

Practical Collisions for EnRUPT

Sebastiaan Indestege

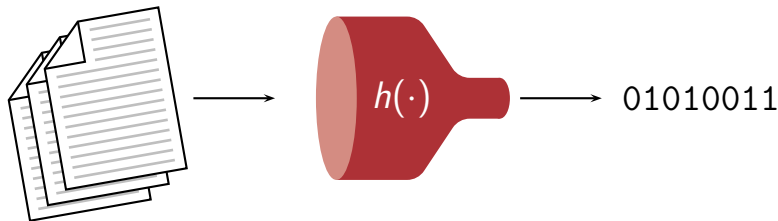
`sebastiaan.indestege@esat.kuleuven.be`

COSIC, ESAT/SCD, K.U. Leuven, Belgium

Dagstuhl

12 January 2009

Cryptographic Hash Functions



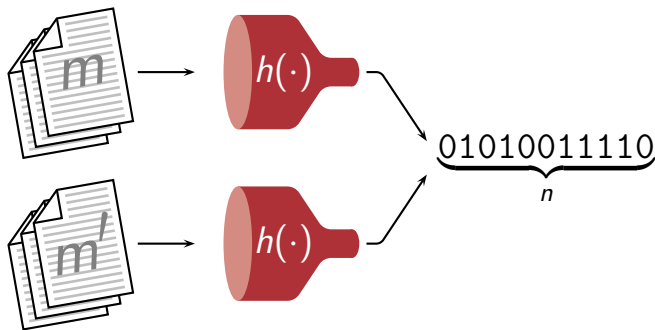
$$h : \{0, 1\}^* \mapsto \{0, 1\}^w$$

Desired properties

- Collision resistance, (Second) preimage resistance, ...
- Efficiently computable, *i.e.*, fast!

Cryptographic Hash Functions

Collision Resistance



- “Hard” to find $m \neq m'$ s.t. $h(m) = h(m')$.
- Birthday paradox $\mathcal{O}(2^{n/2})$

EnRUPT

- SHA-3 round 1 candidate
- Designers: Sean O'Neil, Karsten Nohl, Luca Henzen
- Many parameters, **7 concrete proposals**

EnRUPT

- SHA-3 round 1 candidate
- Designers: Sean O'Neil, Karsten Nohl, Luca Henzen
- Many parameters, **7 concrete proposals**

EnRUPT is a “stream” hash function

- ① Initialisation
- ② Process each 32 or 64-bit message word just once
(*no message expansion, message block schedule, . . .*)
- ③ Finalisation

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $e \leftarrow ((x_\alpha \lll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $f \leftarrow (e \lll 3) \boxplus e$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus f$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus f$ 
11:  end for
12:   $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:   $r \leftarrow r + s \cdot P$ 
14:  return  $\langle d, x, r \rangle$ 
15: end function
```

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $e \leftarrow ((x_\alpha \lll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $f \leftarrow (e \lll 3) \boxplus e$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus f$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus f$ 
11:   end for
12:    $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:    $r \leftarrow r + s \cdot P$ 
14:   return  $\langle d, x, r \rangle$ 
15: end function
```

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $e \leftarrow ((x_\alpha \lll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $f \leftarrow (e \lll 3) \boxplus e$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus f$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus f$ 
11:  end for
12:   $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:   $r \leftarrow r + s \cdot P$ 
14:  return  $\langle d, x, r \rangle$ 
15: end function
```

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $e \leftarrow ((x_\alpha \lll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $f \leftarrow (e \lll 3) \boxplus e$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus f$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus f$ 
11:   end for
12:    $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:    $r \leftarrow r + s \cdot P$ 
14:   return  $\langle d, x, r \rangle$ 
15: end function
```

