Practical Collisions for EnRUPT

Sebastiaan Indesteege Bart Preneel

COSIC, ESAT, K.U. Leuven, Belgium

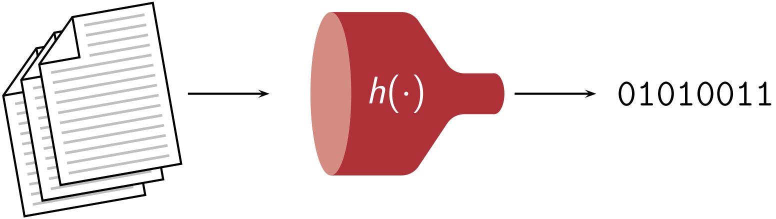
Fast Software Encryption 2009

Outline

Outline

1. Introduction
2. Description of EnRUPT
3. Attacking EnRUPT
4. Results
5. Conclusion

Cryptographic Hash Functions



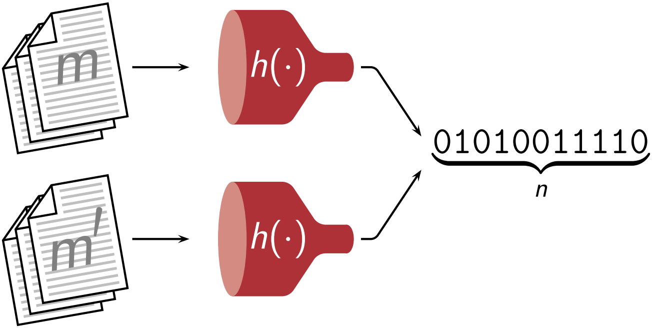
$$h : \{0,1\}^* \mapsto \{0,1\}^w$$

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

EnRUPT

- SHA-3 round 1 candidate
- Sean O'Neil, Karsten Nohl, Luca Henzen [ONH08]
- Many parameters, **7 concrete proposals**

This talk

None of the 7 proposed EnRUPT variants is collision resistant

Outline

Description of EnRUPT

EnRUPT variant	digest length h	word size w	parallelisation level P	security parameter s	number of state words H
EnRUPT-128	128 bits	32 bits	2	4	8
EnRUPT-160	160 bits	32 bits	2	4	10
EnRUPT-192	192 bits	32 bits	2	4	12
EnRUPT-224	224 bits	64 bits	2	4	8
EnRUPT-256	256 bits	64 bits	2	4	8
EnRUPT-384	384 bits	64 bits	2	4	12
EnRUPT-512	512 bits	64 bits	2	4	16

Description of EnRUPT

1. **Initialisation**
   - Set internal state $\langle \mathbf{d[P], x[H], r} \rangle$
2. **Message Processing**
   - Process each or w-bit message word just once
   - No message expansion, message block schedule, ...
   - Uses the **round function**
3. **Finalisation**
   - Generate message digest from internal state

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$

  for $i = 0$ to $s \cdot P - 1$ **do**

    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$

    $\beta \leftarrow r + i + 2P \bmod H$

    $\gamma \leftarrow r + i + P \bmod H$

    $\xi \leftarrow r + i \bmod H$

    $e \leftarrow ((x[\alpha] \lll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $f \leftarrow (e \lll 3) \boxplus e$

    $x_\gamma \leftarrow x_\gamma \oplus f$

    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$

  end for

  $d_{P-1} \leftarrow d_{P-1} \oplus m$

  $r \leftarrow r + s \cdot P$

  return $\langle d[P], x[H], r\rangle$

end function

Round Function

function round $(\langle \mathbf{d[P], x[H], r} \rangle, \mathbf{m})$

  for $i = 0$ to $s \cdot P - 1$ **do**

    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$

    $e \leftarrow ((x[\alpha] \lll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $f \leftarrow (e \lll 3) \boxplus e$

    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for

  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$

  return $\langle d[P], x[H], r \rangle$

end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$

  for $\mathbf{i = 0}$ **to** $\mathbf{s \cdot P - 1}$ **do**

    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$

    $e \leftarrow ((x[\alpha] \lll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $f \leftarrow (e \lll 3) \boxplus e$

    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for

  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$

  return $\langle d[P], x[H], r\rangle$

end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$

  for $i = 0$ to $s \cdot P - 1$ **do**

    $\alpha \leftarrow \mathbf{r + (i + 1 \bmod P) \bmod H}$
    $\beta \leftarrow \mathbf{r + i + 2P \bmod H}$
    $\gamma \leftarrow \mathbf{r + i + P \bmod H}$
    $\xi \leftarrow \mathbf{r + i \bmod H}$

    $e \leftarrow ((x[\alpha] \ll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $f \leftarrow (e \ll 3) \boxplus e$

    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for

  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$

  return $\langle d[P], x[H], r\rangle$

end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$

  for $i = 0$ to $s \cdot P - 1$ **do**

    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$

    $e \leftarrow ((x[\alpha] \lll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $f \leftarrow (e \lll 3) \boxplus e$

