Differential Fault Analysis on the Families of SIMON and SPECK Ciphers

Harshal Tupsamudre, Shikha Bisht, Debdeep Mukhopadhyay
(IIT KHARAGPUR)

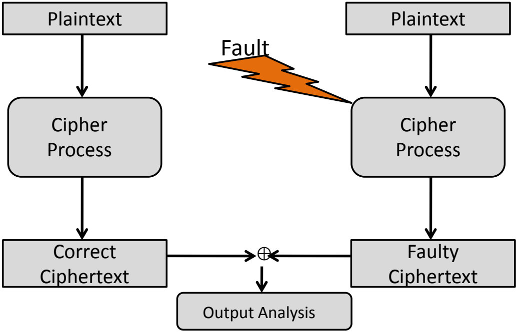
FDTC 2014

South Korea, Busan

September 23, 2014

Outline

Fault Attack



Fault Attack

1. Fault models to model the strength of adversary
   1. Bit flip Fault Model : Affects a bit of the intermediate result
   2. Constant Byte Fault Model : Requires control over fault value and position
   3. Random Byte Fault Model : No control over fault value and position
2. Attacks that require both the correct and faulty ciphertext are known as differential fault attacks

Introduction

1. SIMON and SPECK : Family of lightweight block ciphers

Introduction

1. SIMON and SPECK : Family of lightweight block ciphers
2. Proposed by the National Security Agency(NSA) in 2013

Introduction

1. SIMON and SPECK : Family of lightweight block ciphers
2. Proposed by the National Security Agency(NSA) in 2013
3. No fault attack reported so far

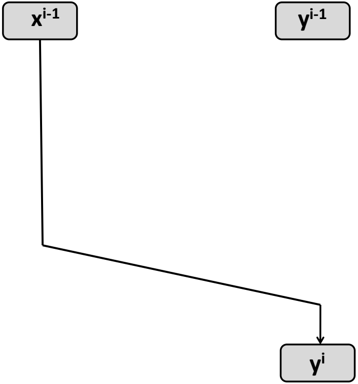
Introduction

1. SIMON and SPECK : Family of lightweight block ciphers
2. Proposed by the National Security Agency(NSA) in 2013
3. No fault attack reported so far
4. Fault models used in the attacks: Bit flip and Random byte fault model

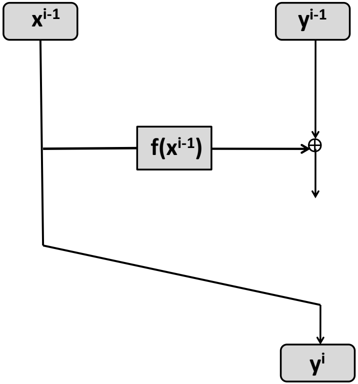
Fault Attack on SIMON

Round Function of SIMON cipher

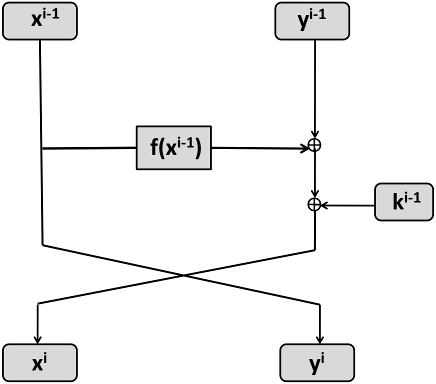
Round Function of SIMON cipher



Round Function of SIMON cipher



Round Function of SIMON cipher



$$(x^i, y^i) = (y^{i-1} \oplus f(x^{i-1}) \oplus k^{i-1}, x^{i-1}), i \in \{1, \ldots, T\}$$

Function f: Source of Information Leakage

$$\boxed{f(x^{i-1})} = \boxed{(S^1x^{i-1} \,\&\, S^8x^{i-1}) \oplus S^2x^{i-1}}$$

