Cryptanalysis of SHA-3 candidates

Sebastiaan Indesteege

sebastiaan.indesteege@esat.kuleuven.be

dept. ESAT/COSIC, Katholieke Universiteit Leuven

Academy Contact Forum

Coding Theory and Cryptography III

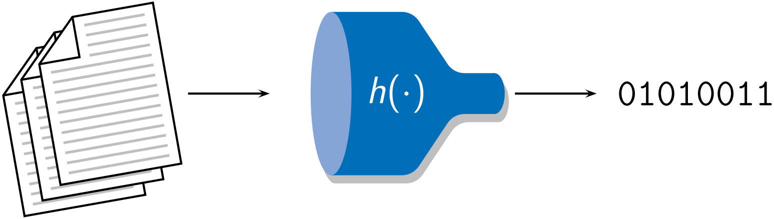
September 25, 2009

Outline

Part 1

Introduction

Cryptographic hash functions



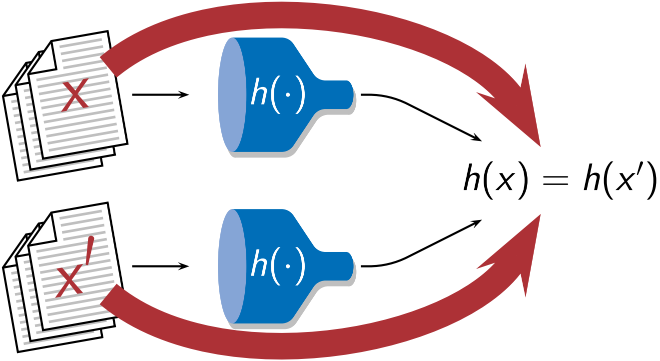
$$h : \{0,1\}^* \mapsto \{0,1\}^w$$

Desired properties

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

Security requirements

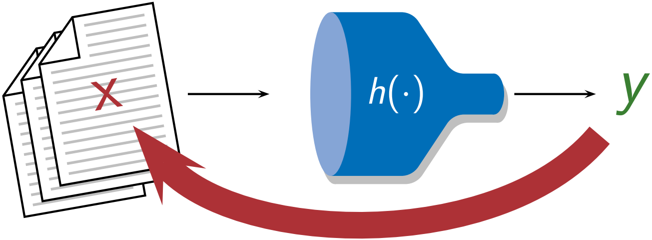
Collision resistance



- "Hard" to find $x \neq x'$ s.t. $h(x) = h(x')$.
- Birthday paradox: $2^{w/2}$

Security requirements

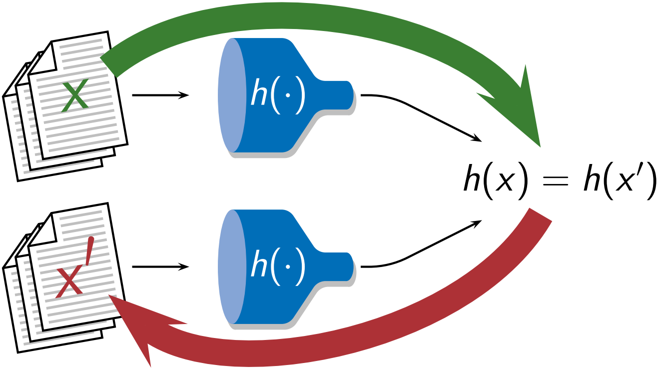
Preimage resistance



- Given y, “hard” to find x s.t. $h(x) = y$.
- Exhaustive search: 2^w

Security requirements

Second preimage resistance



- Given x, "hard" to find $x' \neq x$ s.t. $h(x) = h(x')$.
- Exhaustive search: 2^w

Applications

- integrity checking (tamper detection)
- digital signatures
- key derivation
- pseudorandomness generation
- commitment schemes
- micropayments (Lamport chains)
- anonymisation of data

- entity authentication (*e.g.* UNIX password hashing)
- data authentication (HMAC)
- ...

Applications

Example

Password hashing

- Server application needs to verify user passwords
- Don't want to store user passwords!

Example

Digital signatures

- Want to sign a **long** message
- But RSA and DSA are **too slow**

Applications

Example

Password hashing

- Server application needs to verify user passwords
- Don't want to store user passwords!
- **Solution:**
  Store the **hash value** of the password instead!

Example

Digital signatures

- Want to sign a **long** message
- But RSA and DSA are **too slow**
- **Solution:** *(simplified)*
  Sign the **hash value** of the message instead!

Applications

Example

Password hashing

- Server application needs to verify user passwords
- Don't want to store user passwords!
- **Solution:**
  Store the **hash value** of the password instead!

Example

Digital signatures

- Want to sign a **long** message
- But RSA and DSA are **too slow**
- **Solution:** *(simplified)*
  Sign the **hash value** of the message instead!

- But what if one can find collisions? (second) preimages?

Why research cryptographic hash functions?

- Popular hash functions: MD5, SHA-1, RIPEMD-160
- Wang, 2005: attacks on MD5, SHA-0, SHA-1, ...
- Suddenly lots of research attention
- Slow migration to SHA-2, but little confidence

Need new and better cryptographic hash functions!

Example

MD5 *(short overview)*

- Designed in 1991 by Rivest to replace MD4
- Used **everywhere**

Example

MD5 *(short overview)*

- Designed in 1991 by Rivest to replace MD4
- Used **everywhere**
- First signs of trouble...
  den Boer and Bosselaers (1993), Dobbertin (1996)

Example

MD5 *(short overview)*

- Designed in 1991 by Rivest to replace MD4
- Used **everywhere**
- First signs of trouble...
  den Boer and Bosselaers (1993), Dobbertin (1996)
- **Broken!** (at least in theory)
  Wang 2004, publ. 2005

Example

MD5 *(short overview)*

- Designed in 1991 by Rivest to replace MD4
- Used **everywhere**
- First signs of trouble...
  den Boer and Bosselaers (1993), Dobbertin (1996)
- **Broken!** (at least in theory)
  Wang 2004, publ. 2005
- Real breaks due to MD5!
  Sotirov, Stevens et al., December 2008
  "Creating a rogue CA certificate"
  `http://www.phreedom.org/md5`

Example

MD5 *(short overview)*

- Designed in 1991 by Rivest to replace MD4
- Used **everywhere**
- First signs of trouble...
  den Boer and Bosselaers (1993), Dobbertin (1996)
- **Broken!** (at least in theory)
  Wang 2004, publ. 2005
- Real breaks due to MD5!
  Sotirov, Stevens et al., December 2008
  "Creating a rogue CA certificate"
  `http://www.phreedom.org/md5`

- But MD5 is **still** used...

NIST SHA-3 competition

- International competition aiming to develop a new cryptographic hash function standard
- Cf. AES competition (1997–2001)
- 2007–2012 (?)
- Submission deadline was 31 October 2008
- "First SHA-3 Conference," Leuven, 25–28 February 2009
- 51 candidates in first round

SHA-3 competition round 2 candidates

BLAKE	Jean-Philippe Aumasson
Blue Midnight Wish	Svein Johan Knapskog
CubeHash	Daniel J. Bernstein
ECHO	Henri Gilbert
Fugue	Charanjit S. Jutla
Grøstl	Lars R. Knudsen
Hamsi	Özgül Küçük
JH	Hongjun Wu
Keccak	The Keccak Team
Luffa	Dai Watanabe
Shabal	Jean-François Misarsky
SHAvite-3	Orr Dunkelman
SIMD	Gaëtan Leurent
Skein	Bruce Schneier

(announced on July 24, 2009)

Cryptanalysis of hash functions

- How to select a **good** new hash function standard?

Cryptanalysis of hash functions

- How to select a **good** new hash function standard?

Thorough cryptanalysis of all candidates

...and hope that NIST makes a good choice based on the results...

This talk

- Successful cryptanalysis of two round-1 candidates: EnRUPT and SHAMATA

Sebastiaan Indesteege, and Bart Preneel
Practical Collisions for EnRUPT
In Fast Software Encryption, FSE 2009

Sebastiaan Indesteege, Florian Mendel, Martin Schläffer, and Bart Preneel
Practical Collisions for SHAMATA-256
In Selected Areas in Cryptography, SAC 2009

Part 2

EnRUPT

EnRUPT

EnRUPT

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

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/.