    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for

  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$

  return $\langle d[P], x[H], r\rangle$

end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$

  for $i = 0$ to $s \cdot P - 1$ **do**

    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$

    $e \leftarrow ((x[\alpha] \ll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $\mathbf{f} \leftarrow (\mathbf{e} \lll 3) \boxplus \mathbf{e}$

    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for

  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$

  return $\langle d[P], x[H], r\rangle$

end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$
  for $i = 0$ to $s \cdot P - 1$ **do**
    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$
    $e \leftarrow ((x[\alpha] \lll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$
    $f \leftarrow (e \lll 3) \boxplus e$
    $\mathbf{x_\gamma \leftarrow x_\gamma \oplus f}$
    $\mathbf{d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f}$
  end for
  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$
  return $\langle d[P], x[H], r\rangle$
end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$

  for $i = 0$ to $s \cdot P - 1$ **do**

    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$

    $e \leftarrow ((x[\alpha] \lll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$

    $f \leftarrow (e \lll 3) \boxplus e$

    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for

  $\mathbf{d_{P-1} \leftarrow d_{P-1} \oplus m}$
  $\mathbf{r \leftarrow r + s \cdot P}$

  return $\langle d[P], x[H], r\rangle$

end function

Round Function

function round $(\langle d[P], x[H], r\rangle, m)$
  for $i = 0$ to $s \cdot P - 1$ **do**
    $\alpha \leftarrow r + (i + 1 \bmod P) \bmod H$
    $\beta \leftarrow r + i + 2P \bmod H$
    $\gamma \leftarrow r + i + P \bmod H$
    $\xi \leftarrow r + i \bmod H$
    $e \leftarrow ((x[\alpha] \ll 1) \oplus x[\beta] \oplus d[i \bmod P] \oplus \mathrm{uint}_w(r + i)) \ggg w/4$
    $f \leftarrow (e \ll 3) \boxplus e$
    $x_\gamma \leftarrow x_\gamma \oplus f$
    $d[i \bmod P] \leftarrow d[i \bmod P] \oplus x[\xi] \oplus f$
  end for
  $d_{P-1} \leftarrow d_{P-1} \oplus m$
  $r \leftarrow r + s \cdot P$
  return $\langle \mathbf{d[P], x[H], r} \rangle$
end function

Outline

Attacking EnRUPT

Observation

- EnRUPT is **GF(2)-linear** except $\begin{cases} f & \leftarrow & e \boxplus (e \lll 3) \\ & \text{or} & \\ f & \leftarrow & e \times 9 \end{cases}$

Attack strategy

1. Find a **linear approximation**
2. Find a **differential characteristic**
3. Find a **conforming pair**

Similar to [CJ98] on SHA-0 and [RO05, PRR05] on SHA-1

Linear Approximation of EnRUPT

EnRUPT-$\mathcal{L}$

- Replace all non-linear $\boxplus$ by linear $\oplus$
  - i.e., ignore the carries

- Restrict to some fixed message length $t \cdot w$

$$\text{EnRUPT-}\mathcal{L}(m) = [o]_{1\times h} = [m]_{1\times tw} \cdot [\mathbf{O}]_{tw\times h}$$

- Differentials?

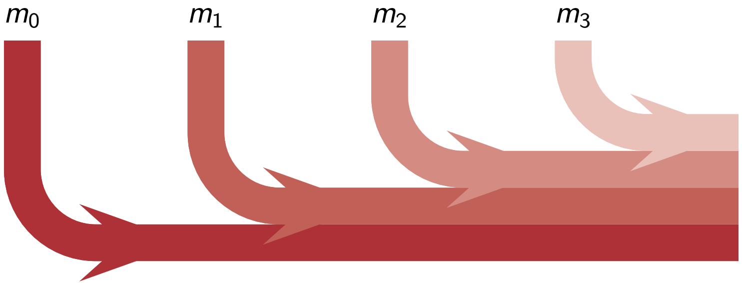
$$[\Delta o]_{1\times h} = [\Delta m]_{1\times tw} \cdot [\mathbf{O}]_{tw\times h}$$

“Good” Differential Characteristic, pt. I

- What is a **“good”** differential characteristic?
- Let’s skip this for now. . .

