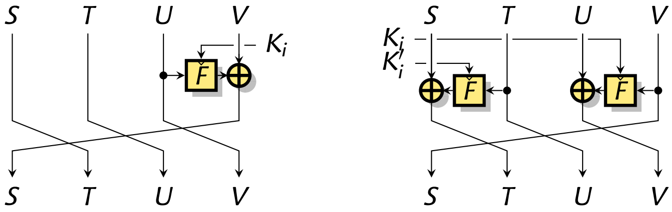
Attacks on Hash Functions based on Generalized Feistel Application to Lesamnta and SHAvite-3_{512}

Charles Bouillaguet, Orr Dunkelman,
Pierre-Alain Fouque, Gaëtan Leurent

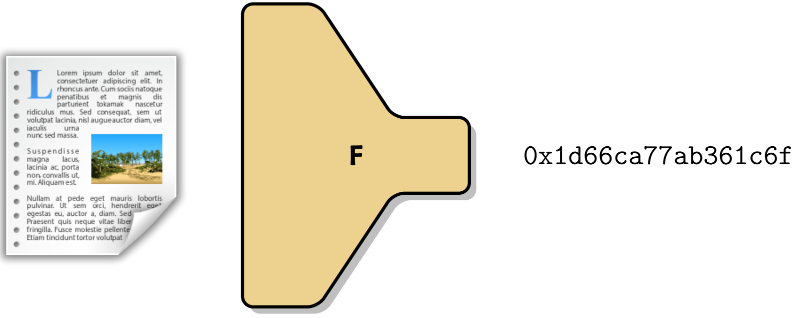
SAC 2010 – University of Waterloo



Hash Functions

- A public function with no structural properties.
  - Cryptographic strength without keys!

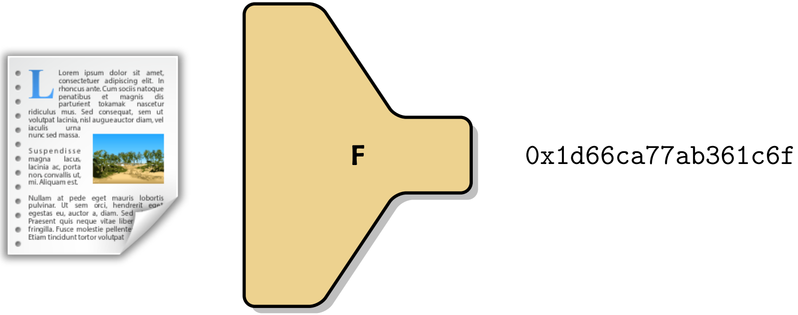
- $F : \{0,1\}^* \rightarrow \{0,1\}^n$



Hash Functions

- A public function with no structural properties.
  - Cryptographic strength without keys!

- $F : \{0,1\}^* \to \{0,1\}^n$



The SHA-3 Competition

- Similar to the AES competition
- Organized by NIST

- Submission dead-line was October 2008: 64 candidiates
- 51 valid submissions

- 14 in the second round (July 2009)
- 5 finalists in September 2010?
- Winner in 2012?

Hash Function Design

- Hash function from a block cipher
  - Davies-Meyer, MMO, ...
- Block cipher from a fixed function
  - Feistel scheme
- Pick your favorite fixed function
  - AES?
- If the fixed function is too small, use a generalized Feistel:

Lesamnta structure

SHAvite-3_{512} structure

Hash Function Design

- Hash function from a block cipher
  - Davies-Meyer, MMO, ...
- Block cipher from a fixed function
  - Feistel scheme
- Pick your favorite fixed function
  - AES?
- If the fixed function is too small, use a generalized Feistel:

Lesamnta structure

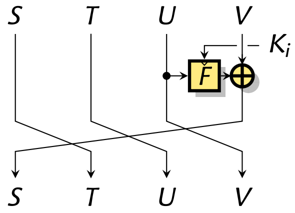
SHAvite-3_{512} structure

Hash Function Design

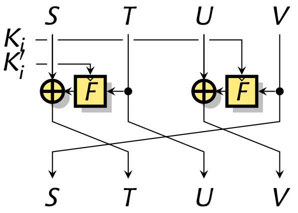
- Hash function from a block cipher
  - Davies-Meyer, MMO, ...
- Block cipher from a fixed function
  - Feistel scheme
- Pick your favorite fixed function
  - AES?
- If the fixed function is too small, use a generalized Feistel:

Hash Function Design

- Hash function from a block cipher
  - Davies-Meyer, MMO, ...
- Block cipher from a fixed function
  - Feistel scheme
- Pick your favorite fixed function
  - AES?
- If the fixed function is too small, use a generalized Feistel:



Lesamnta structure



SHAvite-3_{512} structure

Feistel Design

- Ideal: each F_i is an independent ideal function/permutation
- In practice: $F_i(x) = F(k_i \oplus x)$ with a fixed F

Properties of $F_i(x) = F(k_i \oplus x)$

(i) $\exists c_{i,j} : \forall x,\ F_i(x \oplus c_{i,j}) = F_j(x)$.