1. $S^i x$: Circular left shift of x by i bits

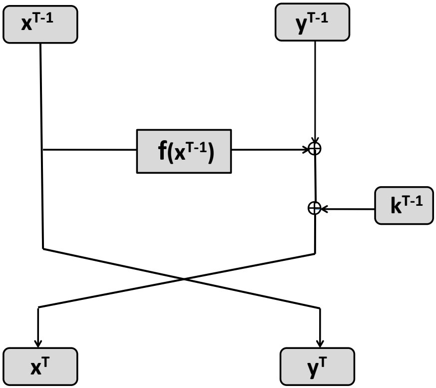
Function f: Source of Information Leakage

$$\boxed{f(x^{i-1})} = \boxed{(S^1x^{i-1} \ \& \ S^8x^{i-1}) \oplus S^2x^{i-1}}$$

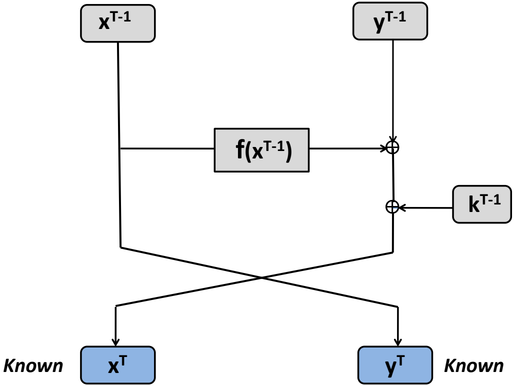
1. $S^i x$: Circular left shift of x by i bits
2. AND operation: A faulty bit in the input leaks information about the non-faulty bit.