Round	Step	Δe	$\rightarrow$	Δf
inject message word difference $\Delta m_{-1} = 0000000008000000_x$				
0	0	0000000000000000_x	$\rightarrow$	0000000000000000_x
	1	0000000000000800_x	$\rightarrow$	0000000000004800_x
	2	9000000000000000_x	$\rightarrow$	1000000000000000_x
	3	4800000000000800_x	$\rightarrow$	0800000000004800_x
	4	9000000000000000_x	$\rightarrow$	1000000000000000_x
	5	4800280000000800_x	$\rightarrow$	0801680000004800_x
	6	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x
	7	0000280168000800_x	$\rightarrow$	$0001680a28004800_x$
inject message word difference $\Delta m_0 = 0000002280000000_x$				
1	0	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x
	1	0000280168000000_x	$\rightarrow$	$0001680a28000000_x$
	2	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x

Finding a Conforming Pair
Observation

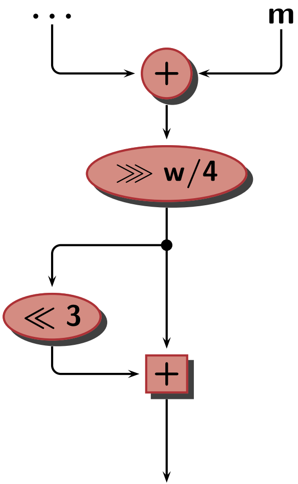


Observation

- Each message word is used only once
- New freedom in every round
- Search **round per round**

Finding a Conforming Pair

Finding it Faster

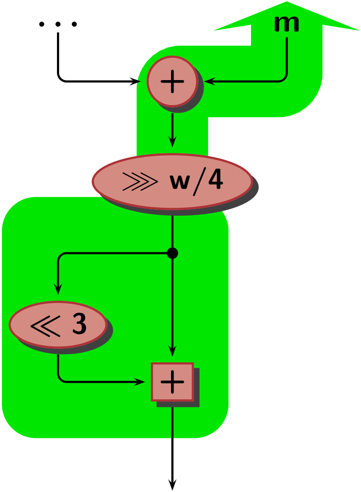


Message modification

- First step of a round **for free**!

Finding a Conforming Pair

Finding it Faster



Message modification

- First step of a round **for free**!

Finding a Conforming Pair
Round Complexities?

Need to estimate/compute $\mathrm{DP}^{\times 9}$

First Attempt

- $\mathbf{x \times 9 = x \boxplus (x << 3)}$
- Could use [LM01] to estimate $\mathrm{DP}^{\times 9}$:

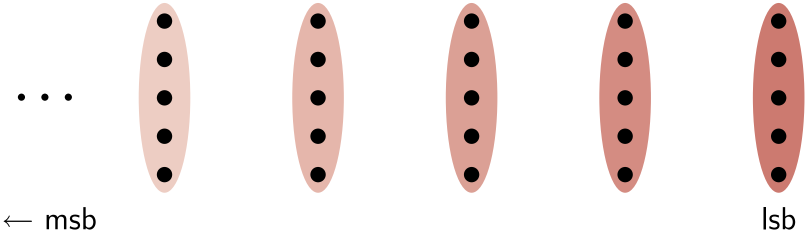
$$\mathrm{DP}^{\times 9}(\Delta) \approx 2^{-\mathrm{wt}\left(\left(\Delta \vee (\Delta \ll 3)\right) \wedge \mathrm{bin}\, 01\cdots 1000\right)}$$

(after simplification)

Finding a Conforming Pair

Round Complexities?

- Compact representation of $\mathbf{x} + (\mathbf{x} \lll 3)$ and $\mathbf{x}' + (\mathbf{x}' \lll 3)$ where $\mathbf{x}' = \mathbf{x} \oplus \mathbf{\Delta}$ in a **trellis**
- 2^5 nodes per segment $(c_i, c'_i, x_{i-2}, x_{i-1}, x_i)$

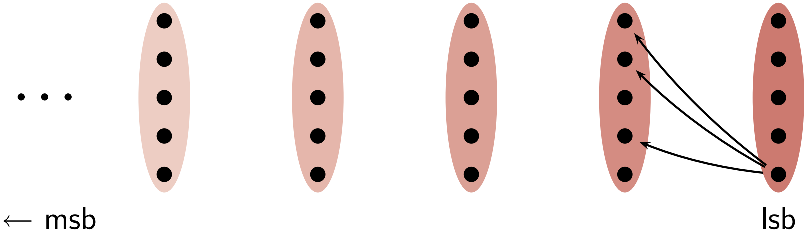


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

- Compact representation of $\mathbf{x} + (\mathbf{x} \lll 3)$ and $\mathbf{x}' + (\mathbf{x}' \lll 3)$ where $\mathbf{x}' = \mathbf{x} \oplus \mathbf{\Delta}$ in a **trellis**
- 2^5 nodes per segment $(c_i, c'_i, x_{i-2}, x_{i-1}, x_i)$

