Observations of non-randomness in the ESSENCE compression function

Nicky Mouha[1,2] Søren S. Thomsen[3]
Meltem Sönmez Turan[4] Bart Preneel[1,2]

[1] ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Belgium

[2] Interdisciplinary Institute for BroadBand Technology (IBBT), Belgium

[3] Department of Mathematics, Technical University of Denmark, Denmark

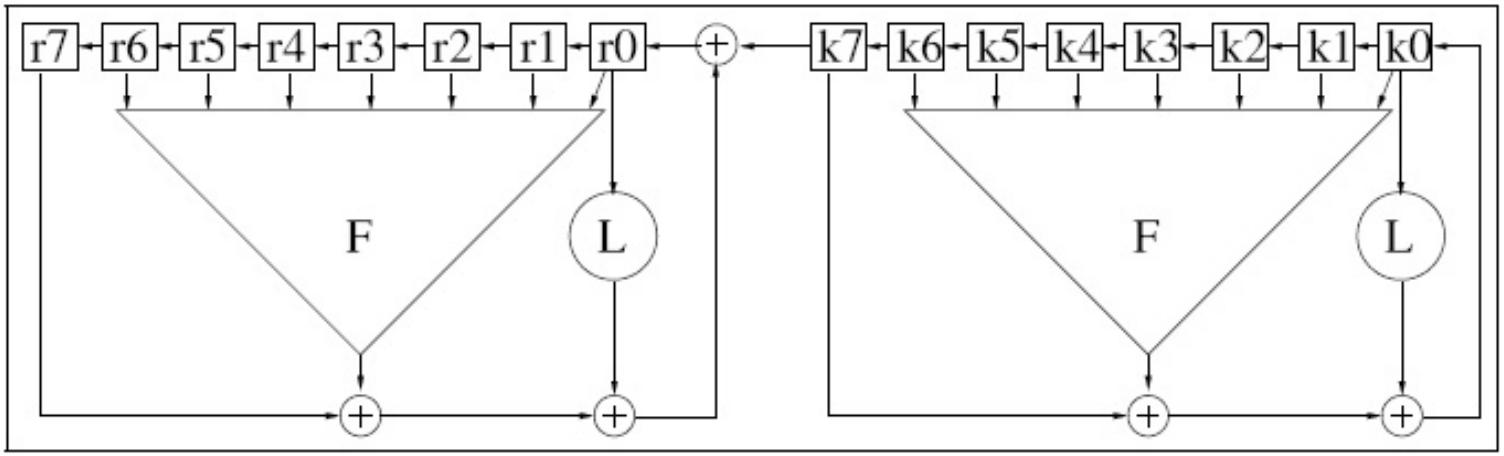
[4] Institute of Applied Mathematics, Middle East Technical University, Turkey