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**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    $\mathbf{x}_\gamma \leftarrow \mathbf{x}_\gamma \oplus \mathbf{f}$

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

  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**

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

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

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

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

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

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

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

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

  end for

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

  $r \leftarrow r + s \cdot P$

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

end function

Attacking EnRUPT

Observation

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

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 $t \cdot w$

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

- Differentials?

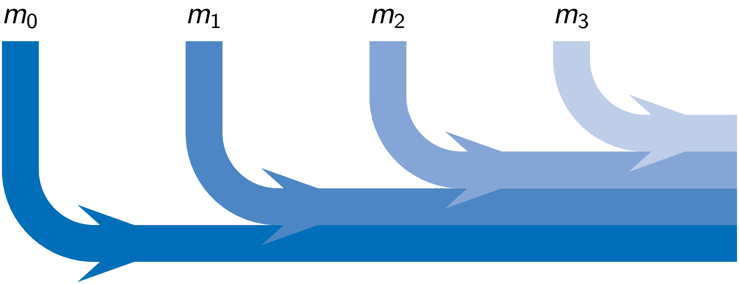
$$[\Delta o]_{1\times h} = [\Delta m]_{1\times tw} \cdot [\mathbf{O}]_{tw\times h}$$

"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	[illegible]	$\rightarrow$	[illegible]

Finding a Conforming Pair

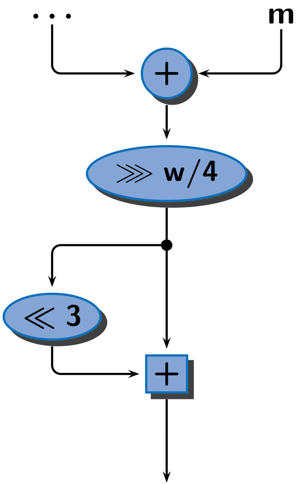


Observation

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

Finding a Conforming Pair

Finding it Faster

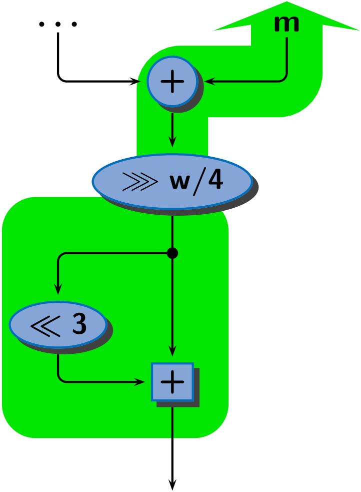


Message modification

- 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 $\mathrm{DP}^{\times 9}$:

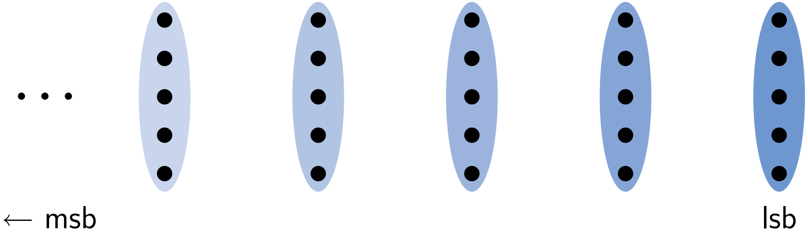
$$\mathrm{DP}^{\times 9}(\Delta) \approx 2^{-\,\mathrm{wt}\left(\left(\Delta \vee (\Delta \lll 3)\right) \wedge \mathrm{bin}\, 01\cdots 1000\right)}$$

(after simplification)

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 $(c_i, c'_i, x_{i-2}, x_{i-1}, x_i)$

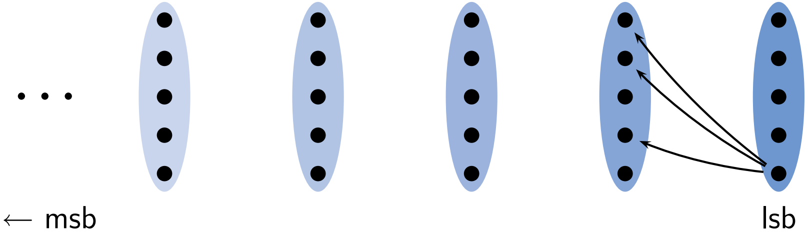


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

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

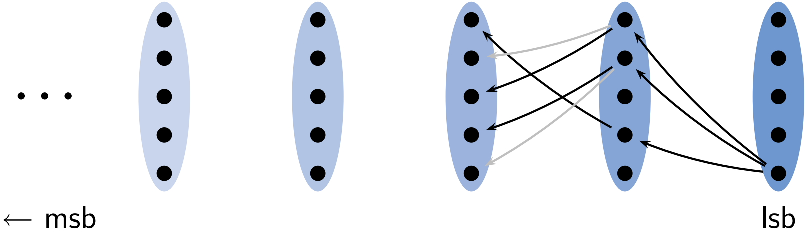


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

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

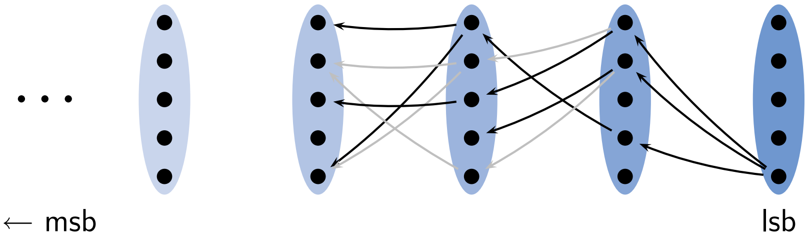


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

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

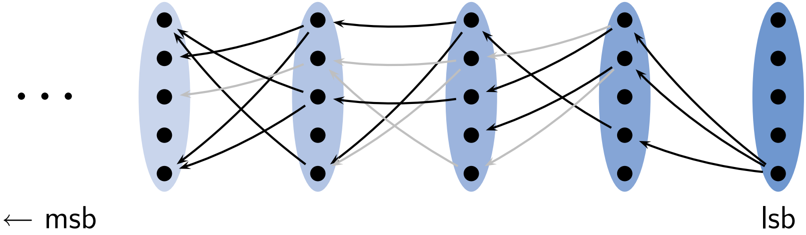


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

Finding a Conforming Pair

Round Complexities?

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

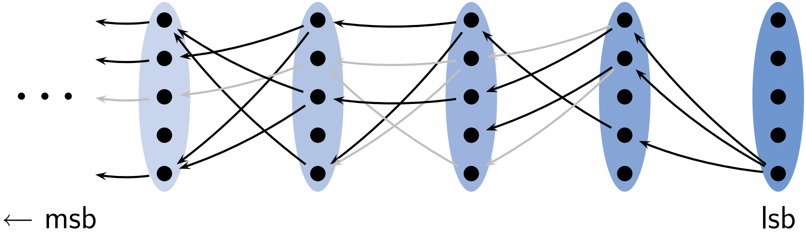


- Can quickly count paths, and thus compute $\mathbf{DP}^{\times 9}$ **exactly** using the Viterbi algorithm (modified)

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

Summary

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

"Good" Differential Characteristic, pt. II

Summary

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

A different view: coding theory

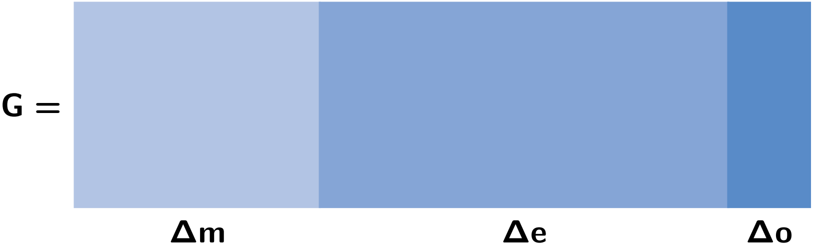
- All linearised differentials are **codewords** of a linear code.

