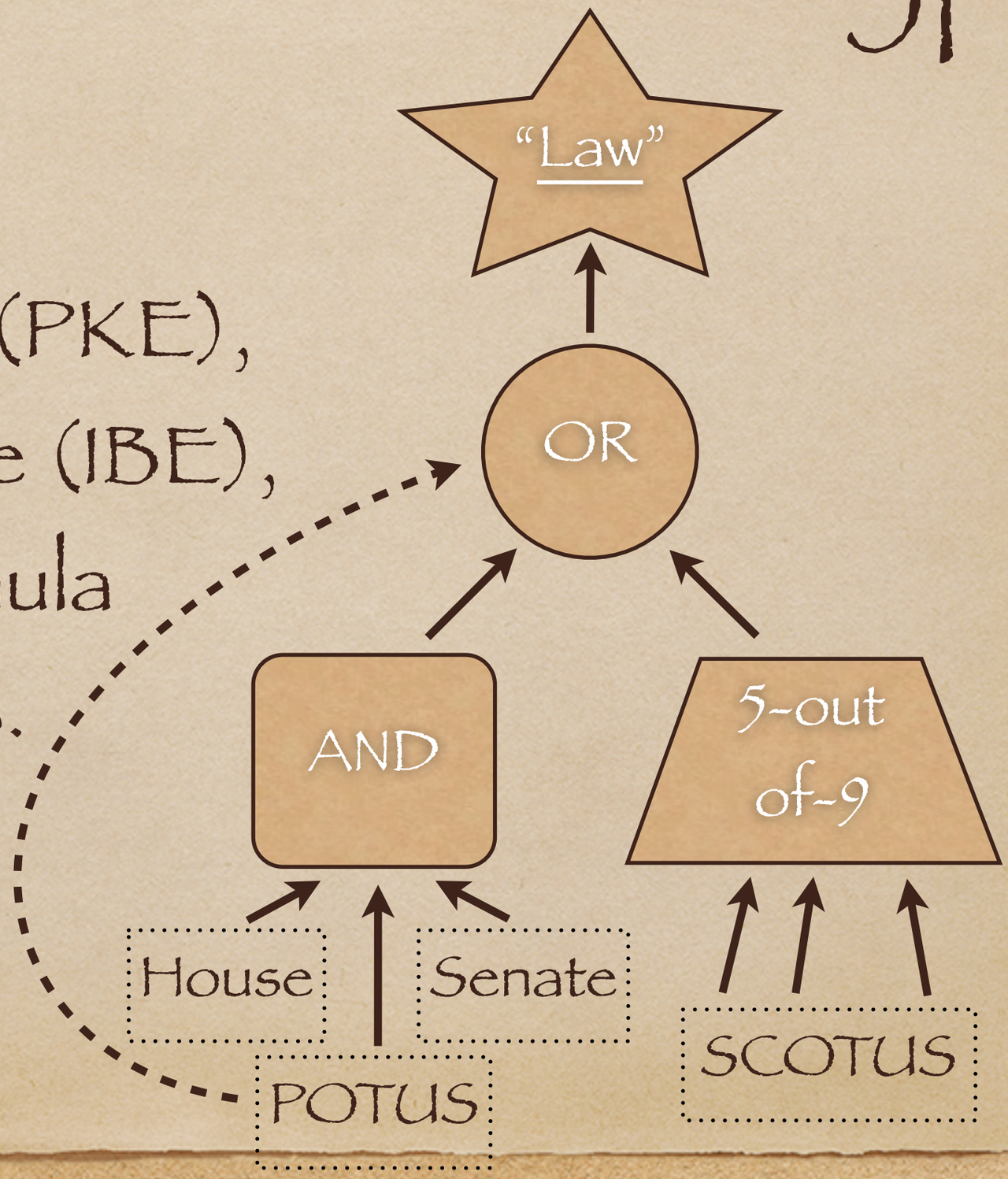
Attribute-Based Encryption from Lattices

