Cryptographic S-Boxes

- S-Box designs are motivated by
  - Differential uniformity (differential cryptanalysis)
  - Nonlinearity (linear cryptanalysis)
  - Algebraic immunity (algebraic attacks)
  - Resiliency
- Studied and analyzed in the context of Boolean functions, but designed using the mathematics of Galois fields
  - They must be efficiently computable!
  - Enables further optimizations in hardware (e.g. through the application of composite fields to reduce combinational logic)

Scaling Up the Size

- Preparing for future needs of larger S-Boxes
- We must revisit Nyberg's design choices for differentially uniform S-Boxes
  - Including inverse mappings and exponent mapping in prime fields
- How do these designs compare over elements in GF(2^16)?
  - Gather hardware metrics from implementations
  - Measure cryptographic strength derived from Boolean function representations
- » How do these designs compare to randomly generated S-Boxes?
  - Can we achieve better security properties at the cost of implementation efficiency?