Cryptographic hash functions V

Sponge functions

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Sponge for hash function

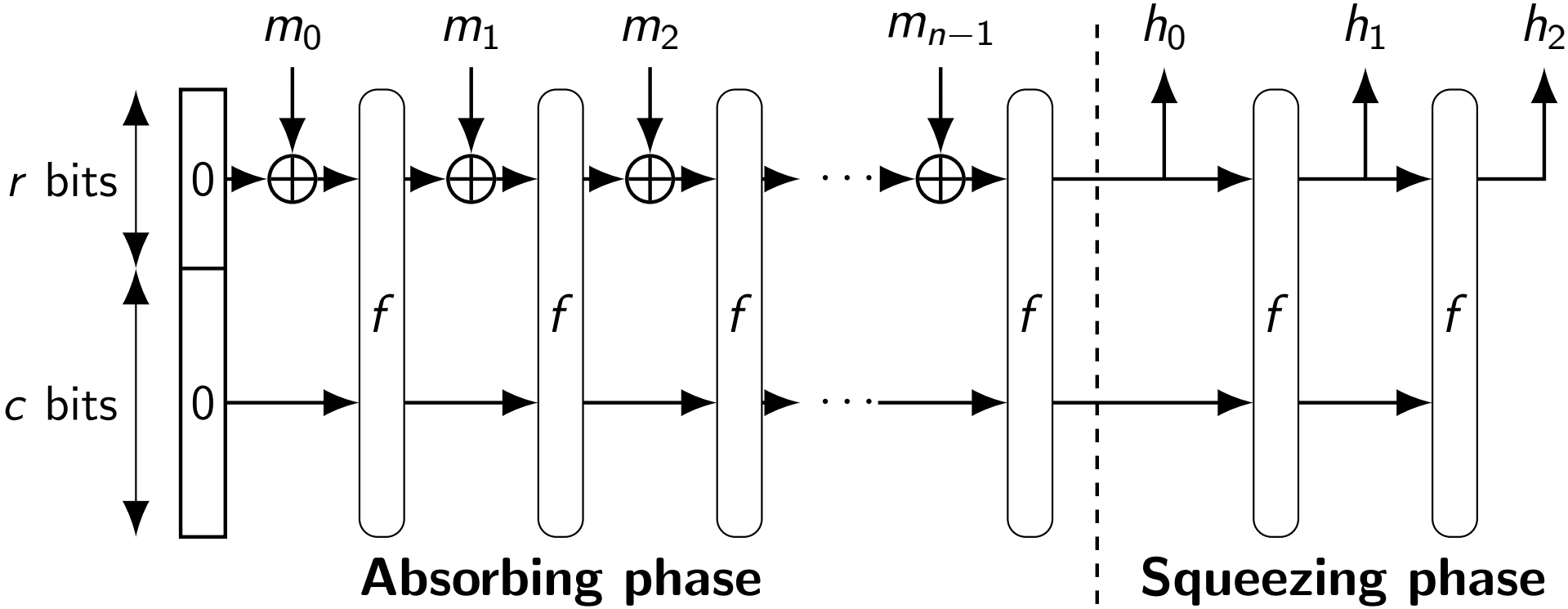

Image credit: adapted from Jérémy Jean

- m_i: message blocks, each having r bits; pad if necessary.
- h_i: blocks of hash output, each having r bits, total of d bits.
- f: permutation on $\{0,1\}^{r+c}$.
- c: "capacity"; never output bits in bottom c positions.
- r: "rate" this many bits are absorbed or squeezed out per f.
- c determines security, r determines efficiency.

Details for SHA-3

SHA-3 is new (2015) hash function standard, issued by NIST after public competition. SHA-3-d outputs d bits, $r + c = 1600$.

- m_i: message blocks, each having r bits; pad if necessary.
- h_i: blocks of hash output, each having r bits, total of d bits.
- f: permutation on $\{0,1\}^{r+c}$.
- c: "capacity"; never output bits in bottom c positions.
- r: "rate" this many bits are absorbed or squeezed out per f.
- c determines security, r determines efficiency.

Details for SHA-3

SHA-3 is new (2015) hash function standard, issued by NIST after public competition. SHA-3-d outputs d bits, $r + c = 1600$.