Xavier Boyen

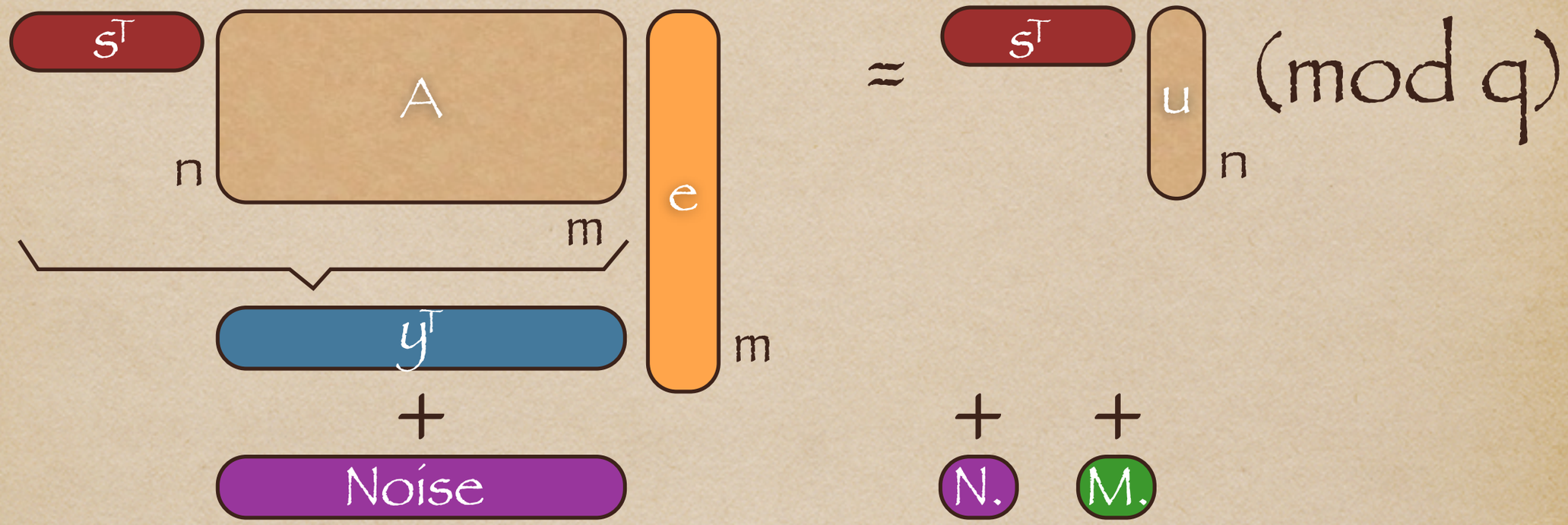
CRYPTO rump session - 2012/08/21

Attribute-based encryption

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

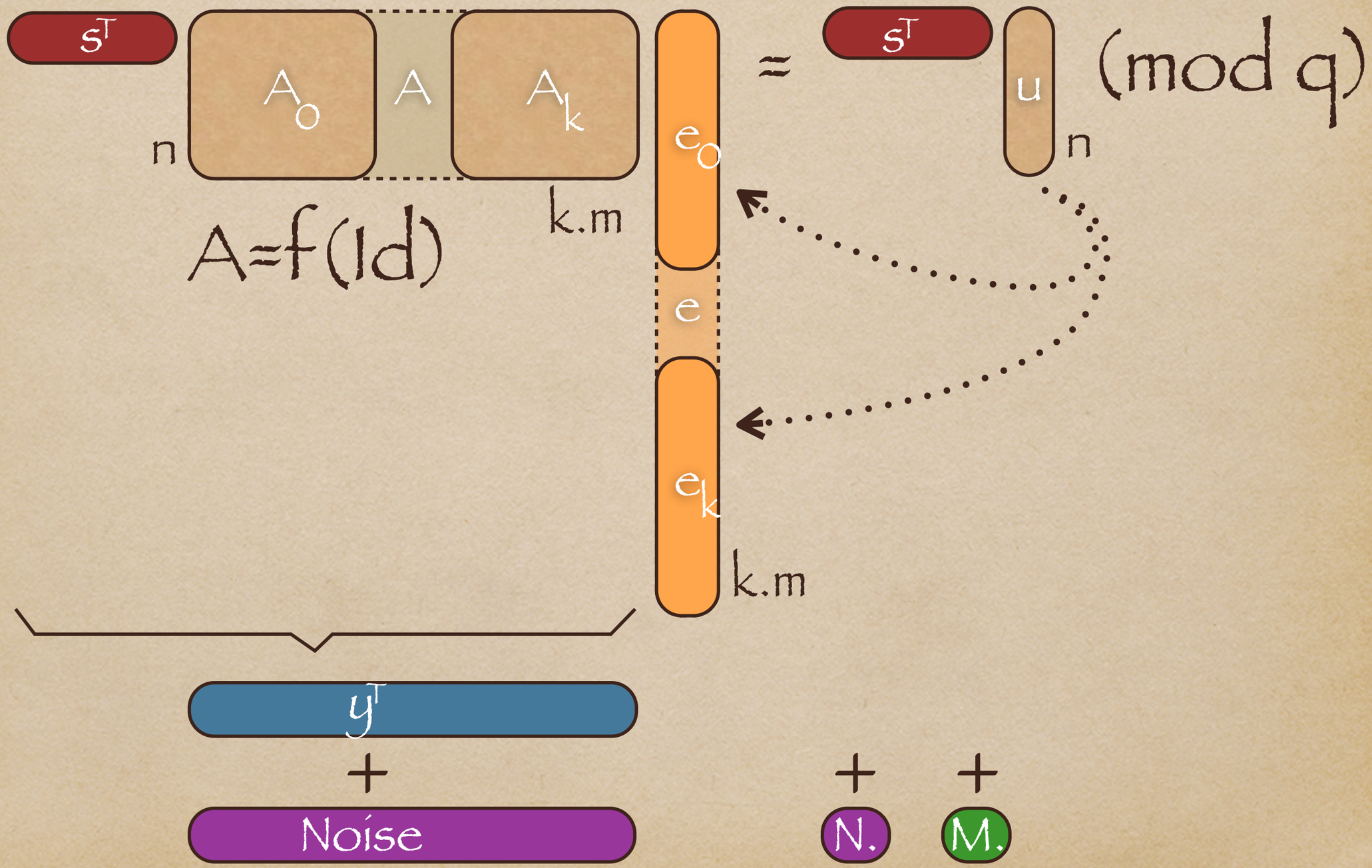


Regev's lattice PKE