(ii) $\forall \alpha,\ \#\{x : F_i(x) \oplus F_j(x) = \alpha\}$ is even

(iii) $\bigoplus_x F_k\big(F_i(x) \oplus F_j(x)\big) = 0$

- $c_{ij} = k_i \oplus k_j$

Feistel Design

- Ideal: each F_i is an independent ideal function/permutation
- In practice: $F_i(x) = F(k_i \oplus x)$ with a fixed F

Properties of $F_i(x) = F(k_i \oplus x)$

(i) $\exists c_{i,j} : \forall x,\ F_i(x \oplus c_{i,j}) = F_j(x)$.

(ii) $\forall \alpha,\ \#\{x : F_i(x) \oplus F_j(x) = \alpha\}$ is even

(iii) $\bigoplus_x F_k\big(F_i(x) \oplus F_j(x)\big) = 0$

- $c_{ij} = k_i \oplus k_j$

Feistel Design

- Ideal: each F_i is an independent ideal function/permutation
- In practice: $F_i(x) = F(k_i \oplus x)$ with a fixed F

Properties of $F_i(x) = F(k_i \oplus x)$

(i) $\exists c_{i,j} : \forall x,\ F_i(x \oplus c_{i,j}) = F_j(x)$.

(ii) $\forall \alpha,\ \#\{x : F_i(x) \oplus F_j(x) = \alpha\}$ is even

(iii) $\bigoplus_x F_k\big(F_i(x) \oplus F_j(x)\big) = 0$

- $c_{ij} = k_i \oplus k_j$

Feistel Design

- Ideal: each F_i is an independent ideal function/permutation
- In practice: $F_i(x) = F(k_i \oplus x)$ with a fixed F

Properties of $F_i(x) = F(k_i \oplus x)$

(i) $\exists c_{i,j} : \forall x,\ F_i(x \oplus c_{i,j}) = F_j(x)$.

(ii) $\forall \alpha,\ \#\{x : F_i(x) \oplus F_j(x) = \alpha\}$ is even

(iii) $\bigoplus_x F_k\big(F_i(x) \oplus F_j(x)\big) = 0$

- $c_{ij} = k_i \oplus k_j$

Cancellation Cryptanalysis

Main idea

Cancel the effect of the non-linear components
Using twice the same input pairs

- Generalized Feistel with slow diffusion
- $F_i(x) = F(k_i \oplus x)$
  - Can sometimes deal with more keys (see *SHAvite-3*$_{512}$)
- Hash function setting
  - Some results apply to block ciphers.

Cancellation Cryptanalysis

Main idea

Cancel the effect of the non-linear components
Using twice the same input pairs

- Generalized Feistel with slow diffusion
- $F_i(x) = F(k_i \oplus x)$
  - Can sometimes deal with more keys (see *SHAvite-3*$_{512}$)
- Hash function setting
  - Some results apply to block ciphers.

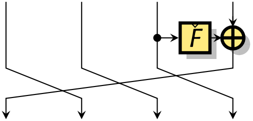
Cancellation Cryptanalysis

Main idea

Cancel the effect of the non-linear components
Using twice the same input pairs

- Generalized Feistel with slow diffusion
- $F_i(x) = F(k_i \oplus x)$
  - Can sometimes deal with more keys (see *SHAvite-3*$_{512}$)
- Hash function setting
  - Some results apply to block ciphers.

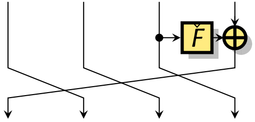
The Cancellation Property



- Full diffusion after 9 rounds
- If $y_1 = y_2 = y$, the differences cancel out
- Use constraints on the state

i	S_i	T_i	U_i	V_i	
0	x	-	-	-	
1	-	x	-	-	
2	-	-	x	-	
3	y_1	-	-	x	$x \to y_1$
4	x	y_1	-	-	
5	-	x	y_1	-	
6	z	-	x	y_1	$y_1 \to z$
7	y'	z	-	x	$x \to y_2, y' = y_1 \oplus y_2$
8	x	y'	z	-	
9	w	x	y'	z	$z \to w$

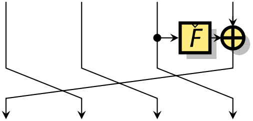
The Cancellation Property



- Full diffusion after 9 rounds
- If $y_1 = y_2 = y$, the differences cancel out
- Use constraints on the state

i	S_i	T_i	U_i	V_i	
0	x	-	-	-	
1	-	x	-	-	
2	-	-	x	-	
3	y_1	-	-	x	$x \to y_1$
4	x	y_1	-	-	
5	-	x	y_1	-	
6	z	-	x	y_1	$y_1 \to z$
7	y'	z	-	x	$x \to y_2, y' = y_1 \oplus y_2$
8	x	y'	z	-	
9	w	x	y'	z	$z \to w$