Equation of the Last Round Key

Equation of the Last Round Key

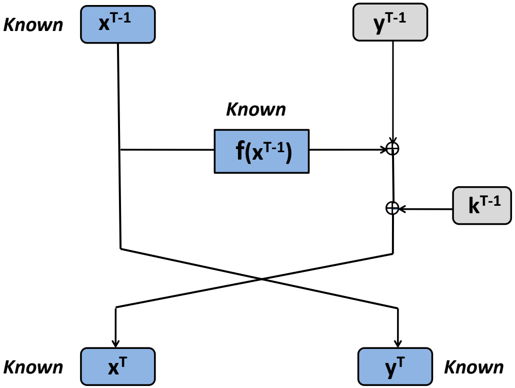


Equation of the Last Round Key

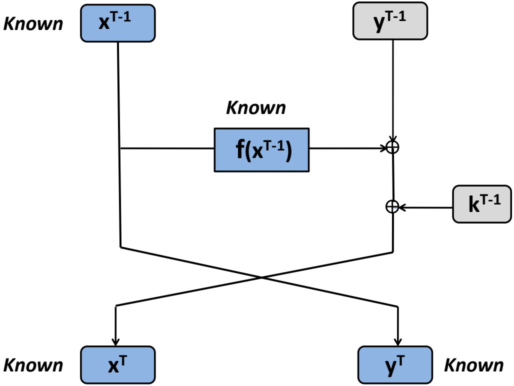


(x^T, y^T): Ciphertext

Equation of the Last Round Key

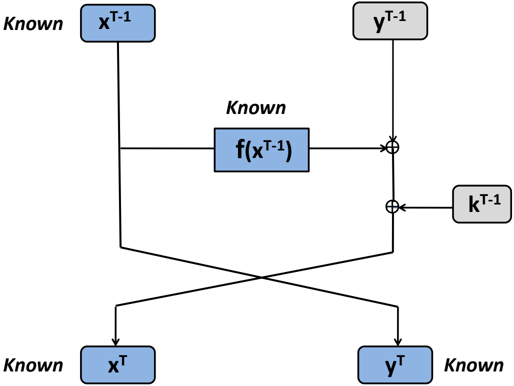


Equation of the Last Round Key



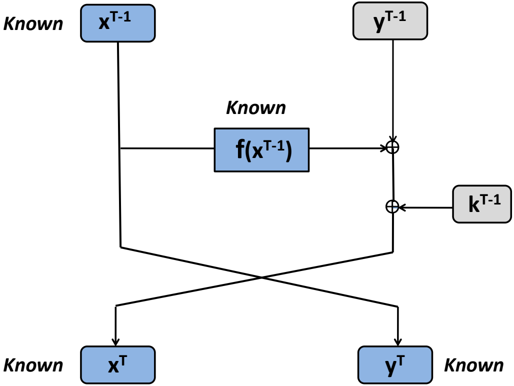
$$\because x^T = y^{T-1} \oplus f(x^{T-1}) \oplus k^{T-1}$$

Equation of the Last Round Key



$$\because x^T = y^{T-1} \oplus f(x^{T-1}) \oplus k^{T-1} = y^{T-1} \oplus f(y^T) \oplus k^{T-1}$$

Equation of the Last Round Key

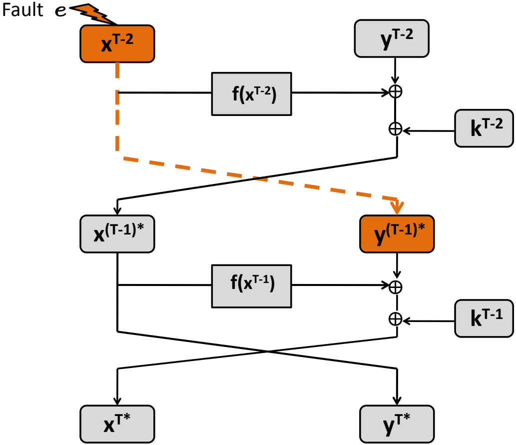


$$\because x^T = y^{T-1} \oplus f(x^{T-1}) \oplus k^{T-1} = y^{T-1} \oplus f(y^T) \oplus k^{T-1}$$

$$\therefore k^{T-1} = y^{T-1} \oplus f(y^T) \oplus x^T$$

Fault Injection in the Target Round

Fault Injection in the Target Round



(x^{T^*}, y^{T^*}): Faulty Ciphertext

Determining Fault Position and Value

Using Correct Ciphertext:

$$\begin{aligned} k^{T-1} \oplus y^{T-1} &= f(y^{T}) \oplus x^{T} \\ k^{T-1} \oplus x^{T-2} &= f(y^{T}) \oplus x^{T} \end{aligned} \tag{1}$$

Determining Fault Position and Value

Using Correct Ciphertext:

$$\begin{aligned} k^{T-1} \oplus y^{T-1} &= f(y^{T}) \oplus x^{T} \\ k^{T-1} \oplus x^{T-2} &= f(y^{T}) \oplus x^{T} \end{aligned} \tag{1}$$

Using Faulty Ciphertext:

$$\begin{aligned} k^{T-1} \oplus y^{(T-1)^*} &= f(y^{T^*}) \oplus x^{T^*} \\ k^{T-1} \oplus x^{T-2} \oplus e &= f(y^{T^*}) \oplus x^{T^*} \end{aligned} \tag{2}$$

Determining Fault Position and Value

Using Correct Ciphertext:

$$\begin{aligned} k^{T-1} \oplus y^{T-1} &= f(y^T) \oplus x^T \\ k^{T-1} \oplus x^{T-2} &= f(y^T) \oplus x^T \end{aligned} \tag{1}$$

Using Faulty Ciphertext:

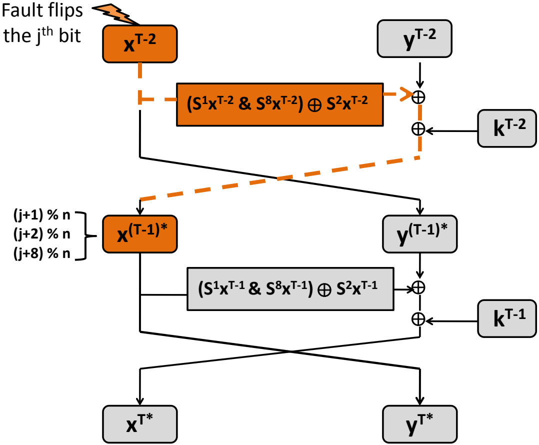
$$\begin{aligned} k^{T-1} \oplus y^{(T-1)^*} &= f(y^{T^*}) \oplus x^{T^*} \\ k^{T-1} \oplus x^{T-2} \oplus e &= f(y^{T^*}) \oplus x^{T^*} \end{aligned} \tag{2}$$