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $\mathbf{e} \leftarrow ((x_\alpha \ll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $\mathbf{f} \leftarrow (\mathbf{e} \ll 3) \boxplus \mathbf{e}$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus \mathbf{f}$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus \mathbf{f}$ 
11:   end for
12:    $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:    $r \leftarrow r + s \cdot P$ 
14:   return  $\langle d, x, r \rangle$ 
15: end function
```

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $e \leftarrow ((x_\alpha \ll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $f \leftarrow (e \ll 3) \boxplus e$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus f$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus f$ 
11:  end for
12:   $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:   $r \leftarrow r + s \cdot P$ 
14:  return  $\langle d, x, r \rangle$ 
15: end function
```

EnRUPT

Round function

```
1: function round ( $\langle d, x, r \rangle, m$ )
2:   for  $i = 0$  to  $s \cdot P - 1$  do
3:      $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$ 
4:      $\beta \leftarrow r + i + 2P \bmod H$ 
5:      $\gamma \leftarrow r + i + P \bmod H$ 
6:      $\xi \leftarrow r + i \bmod H$ 
7:      $e \leftarrow ((x_\alpha \lll 1) \oplus x_\beta \oplus d_{i \bmod P} \oplus \text{uint}_w(r + i)) \ggg w/4$ 
8:      $f \leftarrow (e \lll 3) \boxplus e$ 
9:      $x_\gamma \leftarrow x_\gamma \oplus f$ 
10:     $d_{i \bmod P} \leftarrow d_{i \bmod P} \oplus x_\xi \oplus f$ 
11:  end for
12:   $d_{P-1} \leftarrow d_{P-1} \oplus m$ 
13:   $r \leftarrow r + s \cdot P$ 
14:  return  $\langle d, x, r \rangle$ 
15: end function
```

Attacking EnRUPT

Observation

- Most of EnRUPT is **GF2-linear**
- Only $\mathbf{f} \leftarrow (\mathbf{e} \lll 3) \boxplus \mathbf{e}$ is non-linear

Attacking EnRUPT

Observation

- Most of EnRUPT is **GF2-linear**
- Only $\mathbf{f} \leftarrow (\mathbf{e} \lll 3) \boxplus \mathbf{e}$ is non-linear

Attack strategy

- 1 **Approximate** non-linear \boxplus by linear \oplus

Attacking EnRUPT

Observation

- Most of EnRUPT is **GF2-linear**
- Only $f \leftarrow (e \lll 3) \boxplus e$ is non-linear

Attack strategy

- 1 **Approximate** non-linear \boxplus by linear \oplus
- 2 Find a **differential characteristic**

Attacking EnRUPT

Observation

- Most of EnRUPT is **GF2-linear**
- Only $\mathbf{f} \leftarrow (\mathbf{e} \lll 3) \boxplus \mathbf{e}$ is non-linear

Attack strategy

- 1 **Approximate** non-linear \boxplus by linear \oplus
- 2 Find a **differential characteristic**
- 3 Find a **conforming pair**

Attacking EnRUPT

Details (1)

Finding a good differential characteristic

- Heuristic: **low-weight** difference at input of \boxplus
- Use coding theory?
(search for low-weight codewords in a linear code)
- Can quickly evaluate **DP^{×9} exactly**
(using a trellis and the Viterbi algorithm)
- Use a modified simple algorithm to find low-weight codewords to directly minimize the **real** attack complexity

Attacking EnRUPT

Details (2)

Finding a conforming pair

- New freedom in every round
(message words used only once)
- Do **one round** at a time
(backtrack when required)
- Total complexity: **sum** of round complexities
(not product of round complexities)

Attacking EnRUPT

Details (3)

Speedup: message modification

- Do not pick message word, but
 - ① Pick **input to first** \boxplus of a round
(easy to enumerate “good” values)
 - ② Compute backwards to find message word
- First step of a round comes **for free!**

Results

- Constructed a differential characteristic for all seven EnRUPT variants

variant	time complexity	message length
EnRUPT-128	$2^{36.04}$	6
EnRUPT-160	$2^{37.78}$	7
EnRUPT-192	$2^{38.33}$	8
EnRUPT-224	$2^{37.02}$	6
EnRUPT-256	$2^{37.02}$	6
EnRUPT-384	$2^{39.63}$	8
EnRUPT-512	$2^{38.46}$	10