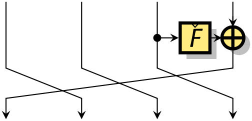
The Cancellation Property



- Full diffusion after 9 rounds
- If $y_1 = y_2 = y$, the differences cancel out
- Use constraints on the state

i	S_i	T_i	U_i	V_i	
0	x	-	-	-	
1	-	x	-	-	
2	-	-	x	-	
3	y	-	-	x	$x \to y$
4	x	y	-	-	
5	-	x	y	-	
6	z	-	x	y	$y_1 \to z$
7	-	z	-	x	$x \to y$
8	x	-	z	-	
9	w	x	-	z	$z \to w$

The Cancellation Property



- Full diffusion after 9 rounds
- If $y_1 = y_2 = y$, the differences cancel out
- Use constraints on the state

i	S_i	T_i	U_i	V_i	
0	x	-	-	-	
1	-	x	-	-	
2	-	-	x	-	
3	y	-	-	x	$x \to y$
4	x	y	-	-	
5	-	x	y	-	
6	z	-	x	y	$y_1 \to z$
7	-	z	-	x	$x \to y$
8	x	-	z	-	
9	w	x	-	z	$z \to w$

The Cancellation Property: Looking at the Values

We study values, starting at round 2:

i	S_i	T_i	U_i	V_i
2	a	b	c	d
3	$F_2(c) \oplus d$	a	b	c
4	$F_3(b) \oplus c$	$F_2(c) \oplus d$	a	b
5	$F_4(a) \oplus b$	$F_3(b) \oplus c$	$F_2(c) \oplus d$	a
6	$F_5(F_2(c) \oplus d) \oplus a$	$F_4(a) \oplus b$	$F_3(b) \oplus c$	$F_2(c) \oplus d$
7	$F_6(F_3(b) \oplus \underline{c}) \oplus F_2(\underline{c}) \oplus d$	$F_5(F_2(c) \oplus d) \oplus a$	$F_4(a) \oplus b$	$F_3(b) \oplus c$

Round 7: $F_6(F_3(b) \oplus \underline{c}) \oplus F_2(\underline{c})$. They cancel if:

$F_3(b) = c_{2,6} = K_2 \oplus K_6$

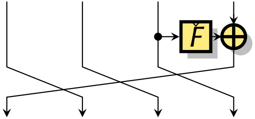
i.e. $b = F_3^{-1}(K_2 \oplus K_6)$

Attack Overview

- Partial preimage: Choose one part of the output
  - Gives preimage and collision attacks.
- Mostly generic in the round function.
- Hash function setting: no keys.

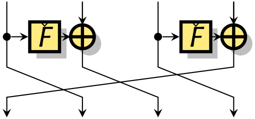
Result Overview

- Attacks on reduced *Lesamnta*



  - 24 rounds out of 32: collision and preimage
  - previous attacks: 16 rounds

- Attacks on reduced *SHAvite-3*$_{512}$



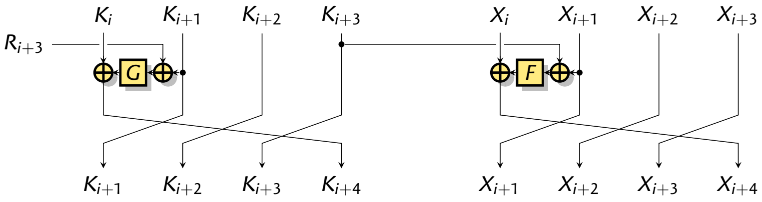
  - 9 rounds out of 14: preimage
  - previous attacks: 8 rounds

Lesamnta

- Merkle-Damgård with an MMO compression function
- Generalized Feistel
- Round function is AES-based

Shoichi Hirose, Hidenori Kuwakado, Hirotaka Yoshida
SHA-3 Proposal: Lesamnta
Submission to the NIST SHA-3 competition

Lesamnta (cont.)



$$X_{i+4} = X_i \oplus F\left(X_{i+1} \oplus K_{i+3}\right)$$
$$K_{i+4} = K_i \oplus G\left(K_{i+1} \oplus R_{i+3}\right).$$

- Chaining value loaded to $K_{-3}, K_{-2}, K_{-1}, K_0$
- Message loaded to $X_{-3}, X_{-2}, X_{-1}, X_0$
- F and G AES-based

Lesamnta: Truncated Differential

i	S_i	T_i	U_i	V_i
0	x	-	-	-
1	-	x	-	-
2	-	-	x	-
⋮		$(x \to x_1)$		
19	x_1	?	?	r
20	?	x_1	?	?
21	?	?	x_1	?
22	?	?	?	x_1
FF	?	?	?	x_1

i	S_i	T_i	U_i	V_i	
2	-	-	x	-	
3	y	-	-	x	$x \to y$
4	x	y	-	-	
5	-	x	y	-	
6	z	-	x	y	$y \to z$
7	-	z	-	x	$x \to y$
8	x	-	z	-	
9	w	x	-	z	$z \to w$
10	z	w	x	-	
11	x_1	z	w	x	$x \to x_1$
12	r	x_1	z	w	$w \to x \oplus r$
13	-	r	x_1	z	$z \to w$
14	?	-	r	x_1	
15	$x_1 + t$	?	-	r	$r \to t$
16	r	$x_1 + t$	?	-	
17	?	r	$x_1 + t$	?	
18	?	?	r	$x_1 + t$	
19	x_1	?	?	r	$r \to t$