Using (1) and (2):

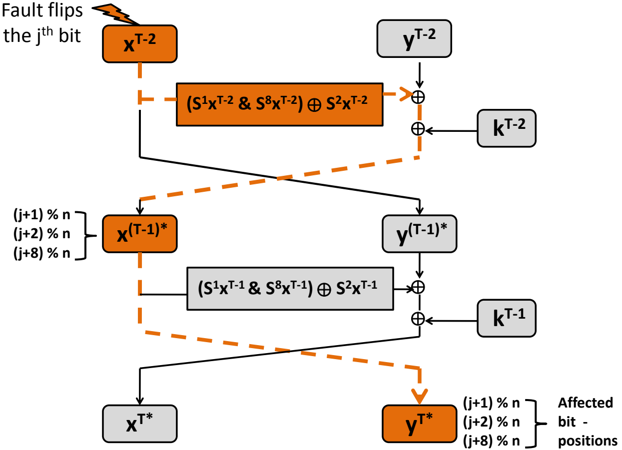
$$e = x^T \oplus x^{T^*} \oplus f(y^T) \oplus f(y^{T^*})$$

Hence, we know the flipped bit(s) of x^{T-2}

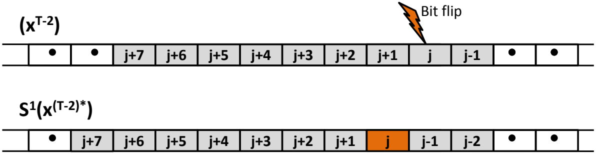
A Bit-Flip Fault Attack on SIMON



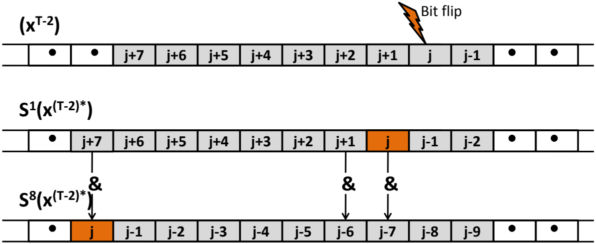
A Bit-Flip Fault Attack on SIMON



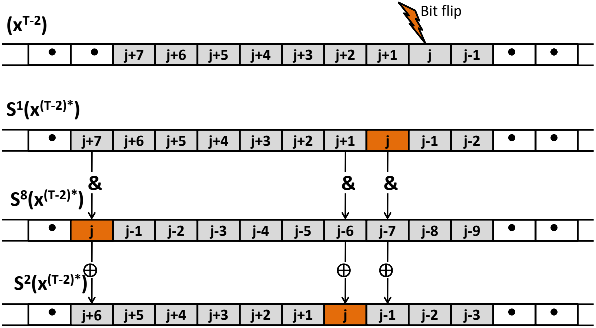
A Bit-Flip Fault Attack on SIMON



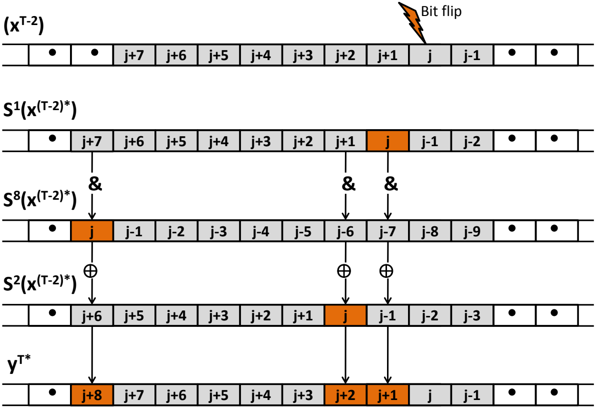
A Bit-Flip Fault Attack on SIMON



A Bit-Flip Fault Attack on SIMON



A Bit-Flip Fault Attack on SIMON



A Bit-Flip Fault Attack on SIMON

case 1 : $x^{T-2}_{(j-7)\%n} = 0$

$$y^{T}{}_{j+1} = (x_j^{T-2} \ \& \ x^{T-2}_{(j-7)\%n}) \oplus Remaining Terms$$
$$y^{T^*}{}_{j+1} = ((x_j^{T-2} \oplus 1) \ \& \ x^{T-2}_{(j-7)\%n}) \oplus Remaining Terms$$

x_j^{T-2}	$x_j^{T-2} \oplus 1$	$x^{T-2}_{(j-7)\%n}$	$(y^T \oplus y^{T^*})_{(j+1)\%n}$
0	1	0	0
1	0	0	0

Table: Secret Value $x^{T-2}_{(j-7)\%n}$ obtained from $(y^T \oplus y^{T^*})_{(j+1)\%n}$

A Bit-Flip Fault Attack on SIMON