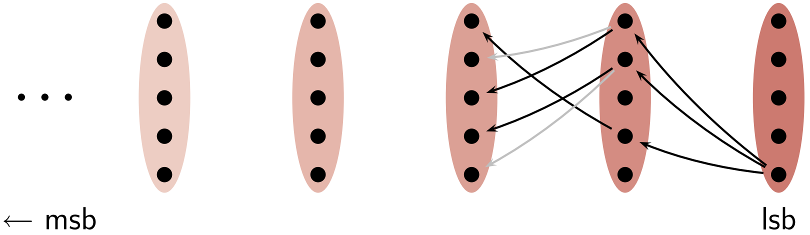


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

- Compact representation of $\mathbf{x} + (\mathbf{x} \lll 3)$ and $\mathbf{x}' + (\mathbf{x}' \lll 3)$ where $\mathbf{x}' = \mathbf{x} \oplus \boldsymbol{\Delta}$ in a **trellis**
- 2^5 nodes per segment $(c_i, c'_i, x_{i-2}, x_{i-1}, x_i)$

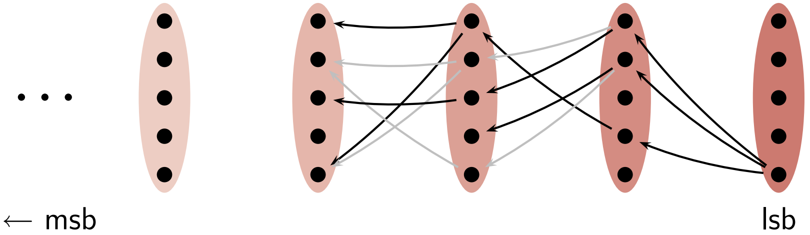


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

- Compact representation of $\mathbf{x} + (\mathbf{x} \ll 3)$ and $\mathbf{x}' + (\mathbf{x}' \ll 3)$ where $\mathbf{x}' = \mathbf{x} \oplus \boldsymbol{\Delta}$ in a **trellis**
- 2^5 nodes per segment $(c_i, c'_i, x_{i-2}, x_{i-1}, x_i)$

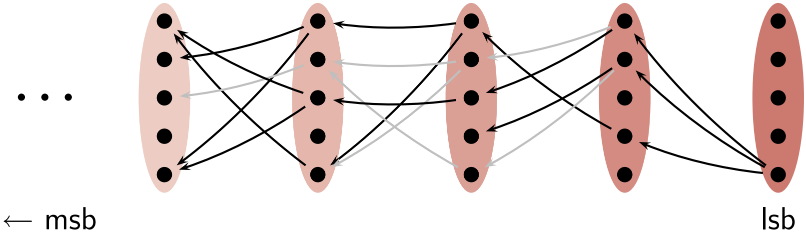


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

- Compact representation of $\mathbf{x} + (\mathbf{x} \ll 3)$ and $\mathbf{x}' + (\mathbf{x}' \ll 3)$ where $\mathbf{x}' = \mathbf{x} \oplus \mathbf{\Delta}$ in a **trellis**
- 2^5 nodes per segment $(c_i, c_i', x_{i-2}, x_{i-1}, x_i)$

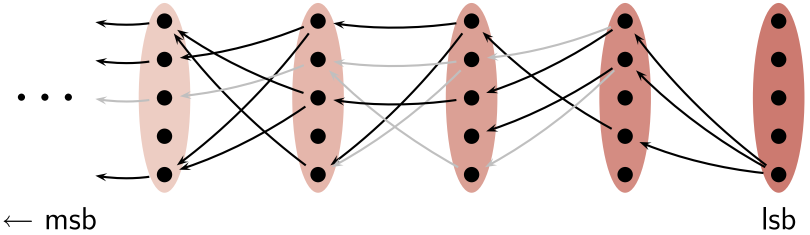


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

- Compact representation of $\mathbf{x} + (\mathbf{x} \ll 3)$ and $\mathbf{x}' + (\mathbf{x}' \ll 3)$ where $\mathbf{x}' = \mathbf{x} \oplus \mathbf{\Delta}$ in a **trellis**
- 2^5 nodes per segment $(c_i, c_i', x_{i-2}, x_{i-1}, x_i)$



- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

“Good” Differential Characteristic, pt. II

Let’s Summarise

- Low Hamming weight in Δe is good
- Can easily compute attack complexity, incl. *tricks*

A Different View: Coding Theory

- All linearised differentials are **codewords** of a linear code.

$$\mathbf{G} = \left[\ \mathbf{I}_{tw \times tw} \ \middle| \ \mathbf{E}_{tw \times tsPw} \ \middle| \ \mathbf{O}_{tw \times h} \ \right]$$

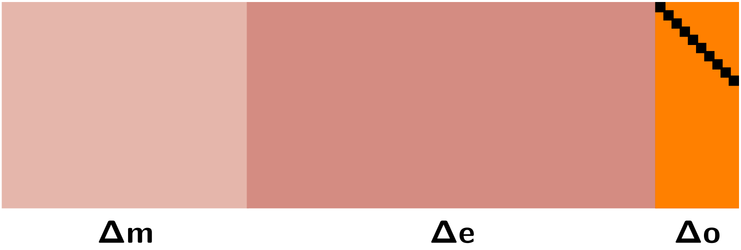
- Low weight codewords [RO05, PRR05]