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

- Low weight codewords [RO05, PRR05]

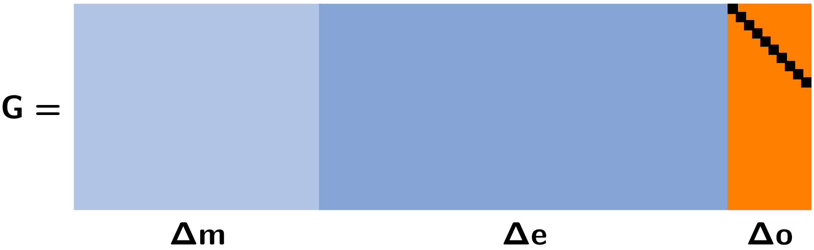
"Good" Differential Characteristic, pt. II

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



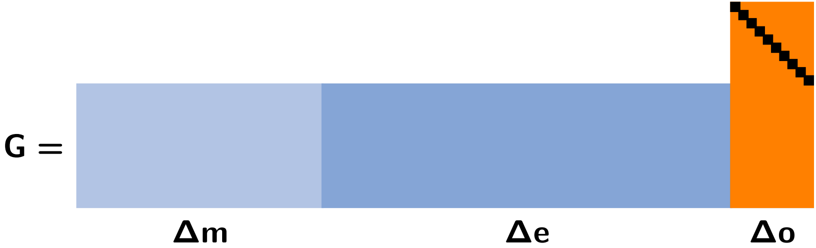
"Good" Differential Characteristic, pt. II

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



"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:

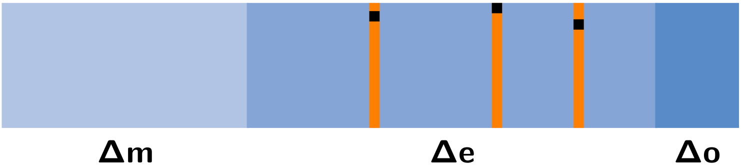
"Good" Differential Characteristic, pt. II

- 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

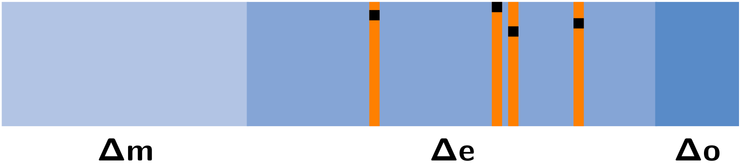
- But low weight is just a **heuristic**
- Use the **actual attack complexity** in an algorithm for finding low weight codewords (similar to [CC98])
- Simplified:

G =



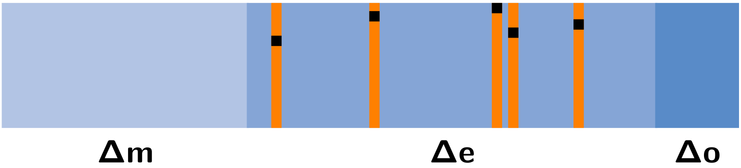
"Good" Differential Characteristic, pt. II

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

G = 

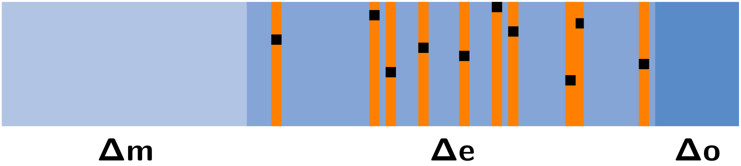
"Good" Differential Characteristic, pt. II

- 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 = 

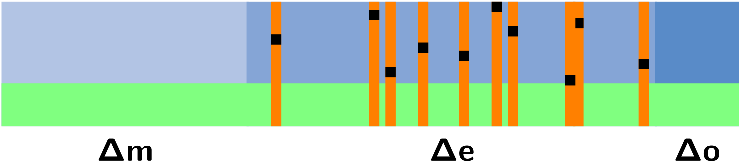
"Good" Differential Characteristic, pt. II

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

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:

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 $\Delta m_{-1} = \mathtt{0000000008000000}_x$						
0	0	$\mathtt{0000000000000000}_x$	$\rightarrow$	$\mathtt{0000000000000000}_x$	$2^{-0.00}$	$\mathbf{2^{-0.00}}$
	1	$\mathtt{0000000000000800}_x$	$\rightarrow$	$\mathtt{0000000000004800}_x$	$\star$	
	2	$\mathtt{9000000000000000}_x$	$\rightarrow$	$\mathtt{1000000000000000}_x$	$2^{-0.85}$	
	3	$\mathtt{4800000000000800}_x$	$\rightarrow$	$\mathtt{0800000000004800}_x$	$2^{-3.70}$	
	4	$\mathtt{9000000000000000}_x$	$\rightarrow$	$\mathtt{1000000000000000}_x$	$2^{-0.85}$	
	5	$\mathtt{4800280000000800}_x$	$\rightarrow$	$\mathtt{0801680000004800}_x$	$2^{-7.28}$	
	6	$\mathtt{90000002d0000000}_x$	$\rightarrow$	$\mathtt{1000001450000000}_x$	$2^{-6.43}$	
	7	$\mathtt{0000280168000800}_x$	$\rightarrow$	$\mathtt{0001680a28004800}_x$	$2^{-11.02}$	
inject message word difference $\Delta m_0 = \mathtt{0000002280000000}_x$						
1	0	$\mathtt{90000002d0000000}_x$	$\rightarrow$	$\mathtt{1000001450000000}_x$	$2^{-6.43}$	$\mathbf{2^{-36.56}}$
	1	$\mathtt{0000280168000000}_x$	$\rightarrow$	$\mathtt{0001680a28000000}_x$	$\star$	
	2	$\mathtt{90000002d0000000}_x$	$\rightarrow$	$\mathtt{1000001450000000}_x$	$2^{-6.43}$	
	3	$\mathtt{4800280000000000}_x$	$\rightarrow$	$\mathtt{0801680000000000}_x$	$2^{-5.43}$	
	4	$\mathtt{90000002d0000000}_x$	$\rightarrow$	$\mathtt{1000001450000000}_x$	$2^{-6.43}$	
	5	$\mathtt{0000028000000000}$		$\mathtt{0000042800000000}$	$2^{-1.85}$	

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	$2^{-3.70}$	

Example: EnRUPT-256

	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_x	$\rightarrow$	0800480820000000_x	$2^{-6.54}$	
inject message word difference $\Delta m_1 = 0000002288000000_x$						

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 $\Delta m_0 = 0000002280000000_x$						
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				$2^{-3.70}$	

Example: EnRUPT-256

	[illegible]	[illegible]		[illegible]	[illegible]	
	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_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	[illegible]		[illegible]	$2^{-3.70}$	

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	[illegible]	$\rightarrow$	[illegible]	$2^{-0.85}$	

Example: EnRUPT-256

	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	$2^{-0.85}$	
	7	4800200000000000_x	$\rightarrow$	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	$\rightarrow$	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	$\rightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\rightarrow$	0000480208000000_x	$2^{-4.70}$	

Example: EnRUPT-256

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	$\rightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\rightarrow$	0000480208000000_x	$2^{-4.70}$	
	6	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	7	4800080000000000_x	$\rightarrow$	0800480000000000_x	$2^{-3.70}$	

Example: EnRUPT-256

	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	$\rightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\rightarrow$	0000480208000000_x	$2^{-4.70}$	
	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	$2^{-3.70}$	$\mathbf{2^{-34.19}}$

Example: EnRUPT-256

	4	9000000240000000_x	$\rightarrow$	1000001040000000_x	$2^{-[illegible]}$	
	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	$\rightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\rightarrow$	0000480208000000_x	$2^{-4.70}$	
	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	$2^{-0.00}$	

Example: EnRUPT-256

	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	$\rightarrow$	$0801680a28000000_x$	$2^{-11.02}$	
	4	9000000090000000_x	$\rightarrow$	1000000410000000_x	$2^{-3.70}$	
	5	0000080048000000_x	$\rightarrow$	0000480208000000_x	$2^{-4.70}$	
	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	$2^{-0.00}$	

