SHA-3 candidate: Grøstl

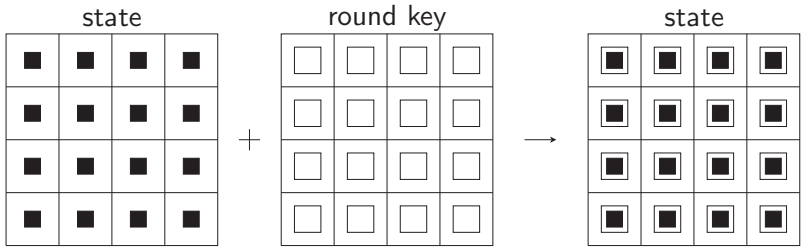
Joint work of Mendel, Rechberger, Schläffer from IAIK, Austria
Knudsen, Thomsen, Matusiewicz, Gauravaram from DTU
Denmark

Slides by S.S. Thomsen and LRK

AES/Rijndael

- 128-bit block cipher
- 4×4 matrix of bytes
- AddRoundKey, SubBytes, ShiftRows, MixColumns
- 10 rounds

AddRoundKey

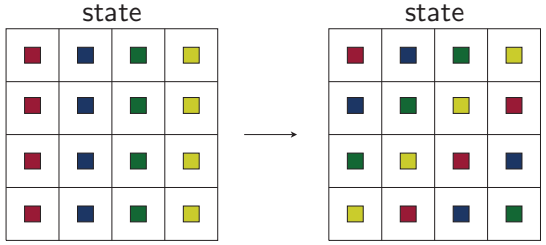


SubBytes

- Operates on each byte individually
- Non-linear
- 8-bit S-box based on inversion in $\mathbb{F}_{256}$
- Very good differential properties
- Algebraic structure

ShiftRows

- Operates on each row individually
- Moves bytes across columns



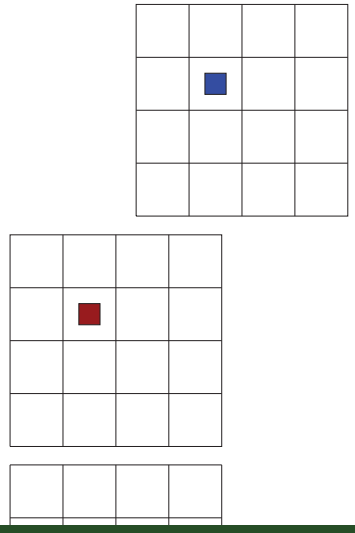
MixColumns

- Operates on each column individually
- Spreads bytes across rows
- Based on "MDS" code (Maximum Distance Separable)
- Input diff. on $d > 0$ bytes $\Longrightarrow$ output diff. on at least $5 - d$ bytes (optimal)

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} \text{state} \end{pmatrix} \rightarrow \begin{pmatrix} \text{state} \end{pmatrix}$$

(in $\mathbb{F}_{256}$)

Diffusion



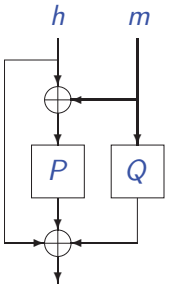
The Grøstl construction

- P an n-bit permutation
- SMASH: $h_i = P(h_{i-1} \oplus m_i) \oplus \theta m_i \oplus h_{i-1}$
- SMASH broken...
- Idea, replace multiplication by θ with something stronger
- $h_i = P(h_{i-1} \oplus m_i) \oplus Q(m_i) \oplus h_{i-1}$ for Q an n-bit permutation
- Two variants, Grøstl-256 and Grøstl-512, focus on the former

The Grøstl256 construction

$$f(h_{i-1}, m_i) = h_i = P(h_{i-1} \oplus m_i) \oplus Q(m_i) \oplus h_{i-1}$$

(P, Q 512-bit permutations)



Security proof

- P and Q ideal 512-bit permutations
- compress:
  - $P(h \oplus m) \oplus Q(m) \oplus h$
  - $P(h \oplus m) \oplus h \oplus m \quad \oplus \quad Q(m) \oplus m$
  - $f(x) \quad \oplus \quad g(y)$, where $x = h \oplus m$ and $y = m$
- $f(x) \oplus g(y) \oplus f(x') \oplus g(y') = 0 \implies$ collision resistance 2^{128}
- using MD-strengthening, same result for hash function
- proof without MD-str., (Fouque/Stern/Zimmer, SAC 2008)

Security below birthday/brute force?

- with 512-bit state, 2^{128} security level for collisions
- use output transformation and truncation
- output transformation

$$P(x) \oplus x$$

  (coll. resistant + one-way if P ideal)
- finally: truncation to 256 bits.

P and Q (Grøstl-256)

- Inspired by Rijndael
- 8×8 matrix of bytes (512 bits)
- ~~AddRoundKey~~ AddRoundConstant
- Same S-box (SubBytes)
- Shift of rows (to the right instead of left)
- Mixing of bytes in columns (d-byte diff. $\rightarrow$ $(9-d)$-byte diff.)
- Same diffusion properties (2 rounds)

New "MixColumns"

$$\begin{pmatrix} 02 & 0c & 06 & 08 & 01 & 04 & 01 & 01 \\ 01 & 02 & 0c & 06 & 08 & 01 & 04 & 01 \\ 01 & 01 & 02 & 0c & 06 & 08 & 01 & 04 \\ 04 & 01 & 01 & 02 & 0c & 06 & 08 & 01 \\ 01 & 04 & 01 & 01 & 02 & 0c & 06 & 08 \\ 08 & 01 & 04 & 01 & 01 & 02 & 0c & 06 \\ 06 & 08 & 01 & 04 & 01 & 01 & 02 & 0c \\ 0c & 06 & 08 & 01 & 04 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{pmatrix} \text{state}$$

(in $\mathbb{F}_{256}$)

P and Q

- 10 rounds each
- P and Q are different permutations with different round constants
- Number of rounds a security parameter
- We do not claim "ideality" of P and Q

Grøstl-512

- similar to Grøstl-256
- 8×16 matrix
- 14 rounds

Speed

- Grøstl with 10 rounds
- 64-bit processors: $\sim$20 cycles/byte (SHA-256: 21)
- 32-bit processors: with MMX/SSE instructions, $\sim$23 cycles/byte
- Hardware(ASIC), throughput 6Gbit/s.

Grøstl

- Simple design, built from known components
- For all versions, internal state at least twice of the output

Name

- Gröstl: Austrian dish, similar to corned beef (hash)
- Often made from leftovers
- Danish name for Gröstl is Biksemad
- Norwegian name for Gröstl is Pytt-i-Panne
- Equivalent of ö in Danish is ø, hence Grøstl