“Good” Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

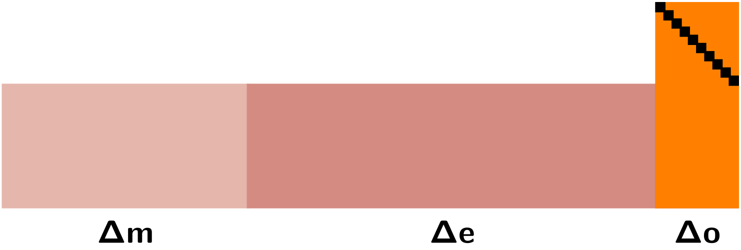
“Good” Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

G = 

"Good" Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

$\mathbf{G} =$ 

"Good" Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

G =

"Good" Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

"Good" Differential Characteristic, pt. II

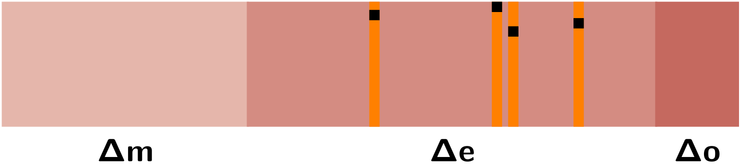
- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

"Good" Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

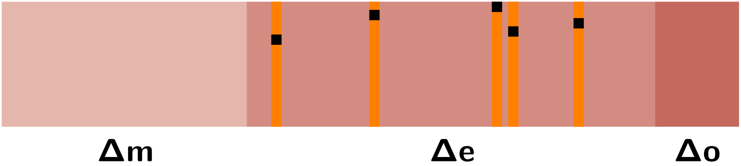
"Good" Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

$\mathbf{G} =$ 

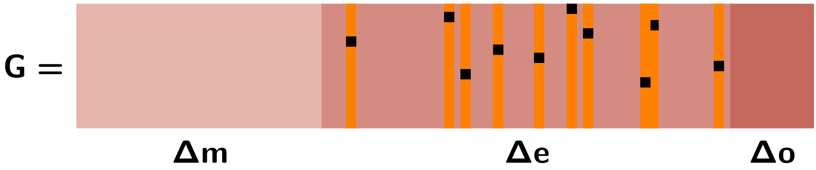
“Good” Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

$\mathbf{G} =$ 

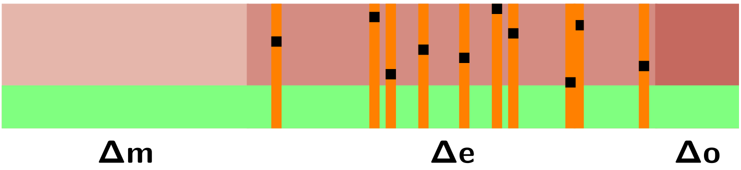
“Good” Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:



“Good” Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

G = 

"Good" Differential Characteristic, pt. II

- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

Outline

Results

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

Round	Step	Δe	$\rightarrow$	Δf	$\mathrm{DP}^{\times 9}$	totals
inject message word difference $\Delta m_{-1} = 0000000008000000_x$						
0	0	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	$\mathbf{2^{-0.00}}$
	1	0000000000000800_x	$\rightarrow$	0000000000004800_x	$\star$	
	2	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	
	3	4800000000000800_x	$\rightarrow$	0800000000004800_x	$2^{-3.70}$	
	4	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	
	5	4800280000000800_x	$\rightarrow$	0801680000004800_x	$2^{-7.28}$	
	6	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	7	0000280168000800_x	$\rightarrow$	$0001680a28004800_x$	$2^{-11.02}$	
inject message word difference $\Delta m_0 = 0000002280000000_x$						
1	0	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	0000280168000000_x	$\rightarrow$	$0001680a28000000_x$	$\star$	
	2	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	3	4800280000000000_x	$\rightarrow$	0801680000000000_x	$2^{-5.43}$	
	4	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	5	0000080000000000_x	$\rightarrow$	0000480000000000_x	$2^{-1.85}$	

Example: EnRUPT-256

inject message word difference $\Delta m_{-1} = 0000000008000000_x$						
0	0	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	$\mathbf{2^{-0.00}}$
	1	0000000000000800_x	$\rightarrow$	0000000000004800_x	$\star$	
	2	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	
	3	4800000000000800_x	$\rightarrow$	0800000000004800_x	$2^{-3.70}$	
	4	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	
	5	4800280000000800_x	$\rightarrow$	0801680000004800_x	$2^{-7.28}$	
	6	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	7	0000280168000800_x	$\rightarrow$	$0001680a28004800_x$	$2^{-11.02}$	
inject message word difference $\Delta m_0 = 0000002280000000_x$						
1	0	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	0000280168000000_x	$\rightarrow$	$0001680a28000000_x$	$\star$	
	2	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	3	4800280000000000_x	$\rightarrow$	0801680000000000_x	$2^{-5.43}$	
	4	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	5	0000080000000000_x	$\rightarrow$	0000480000000000_x	$2^{-1.85}$	
	6	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	7	4800080120000000	$\rightarrow$	0800480820000000	$2^{-6.54}$	