Example: EnRUPT-256

inject message word difference $\Delta m_2 = 0000000200000000_x$						
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	$2^{-8.39}$	
	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	$\star$	
	⋮	⋮		⋮	⋮	

Example: EnRUPT-256

	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	$\star$	
	$\vdots$	$\vdots$	$\longrightarrow$	$\vdots$	$\vdots$	
	7	0000000000000000_x	$\longrightarrow$	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

Conclusion

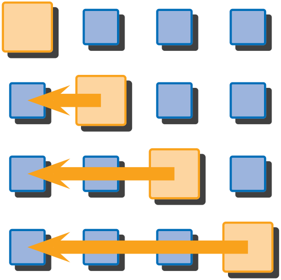
- Collision attacks on EnRUPT
- Breaks **all seven** proposed EnRUPT variants
- **Mitigation:**
  - Increase s-parameter to 8 [O'Neil]
    (i.e., double # steps per round)

Part 3

SHAMATA

Preliminaries

AES round operations: ShiftRows

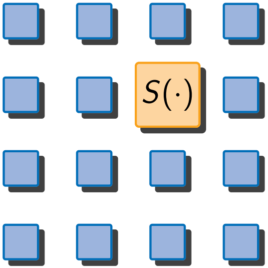


ShiftRows

- Circularly shift rows over 0, 1, 2 resp. 3 byte positions to the left

Preliminaries

AES round operations: SubBytes

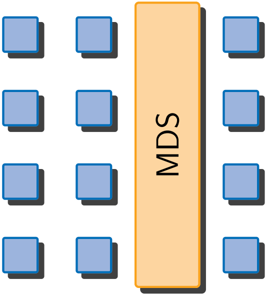


SubBytes

- Apply an 8×8 S-box to each state byte

Preliminaries

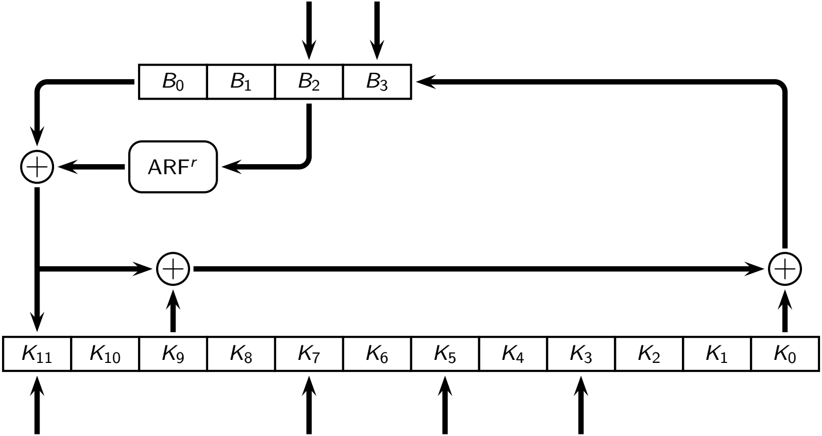
AES round operations: MixColumns



MixColumns

- Multiply each column with 4×4 MDS matrix over $GF(2^8)$

SHAMATA

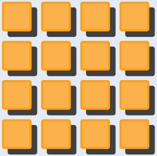


O. Kara, C. Manap, A. Atalay, F. Karakoç
SHAMATA, a candidate hash algorithm for SHA-3

Basic attack idea

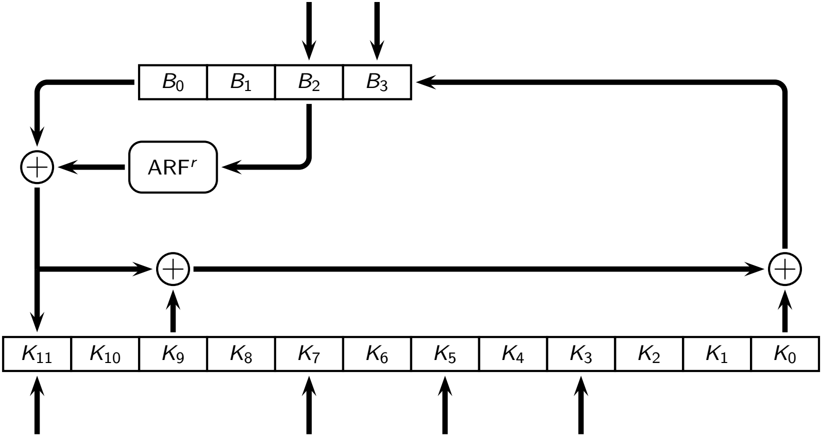
Consider the difference $\Delta = \texttt{0xffff} \cdots \texttt{ffff}$

- ✓ Matrix transposition
- ✓ Column swap
- ✓ ShiftRows
- ✓ MixColumns
- ✓ XOR
- SubBytes

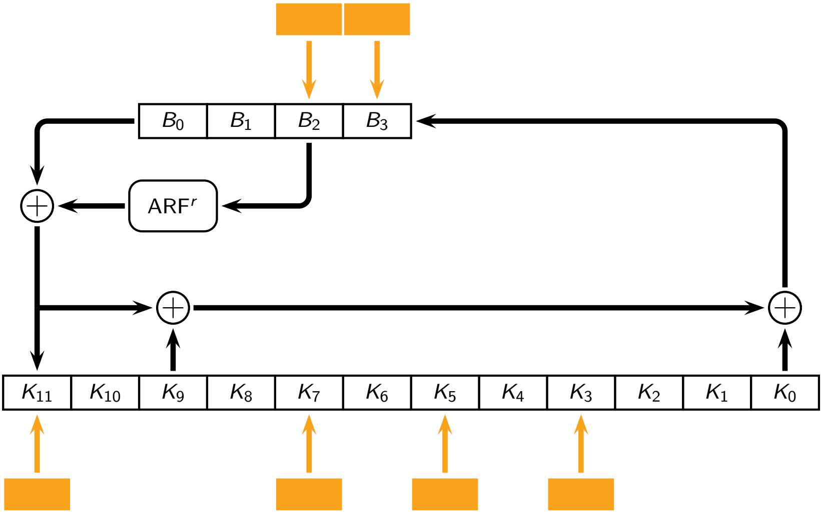


Assume it also passes through SubBytes (for now)

