Trapdoor Computational Fuzzy Extractors

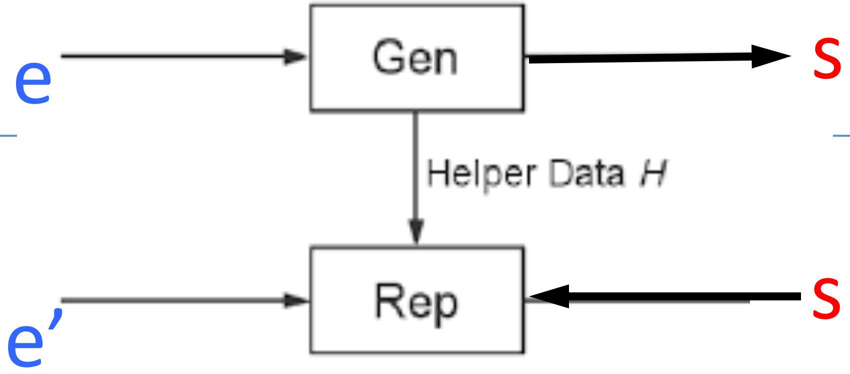
Challenge:

- Use manufacturing variation in silicon to generate stable secret keys

Solution:

- Use a fuzzy commitment scheme
- Use “confidence” information from silicon biometric source to correct errors

CNS 1523572
MIT



Scientific Impact:

- Improve the physical security of integrated circuits
- Theory deepens understanding of computational fuzzy extractors – prior extractors are information theoretic

Broader Impact:

- This research can enable the development of physically- and computationally-secure processors
- PRIMES high-school research outreach program