Example: EnRUPT-256

	1	0000000000000800$_x$	$\longrightarrow$	0000000000004800$_x$	$\star$	
	2	9000000000000000$_x$	$\longrightarrow$	1000000000000000$_x$	$2^{-0.85}$	
	3	4800000000000800$_x$	$\longrightarrow$	0800000000004800$_x$	$2^{-3.70}$	
	4	9000000000000000$_x$	$\longrightarrow$	1000000000000000$_x$	$2^{-0.85}$	
	5	4800280000000800$_x$	$\longrightarrow$	0801680000004800$_x$	$2^{-7.28}$	
	6	90000002d0000000$_x$	$\longrightarrow$	1000001450000000$_x$	$2^{-6.43}$	
	7	0000280168000800$_x$	$\longrightarrow$	0001680a28004800$_x$	$2^{-11.02}$	
inject message word difference $\Delta m_0 =$ 0000002280000000$_x$						
1	0	90000002d0000000$_x$	$\longrightarrow$	1000001450000000$_x$	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	0000280168000000$_x$	$\longrightarrow$	0001680a28000000$_x$	$\star$	
	2	90000002d0000000$_x$	$\longrightarrow$	1000001450000000$_x$	$2^{-6.43}$	
	3	4800280000000000$_x$	$\longrightarrow$	0801680000000000$_x$	$2^{-5.43}$	
	4	90000002d0000000$_x$	$\longrightarrow$	1000001450000000$_x$	$2^{-6.43}$	
	5	0000080000000000$_x$	$\longrightarrow$	0000480000000000$_x$	$2^{-1.85}$	
	6	9000000240000000$_x$	$\longrightarrow$	1000001040000000$_x$	$2^{-3.70}$	
	7	4800080120000000$_x$	$\longrightarrow$	0800480820000000$_x$	$2^{-6.54}$	
inject message word difference $\Delta m_1 =$ 0000002288000000$_x$						
2	0	9000000240000000$_x$	$\longrightarrow$	1000001040000000$_x$	$2^{-3.70}$	$\mathbf{2^{-34.08}}$

Example: EnRUPT-256

	3	4800000000000800$_x$	$\rightarrow$	0800000000004800$_x$	2	
	4	9000000000000000$_x$	$\rightarrow$	1000000000000000$_x$	$2^{-0.85}$	
	5	4800280000000800$_x$	$\rightarrow$	0801680000004800$_x$	$2^{-7.28}$	
	6	90000002d0000000$_x$	$\rightarrow$	1000001450000000$_x$	$2^{-6.43}$	
	7	0000280168000800$_x$	$\rightarrow$	0001680a28004800$_x$	$2^{-11.02}$	
inject message word difference Δm_0 = 0000002280000000$_x$						
1	0	90000002d0000000$_x$	$\rightarrow$	1000001450000000$_x$	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	0000280168000000$_x$	$\rightarrow$	0001680a28000000$_x$	$\star$	
	2	90000002d0000000$_x$	$\rightarrow$	1000001450000000$_x$	$2^{-6.43}$	
	3	4800280000000000$_x$	$\rightarrow$	0801680000000000$_x$	$2^{-5.43}$	
	4	90000002d0000000$_x$	$\rightarrow$	1000001450000000$_x$	$2^{-6.43}$	
	5	0000080000000000$_x$	$\rightarrow$	0000480000000000$_x$	$2^{-1.85}$	
	6	9000000240000000$_x$	$\rightarrow$	1000001040000000$_x$	$2^{-3.70}$	
	7	4800080120000000$_x$	$\rightarrow$	0800480820000000$_x$	$2^{-6.54}$	
inject message word difference Δm_1 = 0000002288000000$_x$						
2	0	9000000240000000$_x$	$\rightarrow$	1000001040000000$_x$	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000$_x$	$\rightarrow$	0000480208000000$_x$	$\star$	
	2	9000000240000000$_x$	$\rightarrow$	1000001040000000$_x$	$2^{-3.70}$	

Example: EnRUPT-256

	[illegible]	[illegible]	→	[illegible]	[illegible]	
	6	$90000002d0000000_x$	→	1000001450000000_x	$2^{-6.43}$	
	7	0000280168000800_x	→	$0001680a28004800_x$	$2^{-11.02}$	
inject message word difference $\Delta m_0 = 0000002280000000_x$						
1	0	$90000002d0000000_x$	→	1000001450000000_x	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	0000280168000000_x	→	$0001680a28000000_x$	⋆	
	2	$90000002d0000000_x$	→	1000001450000000_x	$2^{-6.43}$	
	3	4800280000000000_x	→	0801680000000000_x	$2^{-5.43}$	
	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	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	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	$2^{-3.70}$	