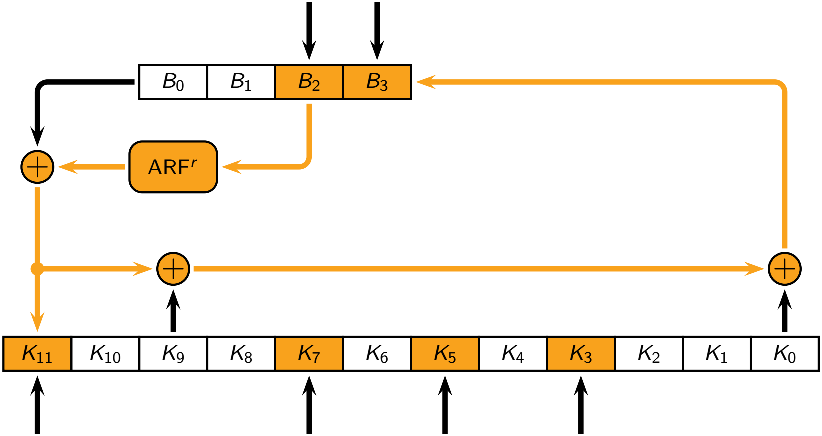
A collision differential path



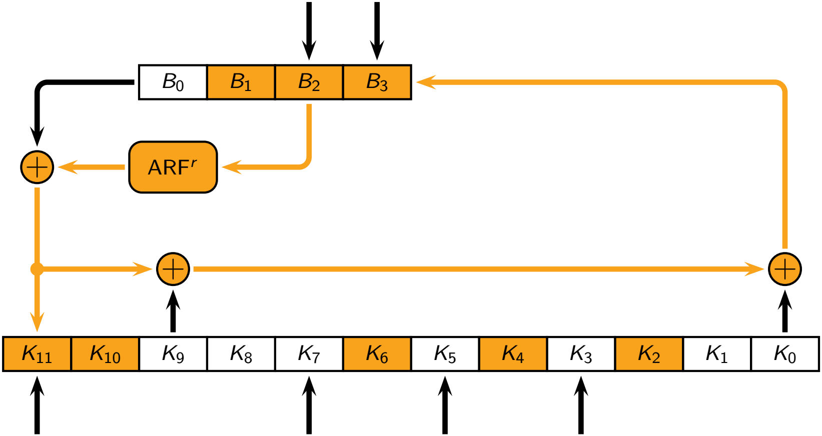
A collision differential path



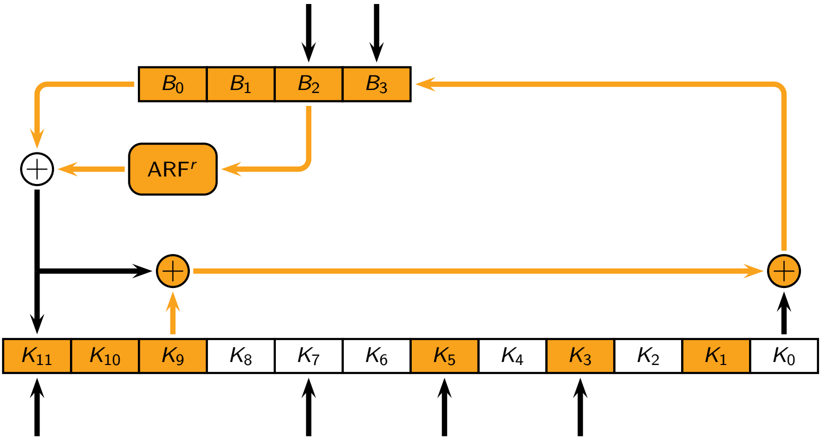
A collision differential path



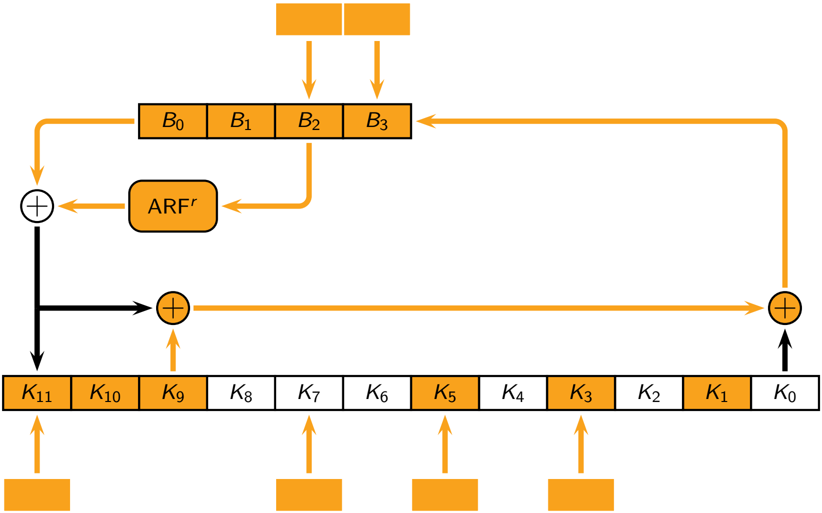
A collision differential path



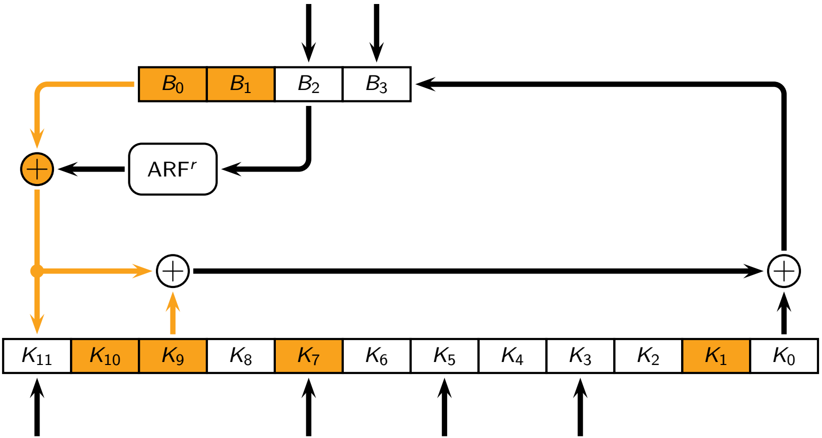
A collision differential path



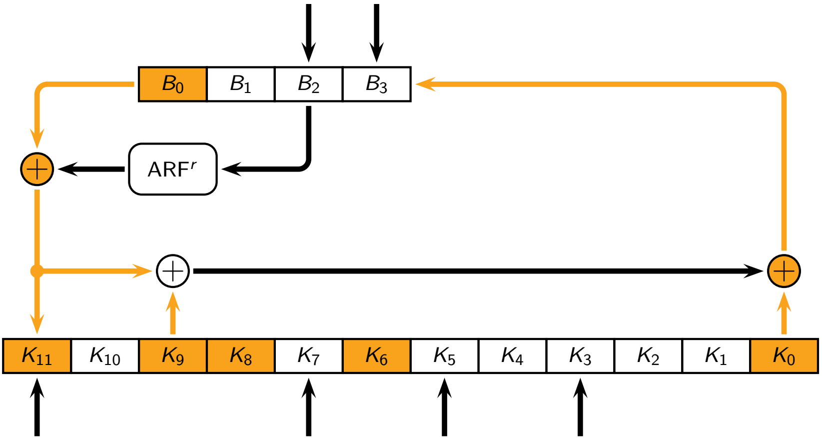
A collision differential path



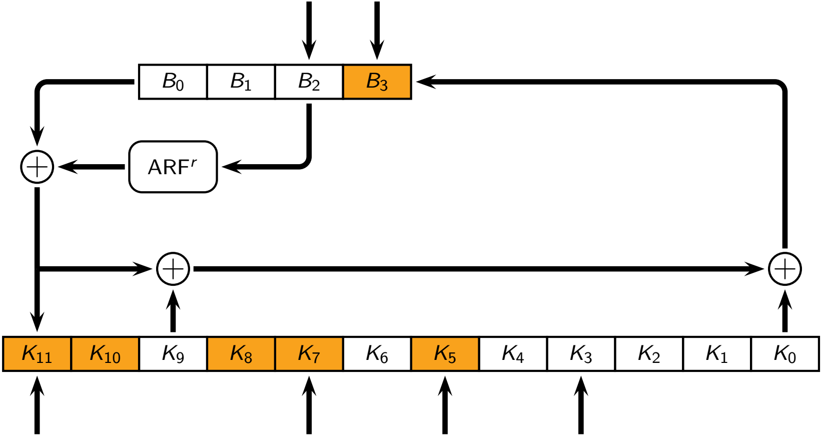
A collision differential path



A collision differential path



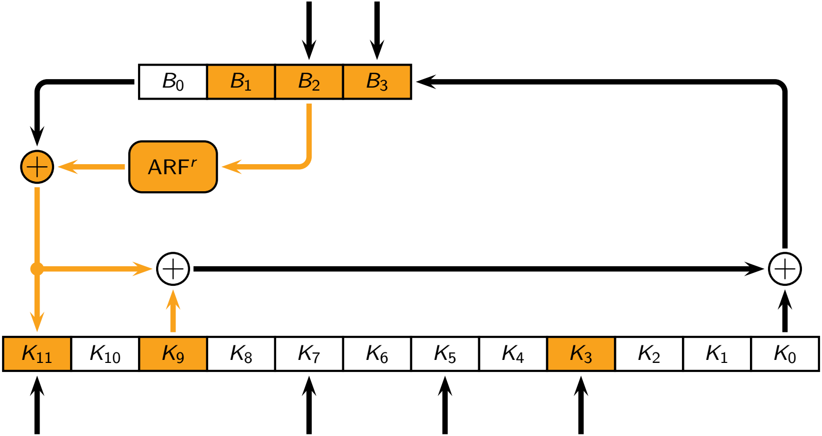
A collision differential path



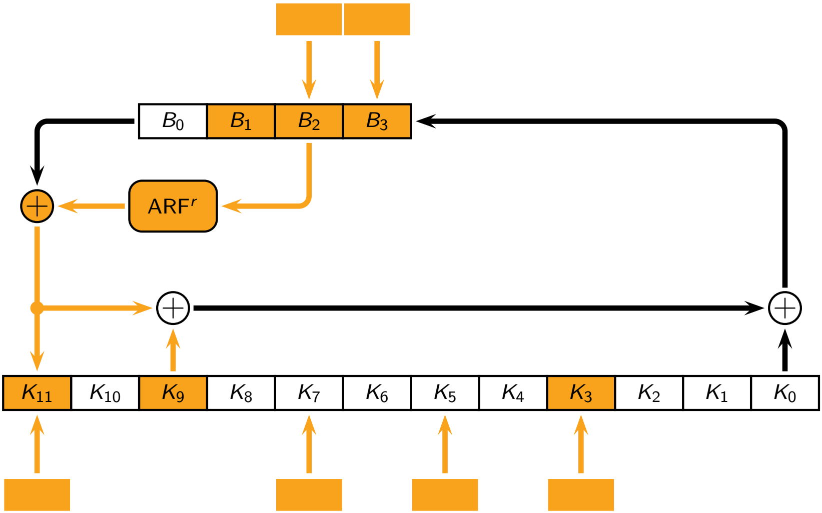
A collision differential path

Fast Forward

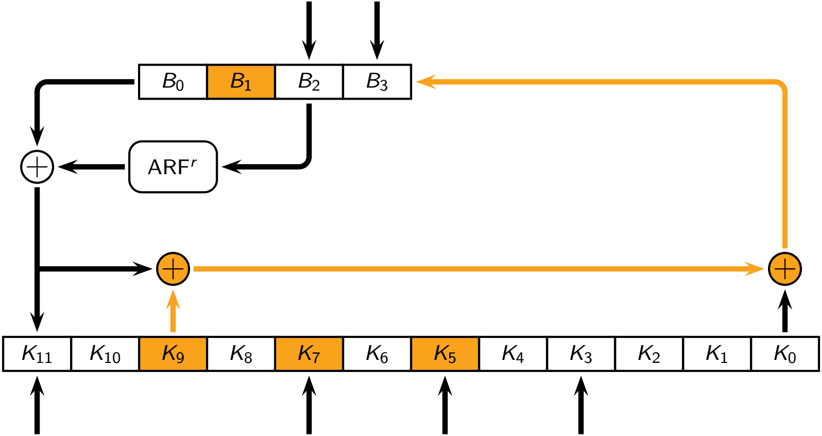
A collision differential path



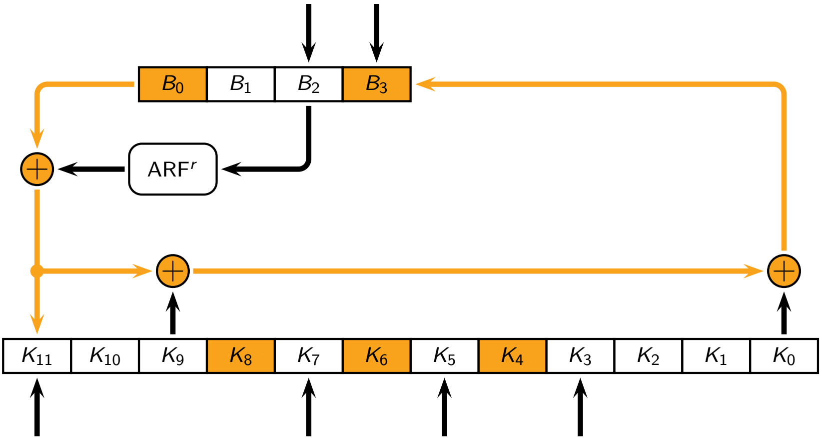
A collision differential path



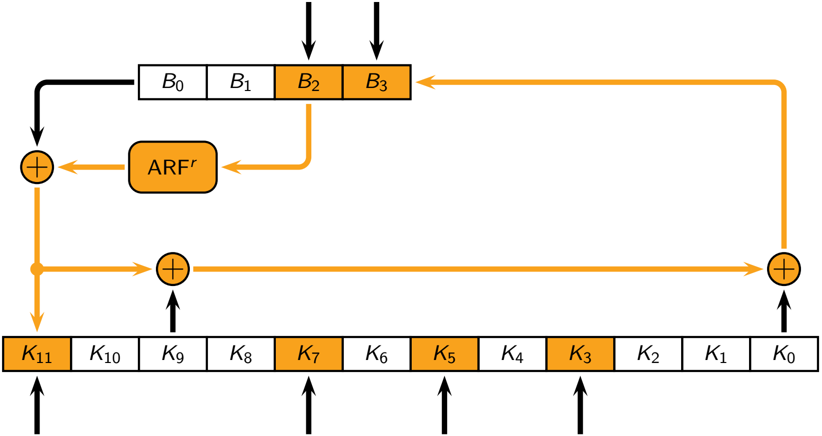
A collision differential path



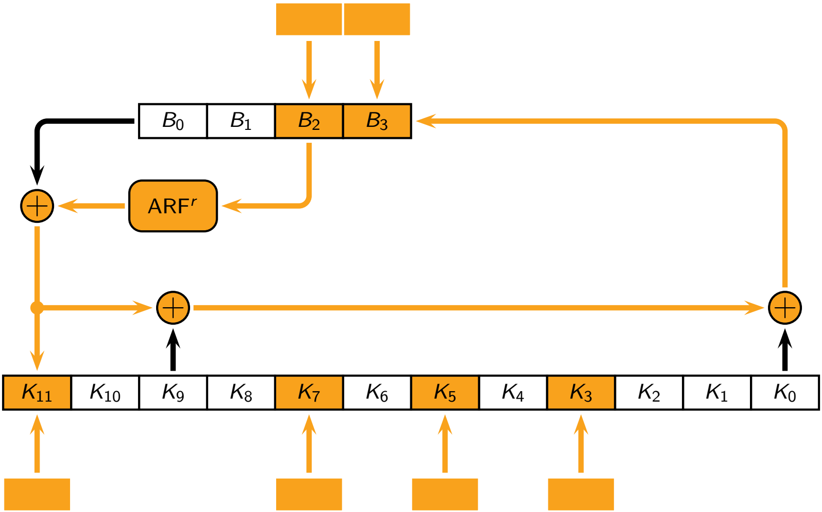
A collision differential path



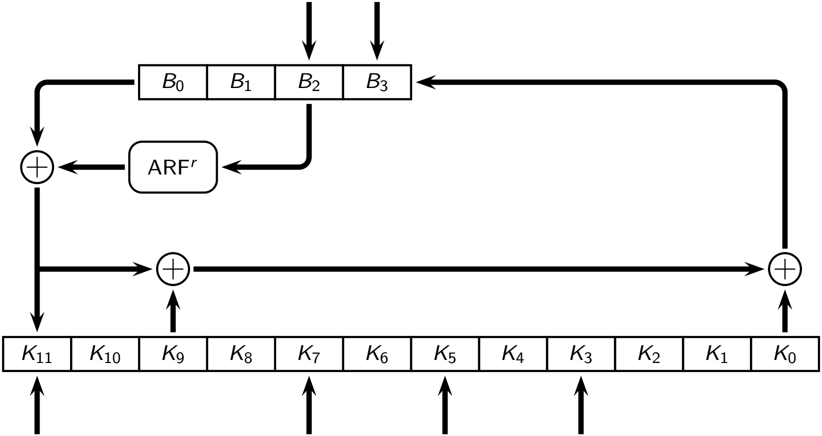
A collision differential path