Lesamnta: Truncated Differential

i	S_i	T_i	U_i	V_i
0	x	-	-	-
1	-	x	-	-
2	-	-	x	-
⋮		$(x \to x_1)$		
19	x_1	?	?	r
20	?	x_1	?	?
21	?	?	x_1	?
22	?	?	?	x_1
FF	?	?	?	x_1

Properties

- Using conditions on the state, probability 1.
- The transition $x \to x_1$ is known.

How to use it

- Start with a random message
- x_1 is the difference between the output and the target value
- Compute x from x_1
- Use $M + (x, 0, 0, 0)$

Lesamnta: Truncated Differential

i	S_i	T_i	U_i	V_i
0	x	-	-	-
1	-	x	-	-
2	-	-	x	-
⋮		$(x \to x_1)$		
19	x_1	?	?	r
20	?	x_1	?	?
21	?	?	x_1	?
22	?	?	?	x_1
FF	?	?	?	x_1

Properties

- Using conditions on the state, probability 1.
- The transition $x \to x_1$ is known.

How to use it

- Start with a random message
- x_1 is the difference between the output and the target value
- Compute x from x_1
- Use $M + (x, 0, 0, 0)$

Lesamnta: Values

i	$X_i (= S_i)$
-1	d
0	c
1	b
2	a
3	$F_2(c) \oplus d$
4	$F_3(b) \oplus c$
5	$F_4(a) \oplus b$
6	$F_5(F_2(c) \oplus d) \oplus a$
7	$F_6(F_3(b) \oplus c) \oplus F_2(c) \oplus d$
8	$F_7(F_4(a) \oplus b) \oplus F_3(b) \oplus c$
9	$F_8(F_5(F_2(c) \oplus d) \oplus a) \oplus F_4(a) \oplus b$
10	$F_9(d) \oplus F_5(F_2(c) \oplus d) \oplus a$
11	$F_{10}(F_7(F_4(a) \oplus b) \oplus F_3(b) \oplus c) \oplus d$
12	$F_{11}(F_8(F_5(F_2(c) \oplus d) \oplus a) \oplus F_4(a) \oplus b) \oplus F_7(F_4(a) \oplus b) \oplus F_3(b) \oplus c$
13	$F_{12}(F_9(d) \oplus F_5(F_2(c) \oplus d) \oplus a) \oplus F_8(F_5(F_2(c) \oplus d) \oplus a) \oplus F_4(a) \oplus b$
15	$F_{14}(X_{12}) \oplus F_{10}(F_7(F_4(a) \oplus b) \oplus F_3(b) \oplus c) \oplus d$
16	$F_{15}(F_4(a) \oplus b) \oplus X_{12}$
19	$F_{18}(F_{15}(F_4(a) \oplus b) \oplus X_{12}) \oplus F_{14}(X_{12}) \oplus F_{10}(F_7(F_4(a) \oplus b) \oplus F_3(b) \oplus c) \oplus d$

Lesamnta Cancellation Conditions

Round 7: $F_6(F_3(b) \oplus \underline{c}) \oplus F_2(\underline{c})$.
They cancel if: $F_3(b) = c_{2,6} = K_2 \oplus K_6$
i.e. $b = F_3^{-1}(K_2 \oplus K_6)$

Round 13: $F_{12}(F_9(d) \oplus \underline{F_5(F_2(c) \oplus d) \oplus a}) \oplus F_8(\underline{F_5(F_2(c) \oplus d) \oplus a})$.
They cancel if: $F_9(d) = c_{8,12} = K_8 \oplus K_{12}$
i.e. $d = F_9^{-1}(K_8 \oplus K_{12})$

Round 19: $F_{18}(F_{15}(F_4(a) \oplus b) \oplus \underline{X_{12}}) \oplus F_{14}(\underline{X_{12}})$.
They cancel if: $F_{15}(F_4(a) \oplus b) = c_{14,18} = K_{14} \oplus K_{18}$
i.e. $a = F_4^{-1}(F_{15}^{-1}(K_{14} \oplus K_{18}) \oplus b)$

22-round Attacks

- Compute a, b, d, to satisfy the cancellation conditions.
- Set the state at round 2 to (a, b, c, d).