February 28, 2009

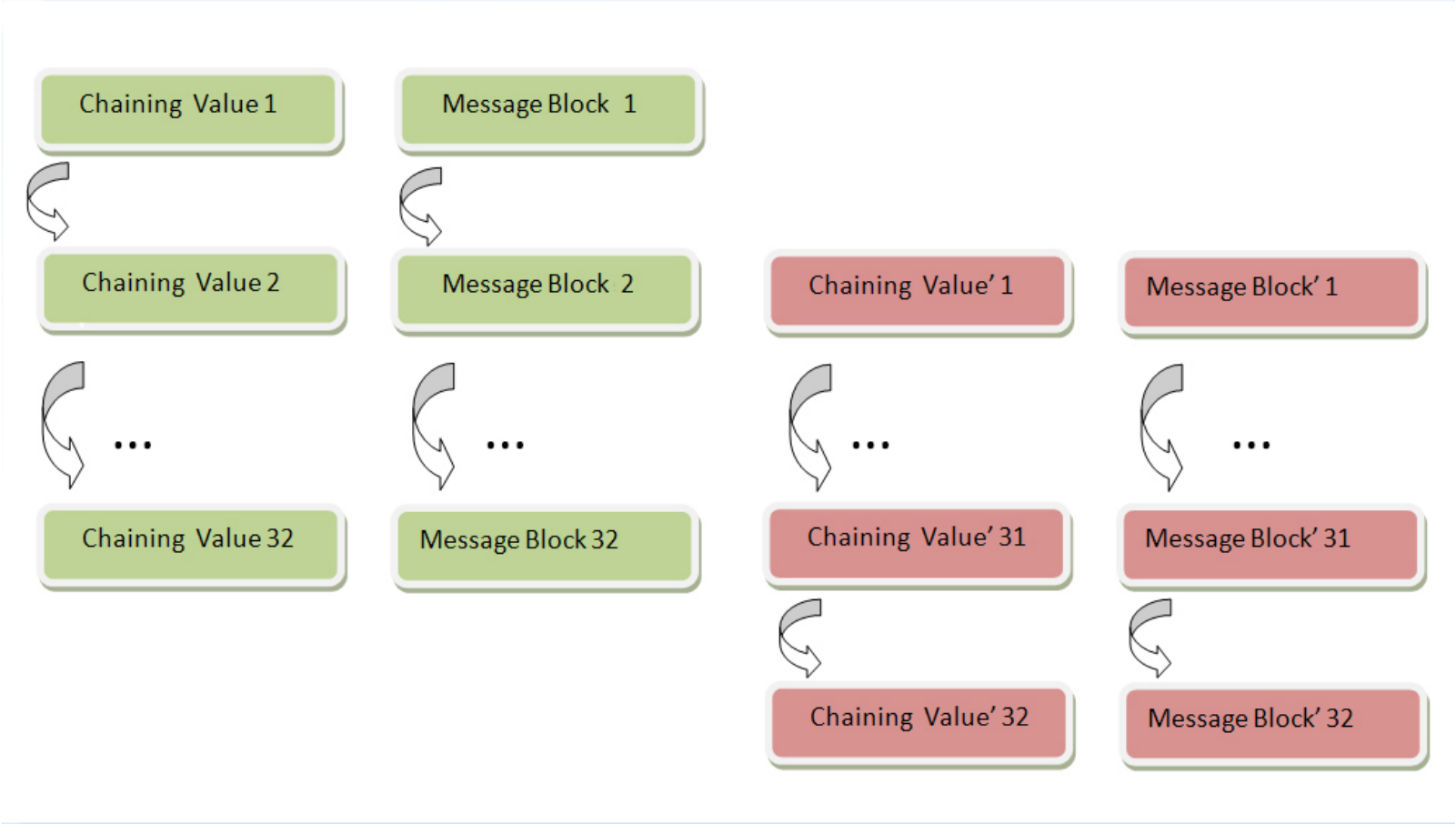
Essence Compression function

- SHA-3 submission by Jason Worth Martin
- Two inputs to compression function:
  - chaining value $(r_0, \ldots, r_7)$
  - message block $(k_0, \ldots, k_7)$
- Step update equations:

$$F(r_6, r_5, r_4, r_3, r_2, r_1, r_0) \oplus r_7 \oplus L(r_0) \oplus k_7 = r_0 \ ,$$
$$F(k_6, k_5, k_4, k_3, k_2, k_1, k_0) \oplus k_7 \oplus L(k_0) = k_0 \ .$$