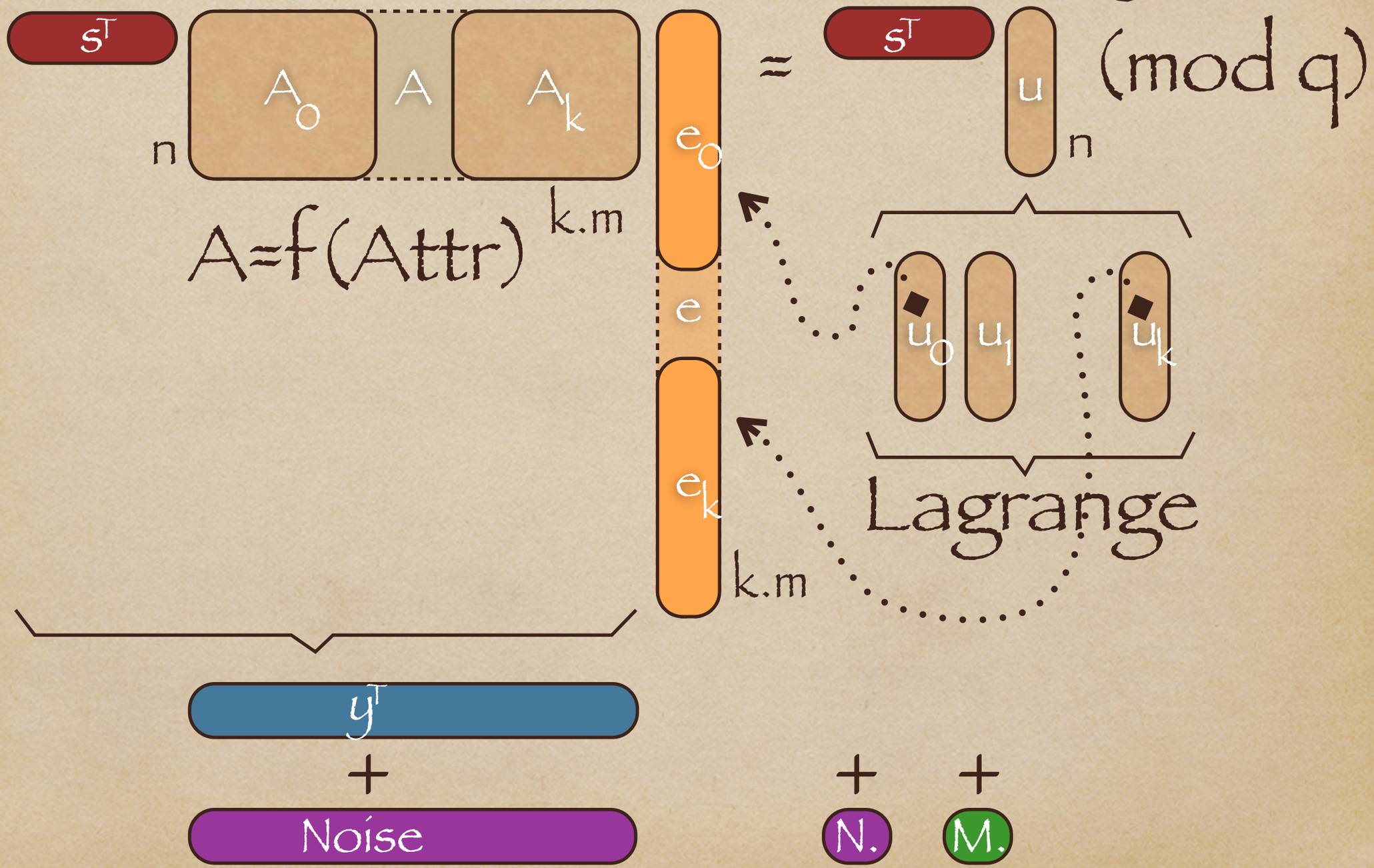


- PK: random (A, u) SK: small e : A.e ≈ u (q)
- Encrypt: pick s, output : $y = s^T A$ + noise
  $x = M.[q/2] + s^T A$ + noise
- Decrypt: $x - y^T e = 0 + M.[q/2]$ + epsilon