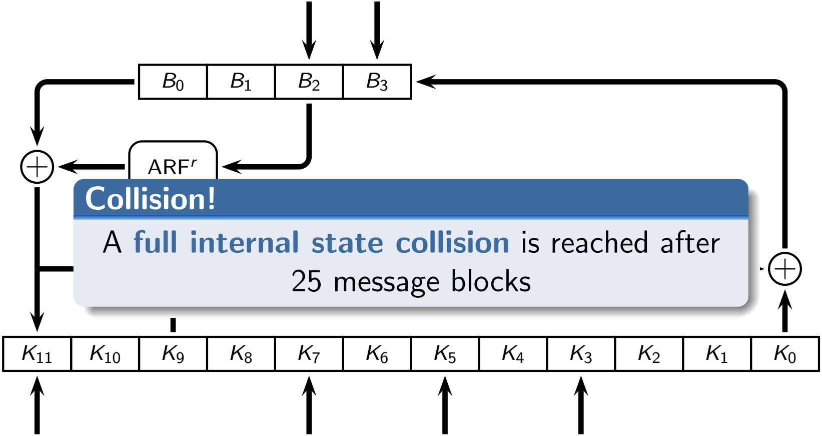
A collision differential path



A collision differential path



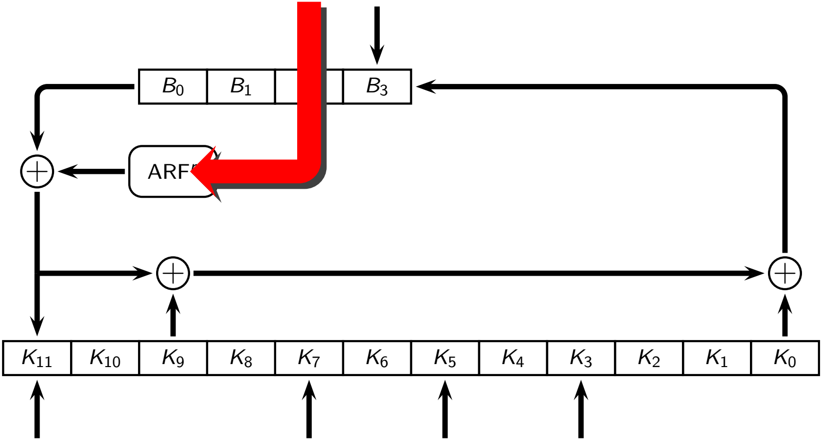
A collision differential path



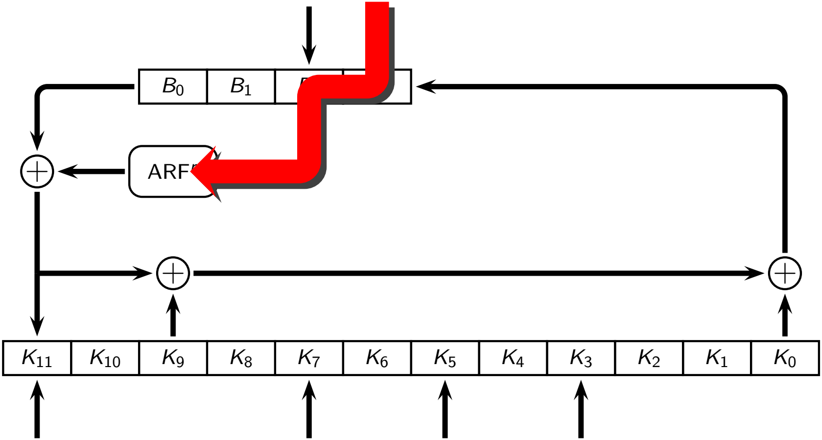
Collision!

A **full internal state collision** is reached after 25 message blocks

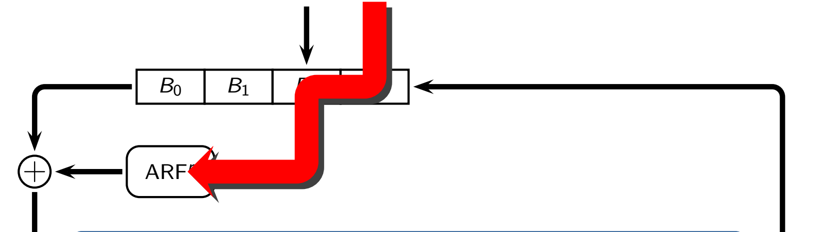
Taming the S-Boxes



Taming the S-Boxes



Taming the S-Boxes



Message Modification

- Direct control over S-box inputs
- Desired S-box behaviour for $\langle$**0x7e, 0x81**$\rangle$*
- Can fix either clock, but **not both**!
- **Our differential:** OK, except for first block!

*SHAMATA-256

A collision differential path, part II

Finding a good differential path

- 128 bit block $\longrightarrow$ **1 bit**
- Everything behaves **linearly**, or is assumed to do so
- So we find a **linear code**

A collision differential path, part II

Finding a good differential path

- 128 bit block → **1 bit**
- Everything behaves **linearly**, or is assumed to do so
- So we find a **linear code**
- Only 1 active *ARF* per round
- Heuristic: **low weight** of (parts of) codewords

