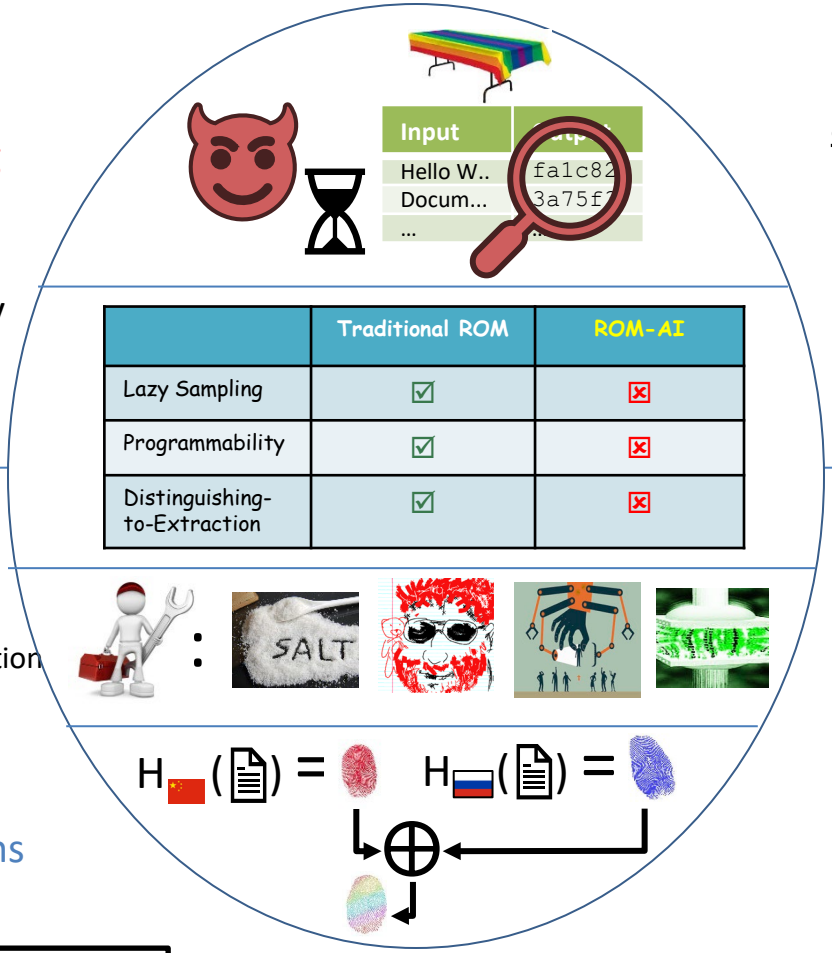
On the Power of Preprocessing and Non-Uniformity

Challenge:

- Withstand preprocessing attacks which are known to significantly speed-up on-line attack complexity



Solution:

- Auxiliary-Input models:
  - Random oracle/permutation
  - Ideal Cipher
  - Generic Group Model
- Salting
- Standard -> AI reductions

Scientific Impact:

- *Techniques*: compression, multi-instance security, presampling
- Salting provably works
- Immunizing Backdoors !!

Broader Impact and Broader Participation:

- Impact on technology
- Withstand powerful (state-run?) adversaries
- Significant mentoring & training opportunities

SaTC #1815546 (New York University)