Example: EnRUPT-256

	5	4800280000000800 _x	→	0801680000004800 _x	2 ^{-11.20}	
	6	90000002d0000000 _x	→	100001450000000 _x	2 ^{-6.43}	
	7	0000280168000800 _x	→	0001680a28004800 _x	2 ^{-11.02}	
inject message word difference $\Delta m_0 = 0000002280000000_x$						
1	0	90000002d0000000 _x	→	100001450000000 _x	2 ^{-6.43}	2^{-36.56}
	1	0000280168000000 _x	→	0001680a28000000 _x	*	
	2	90000002d0000000 _x	→	100001450000000 _x	2 ^{-6.43}	
	3	4800280000000000 _x	→	0801680000000000 _x	2 ^{-5.43}	
	4	90000002d0000000 _x	→	100001450000000 _x	2 ^{-6.43}	
	5	0000080000000000 _x	→	0000480000000000 _x	2 ^{-1.85}	
	6	9000000240000000 _x	→	100001040000000 _x	2 ^{-3.70}	
	7	4800080120000000 _x	→	0800480820000000 _x	2 ^{-6.54}	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000 _x	→	100001040000000 _x	2 ^{-3.70}	2^{-34.08}
	1	0000080048000000 _x	→	0000480208000000 _x	*	
	2	9000000240000000 _x	→	100001040000000 _x	2 ^{-3.70}	
	3	4800080168000000 _x	→	0800480a28000000 _x	2 ^{-9.28}	
	4	9000000240000000 _x	→	100001040000000 _x	2 ^{-3.70}	
	5	0000200000000000 _x	→	0001200000000000 _x	2 ^{-1.85}	
	6	9000000000000000 _x	→	1000000000000000 _x	2 ^{-0.85}	
	7	4800200000000000 _x	→	0801200000000000 _x	2 ^{-3.70}	
inject message word difference $\Delta m_2 = 0000000208000000_x$						

Example: EnRUPT-256

	4	90000002d0000000 _x	→	1000001450000000 _x	2 ^{-6.43}	
	5	0000080000000000 _x	→	0000480000000000 _x	2 ^{-1.85}	
	6	9000000240000000 _x	→	1000001040000000 _x	2 ^{-3.70}	
	7	4800080120000000 _x	→	0800480820000000 _x	2 ^{-6.54}	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000 _x	→	1000001040000000 _x	2 ^{-3.70}	2^{-34.08}
	1	0000080048000000 _x	→	0000480208000000 _x	*	
	2	9000000240000000 _x	→	1000001040000000 _x	2 ^{-3.70}	
	3	4800080168000000 _x	→	0800480a28000000 _x	2 ^{-9.28}	
	4	9000000240000000 _x	→	1000001040000000 _x	2 ^{-3.70}	
	5	0000200000000000 _x	→	0001200000000000 _x	2 ^{-1.85}	
	6	9000000000000000 _x	→	1000000000000000 _x	2 ^{-0.85}	
	7	4800200000000000 _x	→	0801200000000000 _x	2 ^{-3.70}	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000 _x	→	1000000000000000 _x	2 ^{-0.85}	2^{-23.91}
	1	0000280120000000 _x	→	0001680820000000 _x	*	
	2	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70}	
	3	4800280168000000 _x	→	0801680a28000000 _x	2 ^{-11.02}	
	4	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70}	
	5	0000080048000000 _x	→	0000480208000000 _x	2 ^{-4.70}	
	6	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70}	