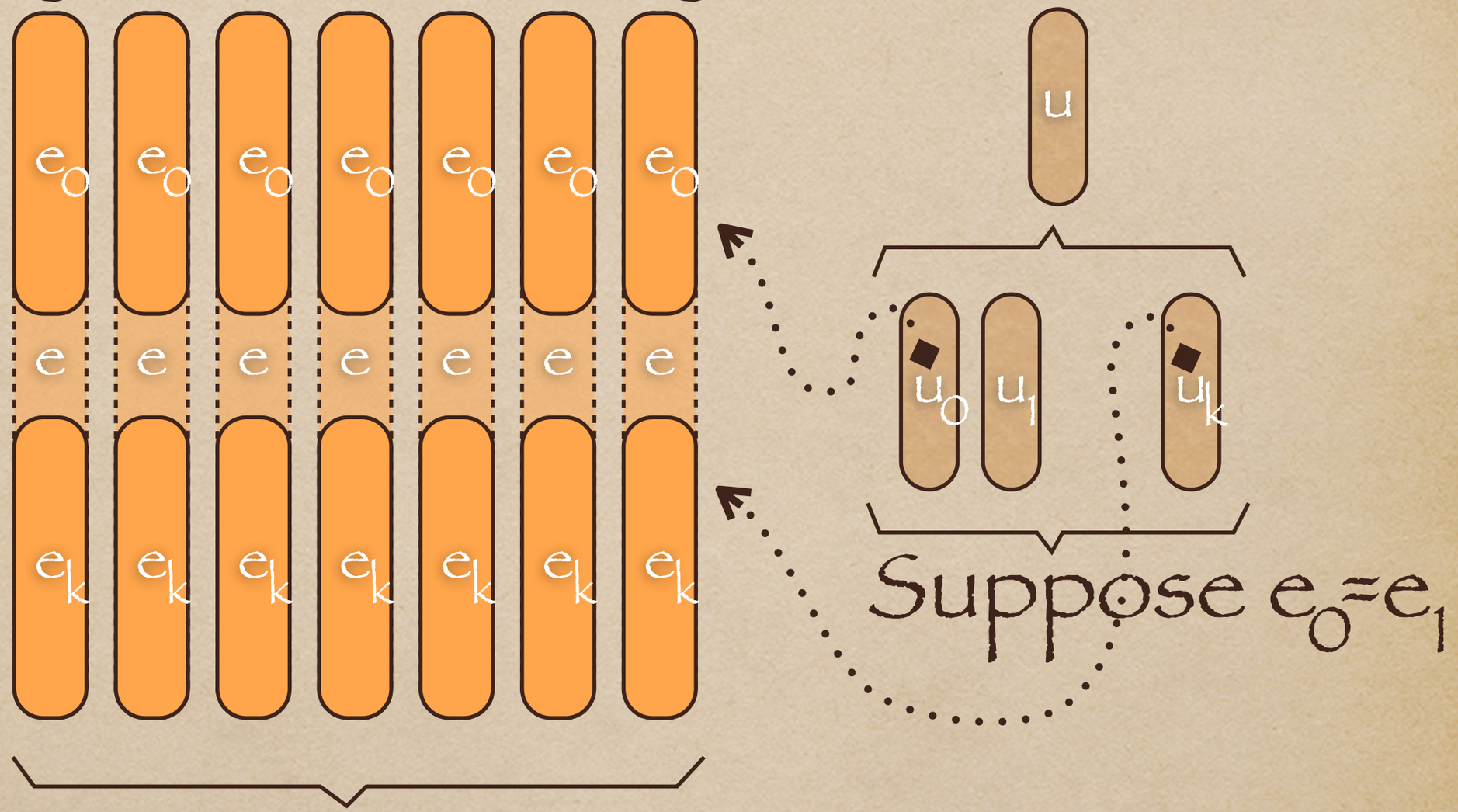
AB&CHKP's lattice IBE



ABVVW's lattice FuzzyIBE