A collision differential path, part II

Finding a good differential path

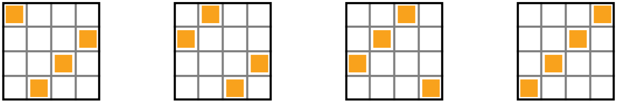
- 128 bit block $\rightarrow$ **1 bit**
- Everything behaves **linearly**, or is assumed to do so
- So we find a **linear code**
- Only 1 active *ARF* per round
- Heuristic: **low weight** of (parts of) codewords

(. . . but in this case exhaustive search also works.)

A problem in the first block...

Problem: Not enough freedom in first block
Solution: Find a suitable prefix block

$$\begin{cases} M_{i-1} & = & MC^{-1}\left(D_1 \oplus SB^{-1}\left(C_1 \oplus SR^{-1}\left(M_i\right)\right)\right) \\ {M_{i-1}}^{\mathrm{T}} & = & MC^{-1}\left(D_2 \oplus SB^{-1}\left(C_2 \oplus SR^{-1}\left({M_i}^{\mathrm{T}}\right)\right)\right) \end{cases}$$



(a) (b) (c) (d)

A problem in the first block. . .

SHAMATA-256

- **Trick:** Guess-and-determine & meet-in-the-middle
- 2^{40} time, 2^{24} memory
- Practice: 256×5 min., 700 MB memory

SHAMATA-512

- Same differential can be used
- 2 AES rounds, so trick fails ☹
- Brute force still works ☺
- 2^{128} time