Example: EnRUPT-256

	3	4800080168000000 _x	→	0800480a28000000 _x	2 ^{-9.28}	
	4	9000000240000000 _x	→	1000001040000000 _x	2 ^{-3.70}	
	5	0000200000000000 _x	→	0001200000000000 _x	2 ^{-1.85}	
	6	9000000000000000 _x	→	1000000000000000 _x	2 ^{-0.85}	
	7	4800200000000000 _x	→	0801200000000000 _x	2 ^{-3.70}	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
	3	0	9000000000000000 _x	→	1000000000000000 _x	2 ^{-0.85} 2^{-23.91}
		1	0000280120000000 _x	→	0001680820000000 _x	*
		2	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70}
		3	4800280168000000 _x	→	0801680a28000000 _x	2 ^{-11.02}
		4	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70}
		5	0000080048000000 _x	→	0000480208000000 _x	2 ^{-4.70}
		6	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70}
		7	4800080000000000 _x	→	0800480000000000 _x	2 ^{-3.70}
inject message word difference $\Delta m_3 = 0000000200000000_x$						
	4	0	9000000090000000 _x	→	1000000410000000 _x	2 ^{-3.70} 2^{-34.19}
		1	0000080000000800 _x	→	0000480000004800 _x	*
		2	0000000000000000 _x	→	0000000000000000 _x	2 ^{-0.00}
		3	0000080000000800 _x	→	0000480000004800 _x	2 ^{-3.70}
		4	0000000000000000 _x	→	0000000000000000 _x	2 ^{-0.00}
		5	4800080048000800 _x	→	0800480208004800 _x	2 ^{-8.39}

Example: EnRUPT-256

	1	0000200120000000 _x	→	0001000020000000 _x	$2^{-3.70}$	
	2	9000000090000000 _x	→	1000000410000000 _x	$2^{-11.02}$	
	3	4800280168000000 _x	→	0801680a28000000 _x	$2^{-3.70}$	
	4	9000000090000000 _x	→	1000000410000000 _x	$2^{-4.70}$	
	5	0000800480000000 _x	→	0000480208000000 _x	$2^{-3.70}$	
	6	9000000090000000 _x	→	1000000410000000 _x	$2^{-3.70}$	
	7	4800080000000000 _x	→	0800480000000000 _x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000002000000000x$						
4	0	9000000090000000 _x	→	1000000410000000 _x	$2^{-3.70}$	$2^{-34.19}$
	1	0000800000000800 _x	→	0000480000004800 _x	*	
	2	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	
	3	0000800000000800 _x	→	0000480000004800 _x	$2^{-3.70}$	
	4	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	
	5	4800080048000800 _x	→	0800480208004800 _x	$2^{-8.39}$	
	6	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	
	7	4800080048000800 _x	→	0800480208004800 _x	$2^{-8.39}$	
inject message word difference $\Delta m_3 = 0000002000000000x$						
5	0	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	$2^{-20.49}$
	1	0000000000000000 _x	→	0000000000000000 _x	*	
	⋮	⋮	→	⋮	⋮	
	7	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	$2^{-0.00}$

Example: EnRUPT-256

4	0	9000000090000000 _x	→	1000000410000000 _x	$2^{-9.70}$	$2^{-9.19}$
	1	0000080000000800 _x	→	0000480000004800 _x	*	
	2	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	
	3	0000080000000800 _x	→	0000480000004800 _x	$2^{-3.70}$	
	4	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	
	5	4800080048000800 _x	→	0800480208004800 _x	$2^{-8.39}$	
	6	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	
	7	4800080048000800 _x	→	0800480208004800 _x	$2^{-8.39}$	
inject message word difference $\Delta m_3 = 0000002000000000_x$						
5	0	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	$2^{-20.49}$
	1	0000000000000000 _x	→	0000000000000000 _x	*	
	⋮	⋮	→	⋮	⋮	
	7	0000000000000000 _x	→	0000000000000000 _x	$2^{-0.00}$	$2^{-0.00}$

Conclusion

- Collision attacks on EnRUPT
- Breaks **all seven** proposed EnRUPT variants
- Mitigation: increase s -parameter (O'Neil)