- Express the output as a function of c
- $V_0 = \eta$
  - $\eta = b \oplus F_0(a \oplus F_3(d))$
- $V_{22} = F(c \oplus \alpha) \oplus \beta$
  - $\alpha = K_{11} \oplus F_8(F_5(a) \oplus b) \oplus F_4(b)$
  - $\beta = d$
- For a target value $\overline{H}$, set $c = F^{-1}(\overline{H} \oplus \eta \oplus \beta) \oplus \alpha$
- This gives $V_0 \oplus V_{22} = \overline{H}$

22-round Attacks

- Compute a, b, d, to satisfy the cancellation conditions.
- Set the state at round 2 to (a, b, c, d).
- Express the output as a function of c
- $V_0 \;= \eta$
  - $\eta = b \oplus F_0(a \oplus F_3(d))$
- $V_{22} = F(c \oplus \alpha) \oplus \beta$
  - $\alpha = K_{11} \oplus F_8(F_5(a) \oplus b) \oplus F_4(b)$
  - $\beta = d$
- For a target value $\overline{H}$, set $c = F^{-1}(\overline{H} \oplus \eta \oplus \beta) \oplus \alpha$
- This gives $V_0 \oplus V_{22} = \overline{H}$

22-round Attacks

- Compute a, b, d, to satisfy the cancellation conditions.
- Set the state at round 2 to (a, b, c, d).

- Express the output as a function of c
- $V_0 = \eta$
  - $\eta = b \oplus F_0(a \oplus F_3(d))$
- $V_{22} = F(c \oplus \alpha) \oplus \beta$
  - $\alpha = K_{11} \oplus F_8(F_5(a) \oplus b) \oplus F_4(b)$
  - $\beta = d$

- For a target value $\overline{H}$, set $c = F^{-1}(\overline{H} \oplus \eta \oplus \beta) \oplus \alpha$
- This gives $V_0 \oplus V_{22} = \overline{H}$

24-round Attacks

- Compute a, b, d, to satisfy the cancellation conditions.
- Set the state at round 4 to (a, b, c, d).

- $V_0 = F(c \oplus \gamma) \oplus \lambda$
  - $\gamma = F_1(b \oplus F_2(a \oplus F_3(d)))$
  - $\lambda = d$
- $V_{24} = F(c \oplus \alpha) \oplus \beta$
  - $\alpha = K_{13} \oplus F_{10}(F_7(a) \oplus b) \oplus F_6(b)$
  - $\beta = d$

- The output is $H = F(c \oplus \gamma) \oplus F(c \oplus \alpha)$.
- To reach a target $\overline{H}$, we need a pair of values for F with
  - input difference $\alpha \oplus \gamma$
  - output difference $\overline{H}$
- We can store them in a table.

24-round Attacks

- Compute a, b, d, to satisfy the cancellation conditions.
- Set the state at round 4 to (a, b, c, d).

- $V_0 = F(c \oplus \gamma) \oplus \lambda$
  - $\gamma = F_1(b \oplus F_2(a \oplus F_3(d)))$
  - $\lambda = d$
- $V_{24} = F(c \oplus \alpha) \oplus \beta$
  - $\alpha = K_{13} \oplus F_{10}(F_7(a) \oplus b) \oplus F_6(b)$
  - $\beta = d$

- The output is $H = F(c \oplus \gamma) \oplus F(c \oplus \alpha)$.
- To reach a target $\overline{H}$, we need a pair of values for F with
  - input difference $\alpha \oplus \gamma$
  - output difference $\overline{H}$
- We can store them in a table.

24-round Attacks

- Compute a, b, d, to satisfy the cancellation conditions.
- Set the state at round 4 to (a, b, c, d).

- $V_0 = F(c \oplus \gamma) \oplus \lambda$
  - $\gamma = F_1(b \oplus F_2(a \oplus F_3(d)))$
  - $\lambda = d$
- $V_{24} = F(c \oplus \alpha) \oplus \beta$
  - $\alpha = K_{13} \oplus F_{10}(F_7(a) \oplus b) \oplus F_6(b)$
  - $\beta = d$

- The output is $H = F(c \oplus \gamma) \oplus F(c \oplus \alpha)$.
- To reach a target $\overline{H}$, we need a pair of values for F with
  - input difference $\alpha \oplus \gamma$
  - output difference $\overline{H}$
- We can store them in a table.

Improved 24-round Attack

- The output is $H = F(c \oplus \gamma) \oplus F(c \oplus \alpha)$.
- F is AES-based.

- Use the symmetry property of AES:
  - If x is symmetric, then $F(x)$ is symmetric
- Try random keys until $\alpha \oplus \gamma$ is symmetric
- For all symmetric u, $c = \alpha \oplus u$ gives a symmetric output

- One output word symmetric for an amortized cost of 1
  - $\approx n/8$ bits set to zero

Results: SHAvite-3_{512}

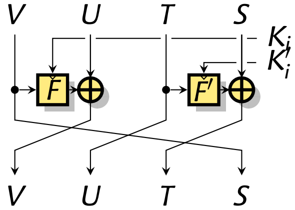
			Lesamnta-256		*Lesamnta*-512	
	Attack	Rounds	Time	Memory	Time	Memory
Generic	Collision	22	2^{96}	-	2^{192}	-
	2^{nd} Preimage	22	2^{192}	-	2^{384}	-
	Collision	24	2^{96}	2^{64}	2^{192}	2^{128}
	2^{nd} Preimage	24	2^{192}	2^{64}	2^{384}	2^{128}
Specific	Collision	24	2^{112}	-	2^{224}	-
	2^{nd} Preimage	24	2^{240}	-	*N/A*	

SHAvite-3_{512}

- Merkle-Damgård with a Davies-Meyer compression function
- Generalized Feistel
- Round function is AES-based

Eli Biham and Orr Dunkelman
The SHAvite-3 Hash Function
Submission to the NIST SHA-3 competition

SHAvite-3_{512} (cont.)