Example: EnRUPT-256

inject message word difference $\Delta m_0 = 0000002280000000_x$						
1	0	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	0000280168000000_x	$\rightarrow$	$0001680a28000000_x$	$\star$	
	2	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	3	4800280000000000_x	$\rightarrow$	0801680000000000_x	$2^{-5.43}$	
	4	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	5	0000080000000000_x	$\rightarrow$	0000480000000000_x	$2^{-1.85}$	
	6	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	7	4800080120000000_x	$\rightarrow$	0800480820000000_x	$2^{-6.54}$	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000_x	$\rightarrow$	0000480208000000_x	$\star$	
	2	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\rightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\rightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	

Example: EnRUPT-256

	1	0000280168000000_x	$\longrightarrow$	$0001680a28000000_x$	$\star$	
	2	$90000002d0000000_x$	$\longrightarrow$	1000001450000000_x	$2^{-6.43}$	
	3	4800280000000000_x	$\longrightarrow$	0801680000000000_x	$2^{-5.43}$	
	4	$90000002d0000000_x$	$\longrightarrow$	1000001450000000_x	$2^{-6.43}$	
	5	0000080000000000_x	$\longrightarrow$	0000480000000000_x	$2^{-1.85}$	
	6	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	7	4800080120000000_x	$\longrightarrow$	0800480820000000_x	$2^{-6.54}$	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$\star$	
	2	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\longrightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\longrightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\longrightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						

Example: EnRUPT-256

	3	4800280000000000_x	$\rightarrow$	0801680000000000_x	$2^{-5.43}$	
	4	$90000002d0000000_x$	$\rightarrow$	1000001450000000_x	$2^{-6.43}$	
	5	0000080000000000_x	$\rightarrow$	0000480000000000_x	$2^{-1.85}$	
	6	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	7	4800080120000000_x	$\rightarrow$	0800480820000000_x	$2^{-6.54}$	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000_x	$\rightarrow$	0000480208000000_x	$\star$	
	2	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\rightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\rightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\rightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\rightarrow$	0001680820000000_x	$\star$	

Example: EnRUPT-256

	5	0000080000000000_x	$\rightarrow$	0000480000000000_x	$2^{-1.85}$	
	6	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	7	4800080120000000_x	$\rightarrow$	0800480820000000_x	$2^{-6.54}$	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000_x	$\rightarrow$	0000480208000000_x	$\star$	
	2	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\rightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\rightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\rightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\rightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\rightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\rightarrow$	$0801680a28000000_x$	$2^{-11.02}$	

Example: EnRUPT-256

	7	4800080120000000_x	$\longrightarrow$	0800480820000000_x	$2^{-6.54}$	
inject message word difference $\Delta m_1 = 0000002288000000_x$						
2	0	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$\star$	
	2	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\longrightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\longrightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\longrightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\longrightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	[illegible]	$\longrightarrow$	[illegible]	$2^{-3.70}$	

Example: EnRUPT-256

2	0	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	$\mathbf{2^{-34.08}}$
	1	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$\star$	
	2	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\longrightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\longrightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\longrightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\longrightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference [illegible]						

Example: EnRUPT-256

	2	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	3	4800080168000000_x	$\longrightarrow$	$0800480a28000000_x$	$2^{-9.28}$	
	4	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{-3.70}$	
	5	0000200000000000_x	$\longrightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\longrightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\longrightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$\star$	

Example: EnRUPT-256

	4	9000000240000000_x	$\longrightarrow$	1000001040000000_x	$2^{[illegible]}$	
	5	0000200000000000_x	$\longrightarrow$	0001200000000000_x	$2^{-1.85}$	
	6	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	
	7	4800200000000000_x	$\longrightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\longrightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$\star$	
	2	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	3	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$2^{-3.70}$	

Example: EnRUPT-256

	6	9000000000000000_x	$\longrightarrow$	1000000000000000_x	2	
	7	4800200000000000_x	$\longrightarrow$	0801200000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_2 = 0000000208000000_x$						
3	0	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\longrightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$\star$	
	2	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	3	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$2^{-3.70}$	
	4	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	5	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	

Example: EnRUPT-256

inject message word difference Δm_2

3	0	9000000000000000_x	$\longrightarrow$	1000000000000000_x	$2^{-0.85}$	$\mathbf{2^{-23.91}}$
	1	0000280120000000_x	$\longrightarrow$	0001680820000000_x	$\star$	
	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$\star$	
	2	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	3	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$2^{-3.70}$	
	4	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	5	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	
	6	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	7	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	

Example: EnRUPT-256

	2	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	3	4800280168000000_x	$\longrightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$\star$	
	2	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	3	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$2^{-3.70}$	
	4	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	5	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	
	6	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	7	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
5	0	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	$\mathbf{2^{-20.49}}$