- m_i: message blocks, each having r bits; pad if necessary. Message m, append $p = 10 \ldots 01$ so that r divides $\text{len}(m||p)$. This appends at least 2 bits (11) and at most $r + 1$ bits. Let $n = \text{len}(m||p)/r$.
- h_i: blocks of hash output, each having r bits, total of d bits.
- f: permutation on $\{0,1\}^{r+c}$.
- c: "capacity"; never output bits in bottom c positions.
- r: "rate" this many bits are absorbed or squeezed out per f.
- c determines security, r determines efficiency.

Details for SHA-3

SHA-3 is new (2015) hash function standard, issued by NIST after public competition. SHA-3-d outputs d bits, $r + c = 1600$.

- m_i: message blocks, each having r bits; pad if necessary. Message m, append $p = 10 \ldots 01$ so that r divides $\text{len}(m||p)$. This appends at least 2 bits (11) and at most $r + 1$ bits. Let $n = \text{len}(m||p)/r$.
- h_i: blocks of hash output, each having r bits, total of d bits. d depends on security level, output blocks possibly truncated.
- f: permutation on $\{0,1\}^{r+c}$.
- c: "capacity"; never output bits in bottom c positions.
- r: "rate" this many bits are absorbed or squeezed out per f.
- c determines security, r determines efficiency.

Details for SHA-3

SHA-3 is new (2015) hash function standard, issued by NIST after public competition. SHA-3-d outputs d bits, $r + c = 1600$.

- m_i: message blocks, each having r bits; pad if necessary.
  Message m, append $p = 10 \ldots 01$ so that r divides $\text{len}(m||p)$.
  This appends at least 2 bits (11) and at most $r + 1$ bits.
  Let $n = \text{len}(m||p)/r$.
- h_i: blocks of hash output, each having r bits, total of d bits.
  d depends on security level, output blocks possibly truncated.
- f: permutation on $\{0,1\}^{r+c}$.
  f should be efficient and look random, optimization target.
- c: "capacity"; never output bits in bottom c positions.
- r: "rate" this many bits are absorbed or squeezed out per f.
- c determines security, r determines efficiency.

Details for SHA-3

SHA-3 is new (2015) hash function standard, issued by NIST after public competition. SHA-3-d outputs d bits, $r + c = 1600$.

- m_i: message blocks, each having r bits; pad if necessary.
  Message m, append $p = 10 \ldots 01$ so that r divides $\text{len}(m||p)$.
  This appends at least 2 bits (11) and at most $r + 1$ bits.
  Let $n = \text{len}(m||p)/r$.
- h_i: blocks of hash output, each having r bits, total of d bits.
  d depends on security level, output blocks possibly truncated.
- f: permutation on $\{0,1\}^{r+c}$.
  f should be efficient and look random, optimization target.
- c: "capacity"; never output bits in bottom c positions.
  Can make security reduction assuming that f is random.
  PRE and SPR are $\min\{2^{c/2}, 2^d\}$. CR is $\min\{2^{c/2}, 2^{d/2}\}$.
- r: "rate" this many bits are absorbed or squeezed out per f.

- c determines security, r determines efficiency.

Details for SHA-3

SHA-3 is new (2015) hash function standard, issued by NIST after public competition. SHA-3-d outputs d bits, $r + c = 1600$.

- m_i: message blocks, each having r bits; pad if necessary.
  Message m, append $p = 10 \ldots 01$ so that r divides $\text{len}(m||p)$.
  This appends at least 2 bits (11) and at most $r + 1$ bits.
  Let $n = \text{len}(m||p)/r$.
- h_i: blocks of hash output, each having r bits, total of d bits.
  d depends on security level, output blocks possibly truncated.
- f: permutation on $\{0,1\}^{r+c}$.
  f should be efficient and look random, optimization target.
- c: "capacity"; never output bits in bottom c positions.
  Can make security reduction assuming that f is random.
  PRE and SPR are $\min\{2^{c/2}, 2^d\}$. CR is $\min\{2^{c/2}, 2^{d/2}\}$.
- r: "rate" this many bits are absorbed or squeezed out per f.
  $r = 1600 - c$. Choices are $c \in \{224, 256, 384, 512\}$.
- c determines security, r determines efficiency.