New Attacks on SHA-3

Adi Shamir
The Weizmann Institute
Israel

Joint work with Itai Dinur and Orr Dunkelman

Rump session of Asiacrypt 2012

SHA-3 = Keccak

- On October 2-nd, NIST announced their choice of Keccak as SHA-3
- Keccak is currently the hottest target for cryptanalysis!
- Lots of interesting observations, but very few published attacks

The Four Flavors of Keccak

- Keccak-224
- Keccak-256
- Keccak-384
- Keccak-512

Collision Attacks on Keccak: > 1 year ago

- Keccak-224 - none
- Keccak-256 - none
- Keccak-384 - none
- Keccak-512 - none

Collision Attacks on Keccak: Indocrypt 2011

Maria Naya-Plasencia, Andrea Rock, and Willi Meier

- Keccak-224 – 2 rounds
- Keccak-256 – 2 rounds
- Keccak-384 - none
- Keccak-512 - none

Collision Attacks on Keccak: FSE 2012

Itai Dinur, Orr Dunkelman and Adi Shamir

- Keccak-224 – 4 rounds
- Keccak-256 – 4 rounds
- Keccak-384 - none
- Keccak-512 - none

Collision Attacks on Keccak: New results

Itai Dinur, Orr Dunkelman and Adi Shamir

- Keccak-224 – 4 rounds
- Keccak-256 – 5 rounds
- Keccak-384 – 4 rounds
- Keccak-512 – 3 rounds

Our New Cryptanalytic Technique: Self-Differential Cryptanalysis

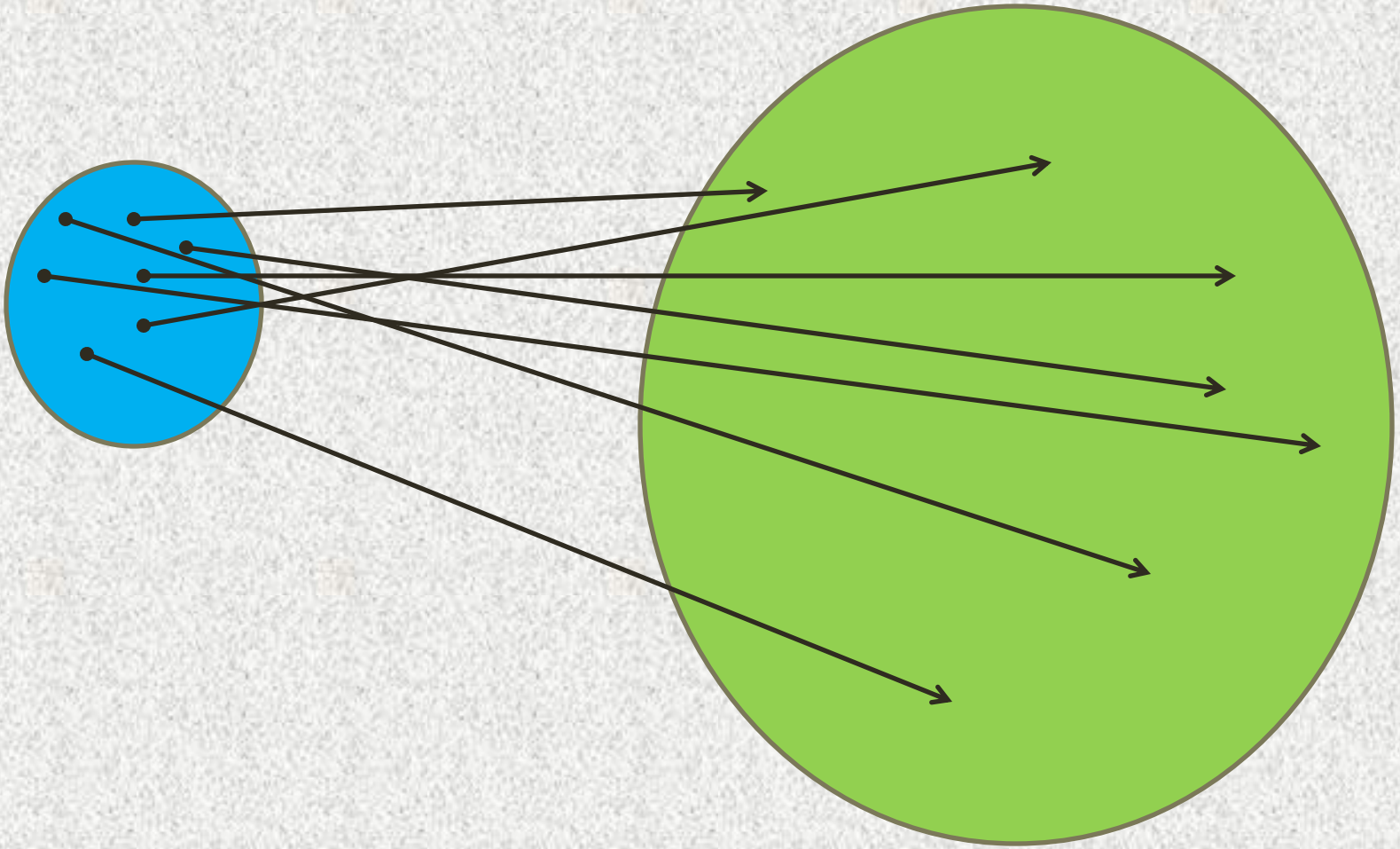
- In standard differential attacks, we consider pairs of plaintexts, and follow the evolution of their differences