Example: EnRUPT-256

	4	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\longrightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\longrightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\longrightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$\star$	
	2	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	3	0000080000000800_x	$\longrightarrow$	0000480000004800_x	$2^{-3.70}$	
	4	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	5	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	
	6	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	
	7	4800080048000800_x	$\longrightarrow$	0800480208004800_x	$2^{-8.39}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
5	0	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$2^{-0.00}$	$\mathbf{2^{-20.49}}$
	1	0000000000000000_x	$\longrightarrow$	0000000000000000_x	$\star$	
	⋮	⋮	$\longrightarrow$	⋮	⋮	

Example: EnRUPT-256

	6	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\rightarrow$	0800480000000000_x	$2^{-3.70}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
4	0	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	$\mathbf{2^{-34.19}}$
	1	0000080000000800_x	$\rightarrow$	0000480000004800_x	$\star$	
	2	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	
	3	0000080000000800_x	$\rightarrow$	0000480000004800_x	$2^{-3.70}$	
	4	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	
	5	4800080048000800_x	$\rightarrow$	0800480208004800_x	$2^{-8.39}$	
	6	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	
	7	4800080048000800_x	$\rightarrow$	0800480208004800_x	$2^{-8.39}$	
inject message word difference $\Delta m_3 = 0000000200000000_x$						
5	0	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	$\mathbf{2^{-20.49}}$
	1	0000000000000000_x	$\rightarrow$	0000000000000000_x	$\star$	
	$\vdots$	$\vdots$	$\rightarrow$	$\vdots$	$\vdots$	
	7	0000000000000000_x	$\rightarrow$	0000000000000000_x	$2^{-0.00}$	$\mathbf{2^{-0.00}}$

Collision Example for EnRUPT-256

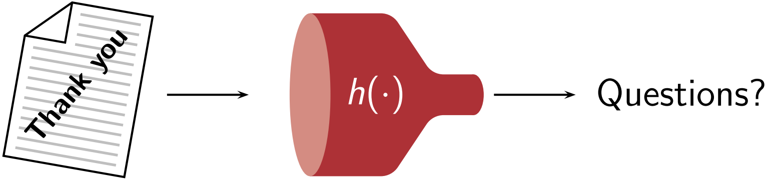
```
Example collision pair for EnRUPT-256
2008-11-06, Sebastiaan Indesteege, COSIC, Katholieke Universiteit Leuven

m1 = 13c84b456270176e04f9317ec36ce7d3e121786a347411197f64a3c940077576a14f9086fdc7334a413a769196062ca1
EnRUPT-256(m1) = bd67517ca6c0412082e03b745ffc4a64e9f092c258c398b8449afecb7fc86f72

m2 = 13c84b456a70176e04f9315c436ce7d3e1217848bc7411197f64a3cb48077576a14f9084fdc7334a413a769396062ca1
EnRUPT-256(m2) = bd67517ca6c0412082e03b745ffc4a64e9f092c258c398b8449afecb7fc86f72

m1 and m2 collide!
```

- http://homes.esat.kuleuven.be/~sindeste/enrupt.html (or see SHA-3 Zoo)

Outline

Conclusion

- Collision attacks on EnRUPT
- Breaks **all seven** proposed EnRUPT variants
- **Mitigation:** increase s-parameter to 8 [O'Neil] (i.e., double # steps per round)



References

Anne Canteaut and Florent Chabaud
A New Algorithm for Finding Minimum-Weight Words in a Linear Code: Application to McEliece's Cryptosystem and to Narrow-Sense BCH Codes of Length 511
IEEE Transactions on Information Theory, vol. 44, nr. 1, pp. 367–378, 1998.

Florent Chabaud and Antoine Joux
Differential Collisions in SHA-0
In Advances in Cryptology – CRYPTO 1998, Lecture Notes in Computer Science, vol. 1462, pp. 56–71, Springer, 1998.

Helger Lipmaa and Shiho Moriai
Efficient Algorithms for Computing Differential Properties of Addition
In Fast Software Encryption – FSE 2001, Lecture Notes in Computer Science, vol. 2355, pp. 336–350, Springer, 2002.

Sean O'Neil, Karsten Nohl and Luca Henzen
EnRUPT Hash Function Specification
Submission to the NIST SHA-3 competition, 2008. Available online at `http://www.enrupt.com/SHA3/`.

Norbert Pramstaller, Christian Rechberger and Vincent Rijmen
Exploiting Coding Theory for Collision Attacks on SHA-1
In Cryptography and Coding, 10th IMA International Conference, Lecture Notes in Computer Science, vol. 3796, pp. 78–95, Springer, 2005.

Vincent Rijmen and Elisabeth Oswald
Update on SHA-1
In Topics in Cryptology – CT-RSA 2005, Lecture Notes in Computer Science, vol. 3376, pp. 58–71, Springer, 2005.