- 14 rounds
- Davies-Meyer (message is the key)
- $F_i(x) = AES(AES(AES(AES(x \oplus k_i^0) \oplus k_i^1) \oplus k_i^2) \oplus k_i^3)$
- F is one AES round.
- Key schedule mixes linear operations and AES rounds.

SHAvite-3_{512}: Truncated Differential

i	S_i	T_i	U_i	V_i	
0	?	x_2	?	x	
1	x	-	x_2	x_1	
2	x_1	x	-	-	$x_1 \to x_2$
3	-	-	x	-	$x \to x_1$
4	-	-	-	x	
5	x	-	-	y	$x \to y$
6	y	x	-	z	$y \to z$
7	z	-	x	w	$x \to y, z \to w$
8	w	z	-	?	
9	?	-	z	?	$z \to w$
FF	?	x_2	?	?	

Properties

- Using conditions on the state, probability 1.
- The transitions $x \to x_1$ and $x_1 \to x_2$ are known.
- Same attack as earlier.

Problem

- F has many keys

SHAvite-3_{512}: Truncated Differential

i	S_i	T_i	U_i	V_i	
0	?	x_2	?	x	
1	x	-	x_2	x_1	
2	x_1	x	-	-	$x_1 \to x_2$
3	-	-	x	-	$x \to x_1$
4	-	-	-	x	
5	x	-	-	y	$x \to y$
6	y	x	-	z	$y \to z$
7	z	-	x	w	$x \to y$, $z \to w$
8	w	z	-	?	
9	?	-	z	?	$z \to w$
FF	?	x_2	?	?	

Properties

- Using conditions on the state, probability 1.
- The transitions $x \to x_1$ and $x_1 \to x_2$ are known.
- Same attack as earlier.

Problem

- F has many keys

SHAvite-3_{512}: Values

i	X_i / Y_i
X_0	$b \oplus F_3(c) \oplus F'_1(c \oplus F_2(d \oplus F'_3(a)))$
Y_0	$d \oplus F'_3(a) \oplus F_1(a \oplus F'_2(b \oplus F_3(c)))$
X_1	$a \oplus F'_2(b \oplus F_3(c))$
Y_1	$c \oplus F_2(d \oplus F'_3(a))$
X_2	$d \oplus F'_3(a)$
Y_2	$b \oplus F_3(c)$
X_3	c
Y_3	a
X_4	b
Y_4	d
X_5	$a \oplus F_4(b)$
Y_5	$c \oplus F'_4(d)$
X_6	$d \oplus F_5(a \oplus F_4(b))$
Y_6	$b \oplus F'_5(c \oplus F'_4(d))$
X_7	$c \oplus F'_4(d) \oplus F_6(d \oplus F_5(a \oplus F_4(b)))$
Y_7	$a \oplus F_4(b) \oplus F'_6(b \oplus F'_5(c \oplus F'_4(d)))$
X_8	$b \oplus F'_5(c \oplus F'_4(d)) \oplus F_7(c)$
Y_8	$d \oplus F_5(a \oplus F_4(b)) \oplus F'_7(a \oplus F_4(b) \oplus F'_6(b \oplus F'_5(c \oplus F'_4(d))))$
X_9	$a \oplus F_4(b) \oplus F'_6(b \oplus F'_5(c \oplus F'_4(d))) \oplus F_8(b \oplus F'_5(c \oplus F'_4(d)) \oplus F_7(c))$

Message Conditions: SHAvite-3_{512}

Round 7 $F'_4(\underline{d}) \oplus F_6(\underline{d} \oplus F_5(a \oplus F_4(b)))$.
They cancel if: $F_5(a \oplus F_4(b)) = k^0_{1,4} \oplus k^0_{0,6}$
and $(k^1_{1,4}, k^2_{1,4}, k^3_{1,4}) = (k^1_{0,6}, k^2_{0,6}, k^3_{0,6})$.

