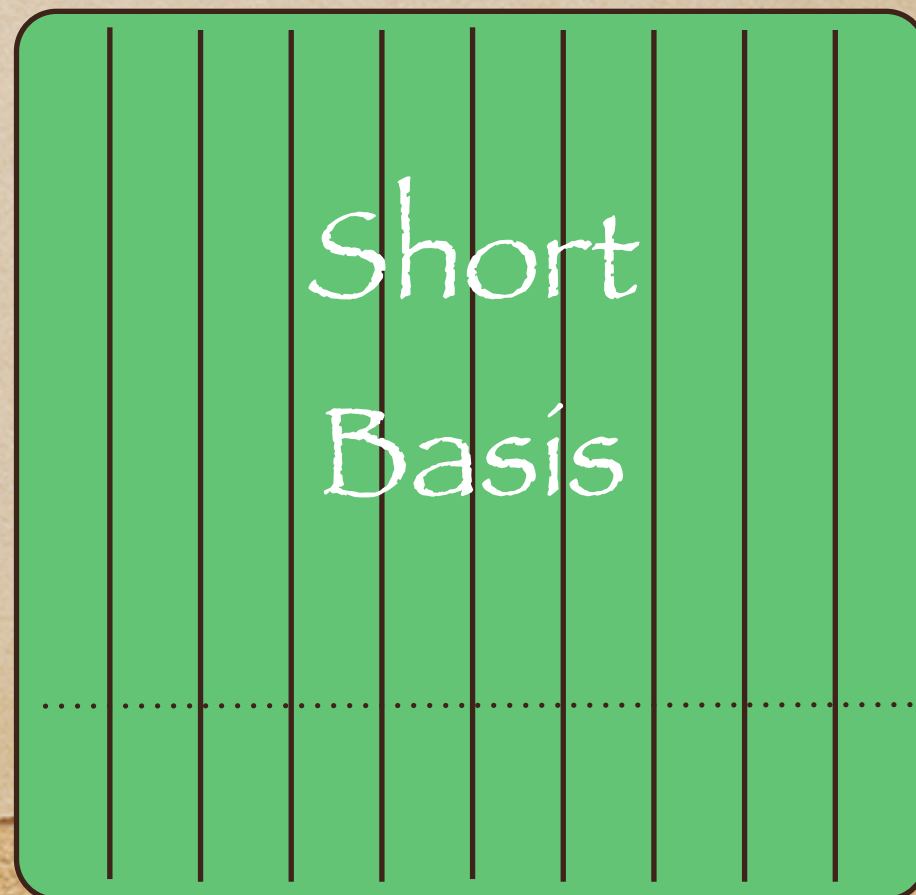
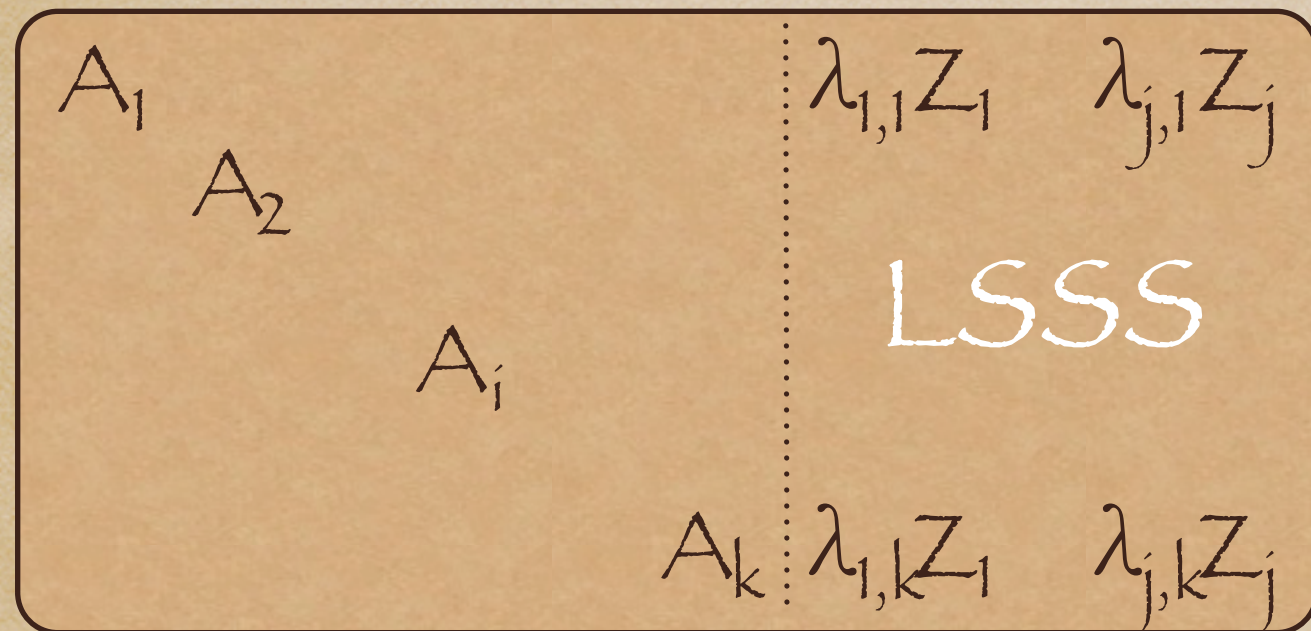
Idea: Split ~~vectors~~ bases

$$\begin{matrix} \text{---} s^T \end{matrix} \begin{matrix} \text{---} A \end{matrix} \begin{matrix} \text{---} e \end{matrix} = \begin{matrix} \text{---} s^T \end{matrix} \begin{matrix} \text{---} u \end{matrix}$$

Public



Private key



Conclusion

- ◆ /Basis Splitting \
\
Basis Sharing /
 - ◆ KP-ABE
 - ◆ CP-ABE
 - ◆ Easy to simulate!
 - ◆ (seemingly)
VERY powerful indeed...