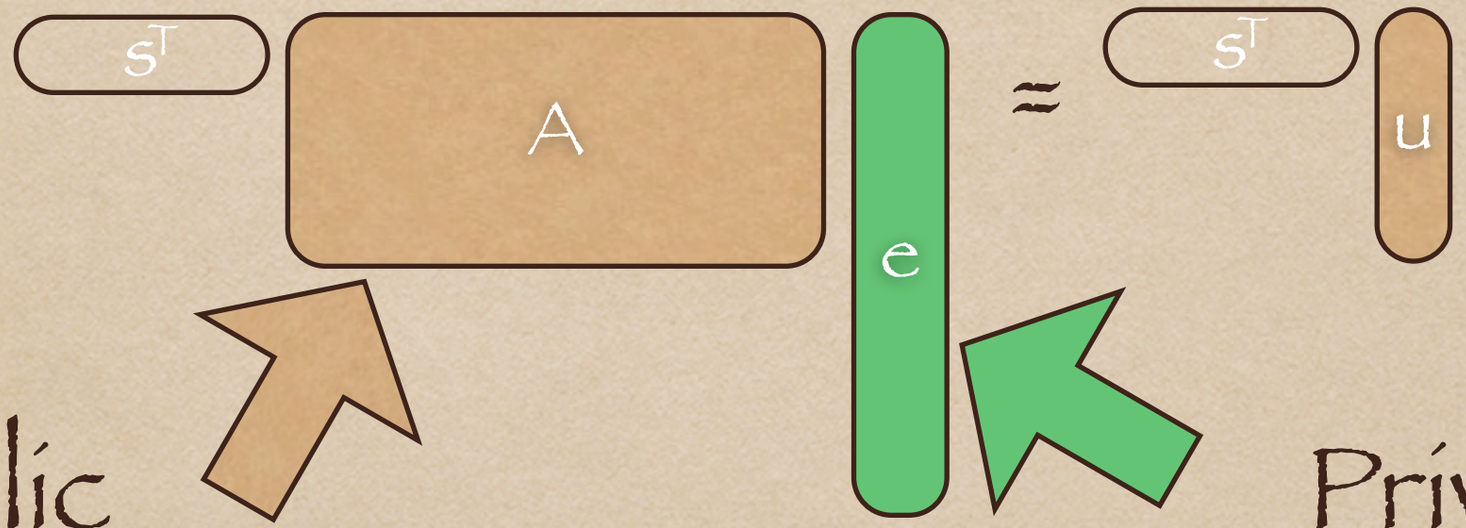
Beyond Fuzzy? Danger!



Not independent;

