Analysis of SHA-512/224 & SHA-512/256

Christoph Dobraunig **Maria Eichlseder** **Florian Mendel**

FSE 2015

SHA-512/224 and SHA-512/256

- Newest members of NIST's SHA-2-family (2012)
- Compute SHA-512 and truncate
- Pros
  - Faster than SHA-224 and SHA-256 on many platforms
  - Wide-pipe construction – more secure?
- Cons
  - Not (yet) widely used
  - No public cryptanalysis

Our results on SHA-512/224 and SHA-512/256

- Collisions: 27/80 steps
  - based on new SHA-512 27-step collision
  - SHA-224, SHA-256: 28/64
- Semi-free-start collisions: 39/80 steps
  - based on new SHA-512 39-step characteristic
  - SHA-224, SHA-256: 38/64
- Free-start collisions: 44/80 (SHA-512/224), 43/80 steps (SHA-512/256)
  - benefit from truncation to get free extra steps
  - SHA-224, SHA-256: 39/64 and 38/64

Also the best practical collision results for SHA-512!