Collision example for SHAMATA-256

```
Example collision pair for SHAMATA-256
Florian Mendel, Martin Schlaeffer, Christian Rechberger (IAIK, T.U.Graz),
Sebastiaan Indesteege (COSIC, K.U.Leuven)

m1 =
00000000: 10 37 fd e7 65 30 1c c0 e3 61 6e 41 24 6f cb b9 |.7..e0...anA$o..|
00000010: 7f 28 81 17 81 4a d1 3f bf 4e ca da 92 f5 35 d0 |.(...J.?.N....5.|
00000020: f0 f0 dc 19 73 d5 a7 07 8c 0b bc 3d b6 85 46 57 |....s......=..FW|
00000030: 02 92 d1 24 00 df 40 67 ca 2c fa 5b 9d 70 2c ce |...$..@g.,.[.p,.|
00000040: de 38 51 f5 01 3c 3b aa d8 ba 38 0e a1 40 b1 91 |.8Q..<;...8..@..|
00000050: 7b 18 18 24 cc d9 76 c0 f7 4a 61 28 86 06 30 8e |{..$..v..Ja(..0.|
00000060: 30 8d ab a3 62 52 aa ee 5d 66 2b 13 ec 71 6b ca |0...bR..]f+..qk.|
00000070: e3 29 f2 2c b3 ed 3d 7e f7 f2 fd 0b 1e c7 d6 e5 |.).,..=~........|
00000080: aa bc bf ab f9 fb 56 d1 b5 8e df 57 ce 90 e8 fe |......V....W....|
00000090: 1e 93 a2 80 e6 4c 6f 43 b3 9a 57 9f 0c c2 69 b6 |.....LoC..W...i.|
000000a0: 7e 29 61 77 24 b7 48 d9 45 27 30 13 b8 19 12 d6 |~)aw$.H.E'0.....|
000000b0: ac b4 56 92 00 c5 d6 b3 60 2d 52 6c ef bc 22 6d |..V.....`-Rl.."m|
000000c0: e5 83 e5 09 3b 2d e2 80 55 13 94 0d 2c a6 e3 d8 |....;-..U...,...|
000000d0: 53 e9 01 66 72 ae 8d cf 68 25 8a b6 ae 64 e7 c1 |S..fr...h%...d..|
000000e0: 5a 39 6b 5a ff 41 0e 5f 6e 60 cb 5d 1c ed ca 01 |Z9kZ.A._n`.]....|
000000f0: 70 af 0a ab dd ed 2c 32 00 c0 3f 2c 66 22 04 c0 |p.....,2..?,f"..|
00000100: 3b 97 65 9d 01 64 98 7b e6 63 d4 d6 4b 77 00 bb |;.e..d.{.c..Kw..|
00000110: bb ac 35 e3 27 66 55 34 0c 0f db d7 2f 16 19 ae |..5.'fU4..../...|
00000120: 5b 6f 1a 5a b0 28 b9 1e 89 84 7b a5 71 46 a7 e2 |[o.Z.(....{.qF..|
00000130: f5 b1 8d d2 9e b9 04 9e 79 43 ca df 65 cf 9f c1 |........yC..e...|
00000140: bb f6 43 f9 cd 88 af 13 ea 2f 93 e8 cd 39 8c a0 |..C....../...9..|
00000150: 3e ba 1b ef e2 d5 0d 6b 59 89 11 cb cf b8 ad c4 |>......kY.......|
00000160: 1a 3f 2f 9d a3 1d 82 3c e0 75 9d 83 b2 ac 3c bf |.?/....<.u....<.|
00000170: e0 27 0c c5 af b0 be a9 94 1e de 9d 50 69 10 cb |.'..........Pi..|
00000180: 69 3a 97 08 f4 9b a6 6d df 71 4d 44 40 ec 05 7e |i:.....m.qMD@..~|
00000190: a6 21 6d 89 f6 7b f4 4f 04 05 1a d3 bd c7 97 27 |.!m..{.O.......'|

SHAMATA-256(m1) =
00000000: 6e a3 b1 a1 29 75 8d 3f f5 60 f8 1b 6b 11 02 9a |n...)u.?.`..k...|
00000010: 14 b9 b2 d9 b3 2a b6 02 2a f5 83 ab e3 4c 1a 2a |.....*..*....L.*|
```

```
m2 =
00000000: 10 37 fd e7 65 30 1c c0 e3 61 6e 41 24 6f cb b9 |.7..e0...anA$o..|
00000010: 80 d7 7e e8 7e b5 2e c0 40 b1 35 25 6d 0a ca 2f |..~.~...@.5%m../|
00000020: 0f 0f 23 e6 8c 2a 58 f8 73 f4 43 c2 49 7a b9 a8 |..#..*X.s.C.Iz..|
00000030: fd 6d 2e db ff 20 bf 98 35 d3 05 a4 62 8f d3 31 |.m... ..5...b..1|
00000040: 21 c7 ae 0a fe c3 c4 55 27 45 c7 f1 5e bf 4e 6e |!......U'E..^.Nn|
00000050: 7b 18 18 24 cc d9 76 c0 f7 4a 61 28 86 06 30 8e |{..$..v..Ja(..0.|
00000060: 30 8d ab a3 62 52 aa ee 5d 66 2b 13 ec 71 6b ca |0...bR..]f+..qk.|
00000070: 1c d6 0d d3 4c 12 c2 81 08 0d 02 f4 e1 38 29 1a |....L.......8).|
00000080: 55 43 40 54 06 04 a9 2e 4a 71 20 a8 31 6f 17 01 |UC@T....Jq .1o..|
00000090: 1e 93 a2 80 e6 4c 6f 43 b3 9a 57 9f 0c c2 69 b6 |.....LoC..W...i.|
000000a0: 81 d6 9e 88 db 48 b7 26 ba d8 cf ec 47 e6 ed 29 |.....H.&....G..)|
000000b0: ac b4 56 92 00 c5 d6 b3 60 2d 52 6c ef bc 22 6d |..V.....`-Rl.."m|
000000c0: e5 83 e5 09 3b 2d e2 80 55 13 94 0d 2c a6 e3 d8 |....;-..U...,...|
000000d0: ac 16 fe 99 8d 51 72 30 97 da 75 49 51 9b 18 3e |.....Qr0..uIQ..>|
000000e0: 5a 39 6b 5a ff 41 0e 5f 6e 60 cb 5d 1c ed ca 01 |Z9kZ.A._n`.]....|
000000f0: 8f 50 f5 54 22 12 d3 cd ff 3f c0 d3 99 dd fb 3f |.P.T"....?.....?|
00000100: 3b 97 65 9d 01 64 98 7b e6 63 d4 d6 4b 77 00 bb |;.e..d.{.c..Kw..|
00000110: 44 53 ca 1c d8 99 aa cb f3 f0 24 28 d0 e9 e6 51 |DS........$(...Q|
00000120: a4 90 e5 a5 4f d7 46 e1 76 7b 84 5a 8e b9 58 1d |....O.F.v{.Z..X.|
00000130: 0a 4e 72 2d 61 46 fb 61 86 bc 35 20 9a 30 60 3e |.Nr-aF.a..5 .0`>|
00000140: bb f6 43 f9 cd 88 af 13 ea 2f 93 e8 cd 39 8c a0 |..C....../...9..|
00000150: 3e ba 1b ef e2 d5 0d 6b 59 89 11 cb cf b8 ad c4 |>......kY.......|
00000160: 1a 3f 2f 9d a3 1d 82 3c e0 75 9d 83 b2 ac 3c bf |.?/....<.u....<.|
00000170: e0 27 0c c5 af b0 be a9 94 1e de 9d 50 69 10 cb |.'..........Pi..|
00000180: 69 3a 97 08 f4 9b a6 6d df 71 4d 44 40 ec 05 7e |i:.....m.qMD@..~|
00000190: 59 de 92 76 09 84 0b b0 fb fa e5 2c 42 38 68 d8 |Y..v.......,B8h.|

SHAMATA-256(m2) =
00000000: 6e a3 b1 a1 29 75 8d 3f f5 60 f8 1b 6b 11 02 9a |n...)u.?.`..k...|
00000010: 14 b9 b2 d9 b3 2a b6 02 2a f5 83 ab e3 4c 1a 2a |.....*..*....L.*|

m1 and m2 collide!
```

- http://homes.esat.kuleuven.be/~sindeste/shamata.html

Conclusion

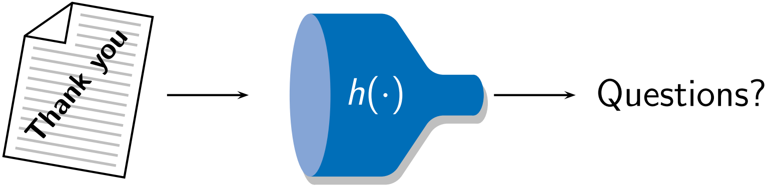
- Collision attack on SHAMATA
- Practical collisions for SHAMATA-256
- **Mitigation:**
  - More clocks per message block
  - More AES rounds + round constants
  - ...

Part 4

Conclusion

Conclusion

Thank you for your attention!



sebastiaan.indesteege@esat.kuleuven.be

References I

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.

Sebastiaan Indesteege, Florian Mendel, Martin Schläffer, and Bart Preneel
Practical Collisions for SHAMATA-256
In Selected Areas in Cryptography, SAC 2009

Sebastiaan Indesteege, and Bart Preneel
Practical Collisions for EnRUPT
In Fast Software Encryption, FSE 2009

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/`.

References II

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.