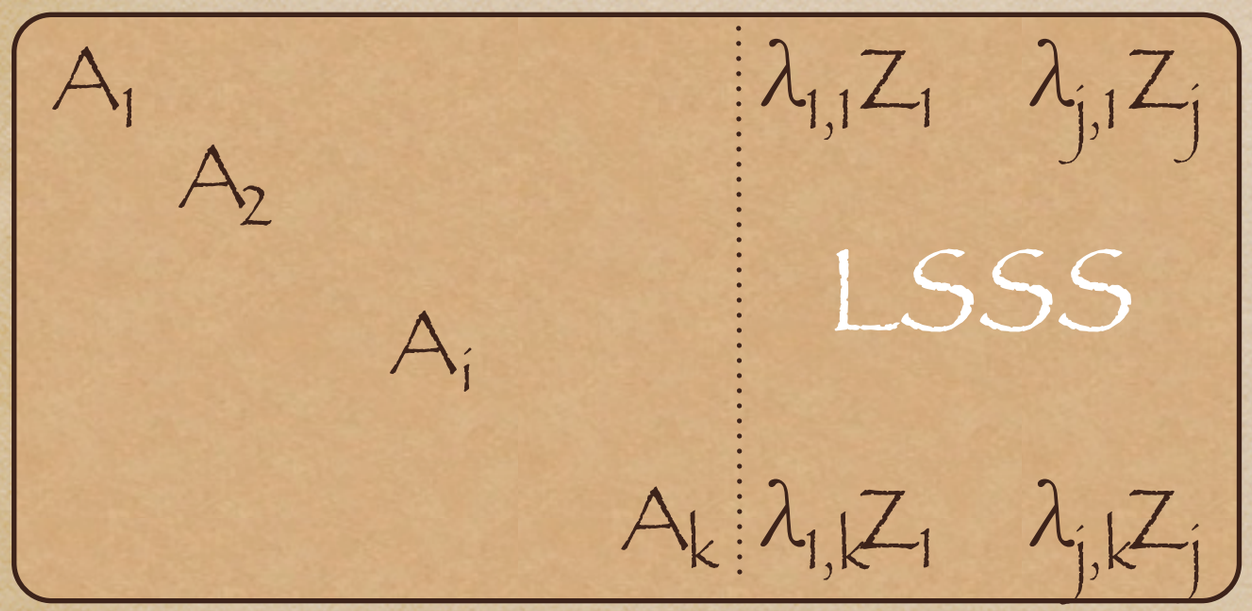
there be Rogue Basis!

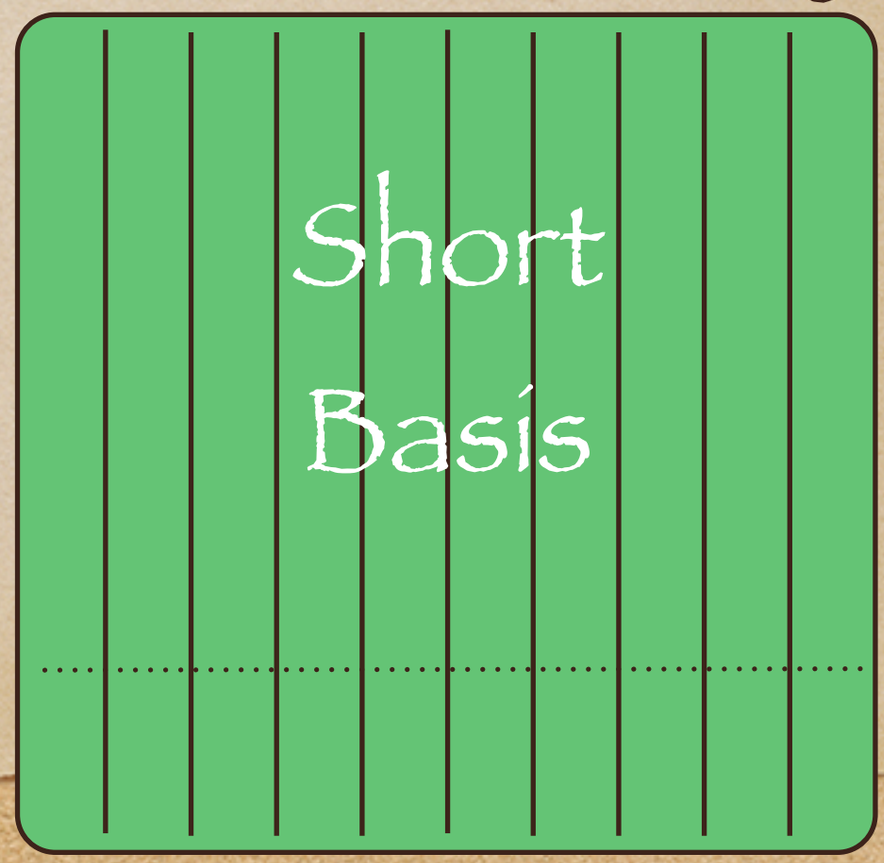
Idea: Split ~~vectors~~ bases



Public

Private key





Conclusion

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