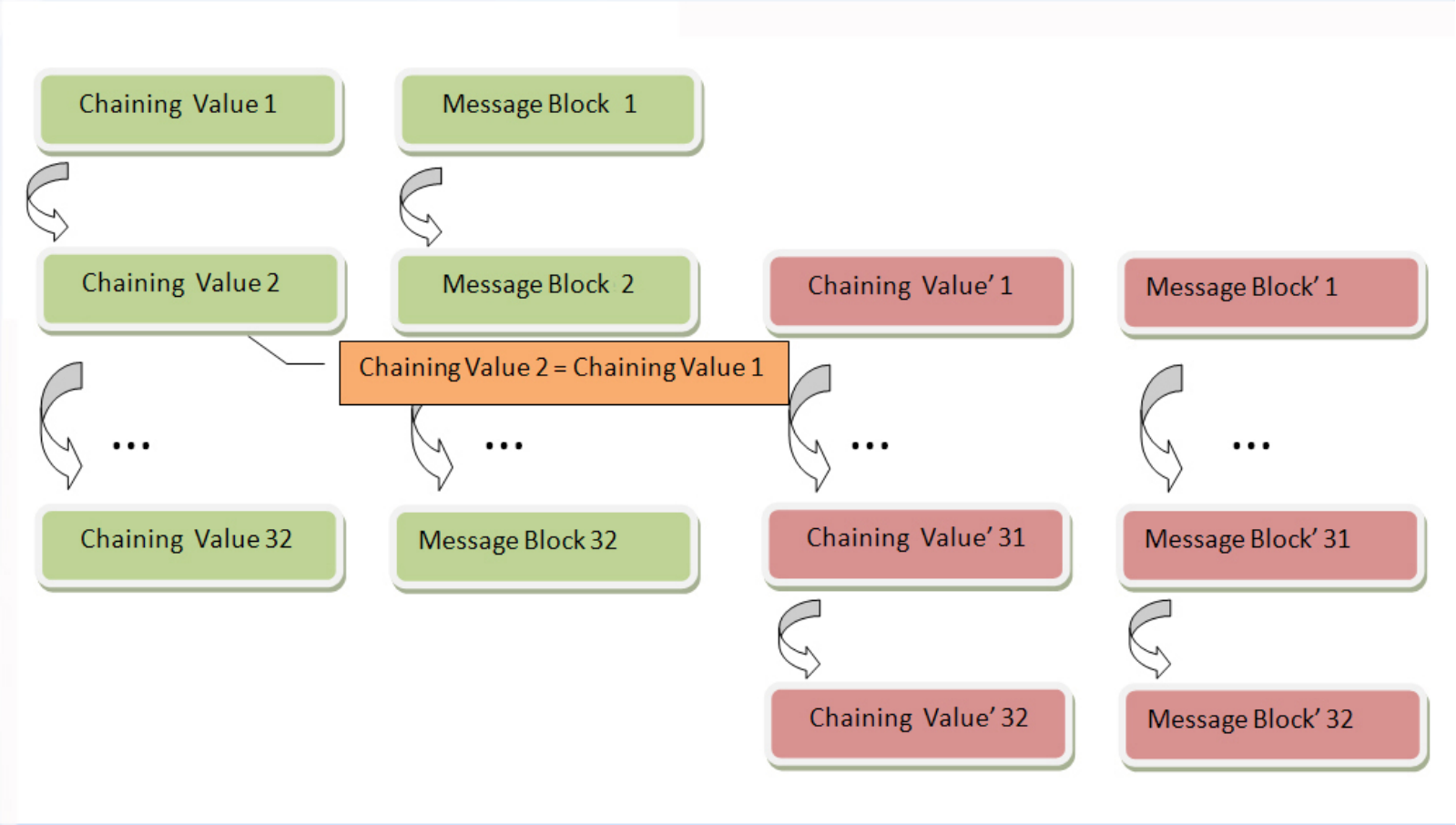


Slid Pairs in ESSENCE Compression Function



c	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
c'	ffffffff	00000000	00000000	00000000	00000000	00000000	00000000	00000000
m	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
m'	ffffffff	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R	6b202ef2	bb610a07	97e43146	9bd34ae3	c8bc7cbf	b8ee4a3c	b6118dc5	775f7bbf
R'	c07abcfa	6b202ef2	bb610a07	97e43146	9bd34ae3	c8bc7cbf	b8ee4a3c	b6118dc5

Slid Pairs with Identical Chaining Values



$c = c'$	243f6a88	243f6a88	243f6a88	243f6a88	243f6a88	243f6a88	243f6a88	243f6a88
m	00000000	00000000	00000000	00000000	00000000	00000000	00000000	f6b1eb63
m'	094e149c	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R	be31aa01	eb6e9f07	ead99889	6fe79b44	391ccd35	67fdb8b6	fc3aa0f6	6e80148e
R'	f86d77c6	be31aa01	eb6e9f07	ead99889	6fe79b44	391ccd35	67fdb8b6	fc3aa0f6

Fixed Points for Reduced Rounds of ESSENCE Compression Function

- 1-step fixed point $\Rightarrow$ 32-step fixed point
- After Davies-Meyer feed-forward, resulting hash value is zero.

Fixed Points for Reduced Rounds of ESSENCE Compression Function

- 1-step fixed point $\Rightarrow$ 32-step fixed point
- After Davies-Meyer feed-forward, resulting hash value is zero.

Fixed Points for one step

For one-step fixed point, $c_0 = c_1 = \ldots = c_7$ and $m_0 = m_1 = \ldots = m_7$

$$F(c_0, c_0, c_0, c_0, c_0, c_0, c_0) \oplus c_0 \oplus L(c_0) \oplus m_0 = c_0 \ ,$$
$$F(m_0, m_0, m_0, m_0, m_0, m_0, m_0) \oplus m_0 \oplus L(m_0) = m_0 \ .$$

	ESSENCE-256	ESSENCE-512
c_0	0x993ae9b9	0xd5b330380561ecf7
m_0	0x307a380c	0x10ad290affb19779

Conclusion

- For ESSENCE compression function:
  - Slid pairs
  - Fixed point
- For ESSENCE hash function:
  - No direct consequences
  - Still secure
- Full article at SHA-3 Zoo:
  - `http://ehash.iaik.tugraz.at/wiki/ESSENCE`