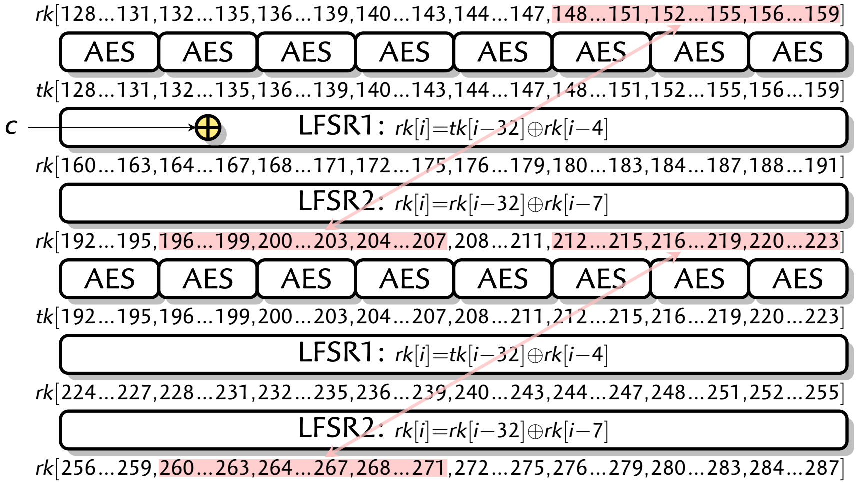
Round 9 $F'_6(\underline{b \oplus F'_5(c \oplus F'_4(d))}) \oplus F_8(\underline{b \oplus F'_5(c \oplus F'_4(d))} \oplus F_7(c))$.
They cancel if: $F_7(c) = k^0_{1,6} \oplus k^0_{0,8}$
and $(k^1_{1,6}, k^2_{1,6}, k^3_{1,6}) = (k^1_{0,8}, k^2_{0,8}, k^3_{0,8})$.

Message Conditions: SHAvite-3_{512}

Round 7 $F'_4(\underline{d}) \oplus F_6(\underline{d} \oplus F_5(a \oplus F_4(b)))$.
They cancel if: $F_5(a \oplus F_4(b)) = k^0_{1,4} \oplus k^0_{0,6}$
and $(k^1_{1,4}, k^2_{1,4}, k^3_{1,4}) = (k^1_{0,6}, k^2_{0,6}, k^3_{0,6})$.

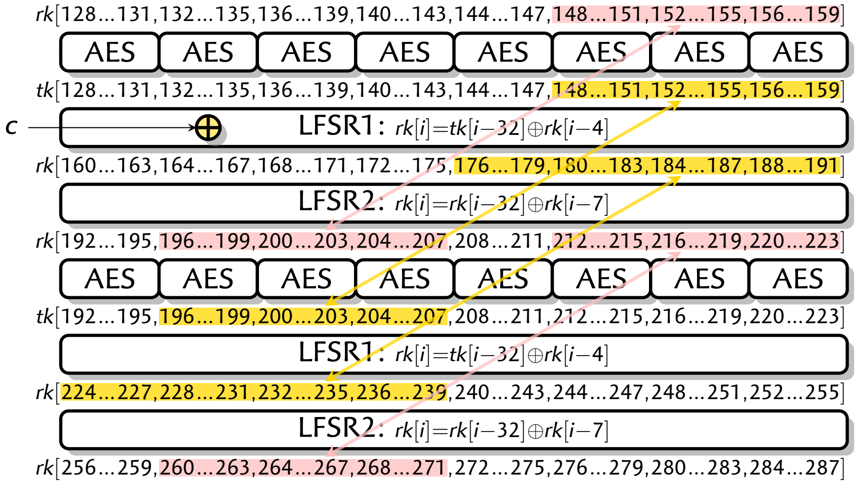
Round 9 $F'_6(\underline{b \oplus F'_5(c \oplus F'_4(d))}) \oplus F_8(\underline{b \oplus F'_5(c \oplus F'_4(d))} \oplus F_7(c))$.
They cancel if: $F_7(c) = k^0_{1,6} \oplus k^0_{0,8}$
and $(k^1_{1,6}, k^2_{1,6}, k^3_{1,6}) = (k^1_{0,8}, k^2_{0,8}, k^3_{0,8})$.