- In self –differential attacks, we consider a single plaintext, and follow the evolution of differences between various parts of the single state during the first few rounds

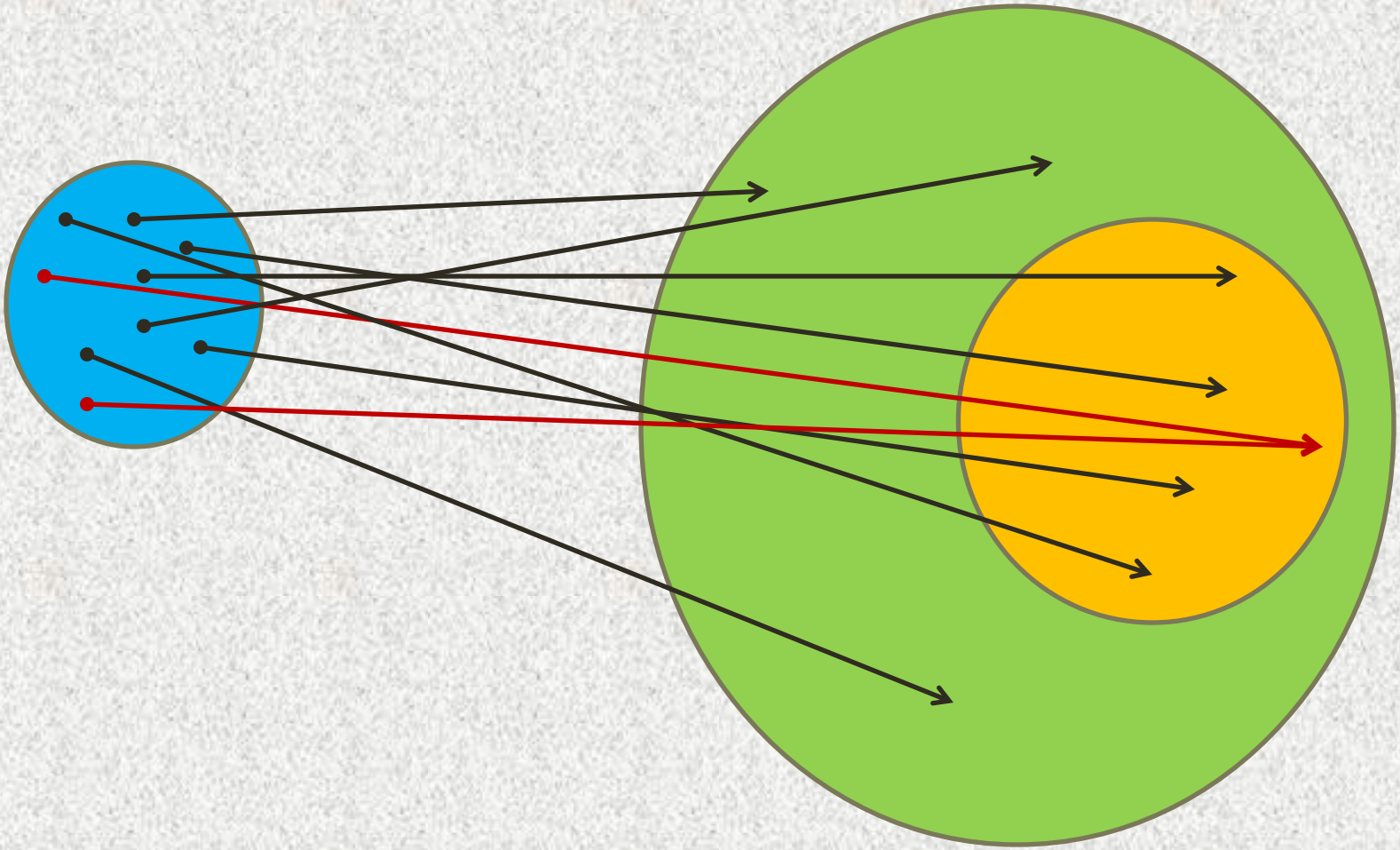
Our New Cryptanalytic Technique: Self-Differential Cryptanalysis

- We use the fact that most of the operations in SHA-3 preserve some state symmetries
- The designers were aware of this problem
- They tried to avoid it by adding asymmetric constants at each round of SHA-3
- However, these constants have very low HW
- We follow the evolution of such asymmetries
- We use a Squeeze attack to map many inputs into the small set of almost symmetric outputs

Squeeze Attack



Squeeze Attack



Final Comments about SHA-3:

- These are the first published collision attacks on reduced round Keccak-384 and Keccak-512
- We improve the best published attack on Keccak-256
- However, full Keccak has 24 rounds
- So we are still very far from breaking SHA-3…
- More details: see our new ePrint paper