Message Expansion



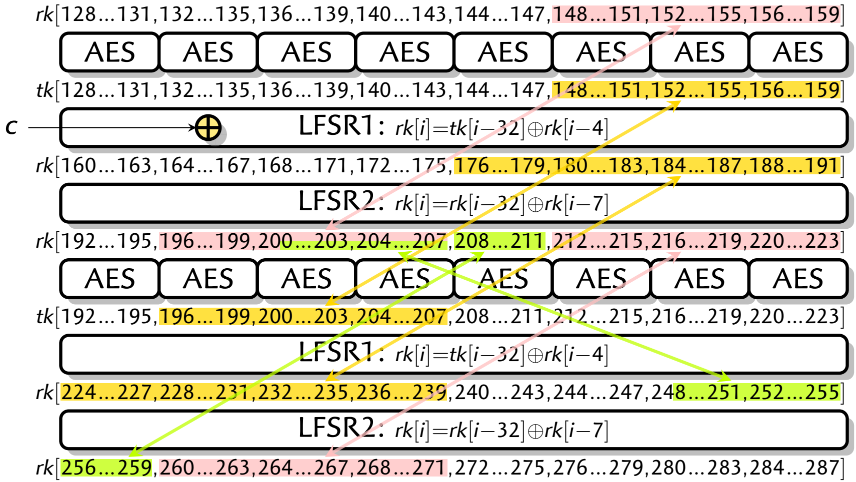
1. Propagate constraints

Message Expansion



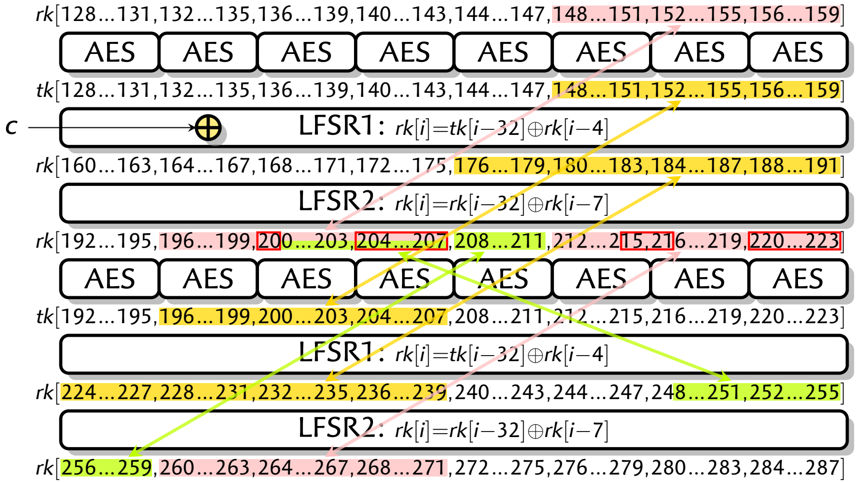
1. Propagate constraints

Message Expansion



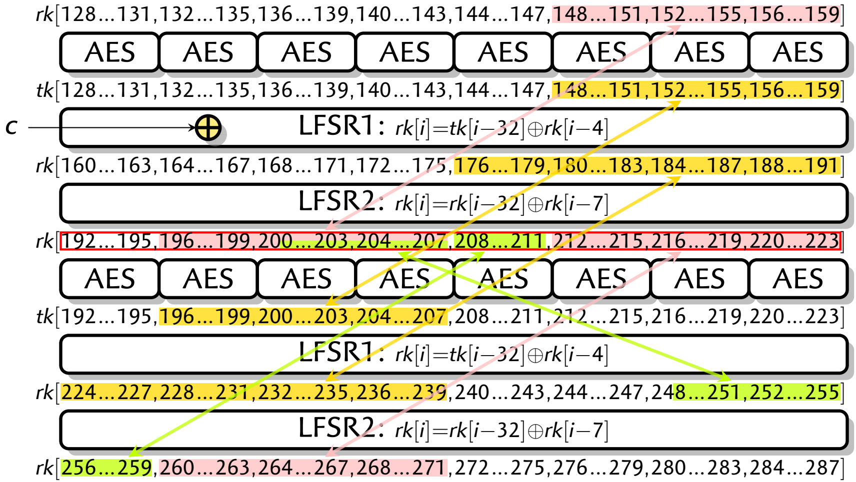
1. Propagate constraints

Message Expansion



2. Guess values

Message Expansion



3 Compute the missing values; check coherence

Solving the Conditions

- We can build a chaining value satisfying the 6 conditions with cost 2^{96}.
- Each chaining value can be used 2^{128} times to fix 128 bits of the output.
  - Cost of finding a good message is amortized.
- Attacks on 9-round *SHAvite-3*$_{512}$:
  - Free-start preimage with complexity 2^{384}
  - Second-Preimage with complexity 2^{448}.

Later Improvements

- 10-round attack using both degrees of freedom
- Pseudo-attacks on the full 14 rounds (chosen salts)

Praveen Gauravaram, Gaëtan Leurent, Florian Mendel, María Naya-Plasencia, Thomas Peyrin, Christian Rechberger, and Martin Schläffer
Cryptanalysis of the 10-Round Hash and Full Compression Function of *SHAvite-3*$_{512}$
Africacrypt 2010

Results: SHAvite-3_{512}

Attack		Rounds	Comp. Fun.		Hash Fun.	
			Time	Mem.	Time	Mem.
2nd Preimage	new	9	2^{384}	-	2^{448}	2^{64}
2nd Preimage	[AF'10]	10	2^{480}	-	2^{496}	2^{16}
2nd Preimage	improved	10	2^{448}	-	2^{480}	2^{32}
2nd Preimage	improved	10	2^{416}	2^{64}	2^{464}	2^{64}
2nd Preimage	improved	10	2^{384}	2^{128}	2^{448}	2^{128}
Collision[1]	[AF'10]	14	2^{192}	2^{128}	*N/A*	
Preimage[1]	[AF'10]	14	2^{384}	2^{128}	*N/A*	
Preimage[1]	[AF'10]	14	2^{448}	-	*N/A*	

[1] Chosen salt attacks

Conclusion

- Shows the difference an ideal Feistel with independent round functions and a practical construction.
- *Full version*: ePrint report 2009/634.
  - Includes some block cipher results
- Any questions?