case 2 : $x^{T-2}_{(j-7)\%n} = 1$

$$y^{T} = (x^{T-2}_{j} \ \& \ x^{T-2}_{(j-7)\%n}) \oplus RemainingTerms$$
$$y^{T^*} = ((x^{T-2}_{j} \oplus 1) \ \& \ x^{T-2}_{(j-7)\%n}) \oplus RemainingTerms$$

x^{T-2}_{j}	$x^{T-2}_{j} \oplus 1$	$x^{T-2}_{(j-7)\%n}$	$(y^{T} \oplus y^{T^*})_{(j+1)\%n}$
0	1	1	1
1	0	1	1

Table: Secret Value $x^{T-2}_{(j-7)\%n}$ obtained from $(y^{T} \oplus y^{T^*})_{(j+1)\%n}$

A Bit-Flip Fault Attack on SIMON

$$k_{j-7}^{T-1} = y_{j-7}^{T-1} \oplus f(y^T)_{j-7} \oplus x_{j-7}^{T}$$
$$k_{j+7}^{T-1} = y_{j+7}^{T-1} \oplus f(y^T)_{j+7} \oplus x_{j+7}^{T}$$

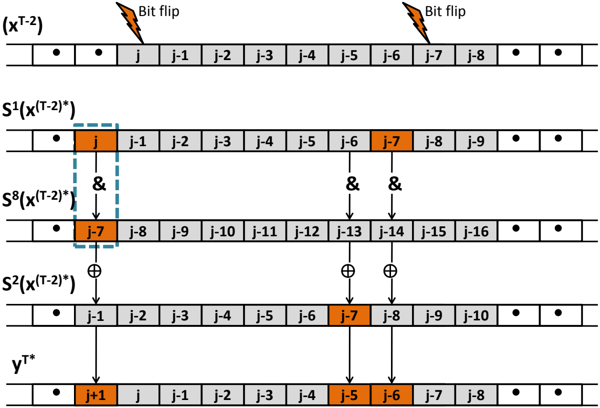
Using a single bit-flip, we can retrieve two bits of last round key.

Simulation Results

n bits	k^{T-1}	Avg. No. of Faulty Encryptions
16	0xfa 0x24	25
24	0x26 0x53 0xaf	43
32	0x87 0x46 0x09 0x1a	62
48	0x22 0x4d 0xe9 0xcf 0x51 0xdd	104
64	0x19 0x26 0x5a 0xc7 0x4f 0xf2 0x90 0x01	150

Table: Bit-flip Fault Attack on SIMON Assuming no Control Over the Fault Position

A Random-Byte Fault Attack on SIMON: Case 1



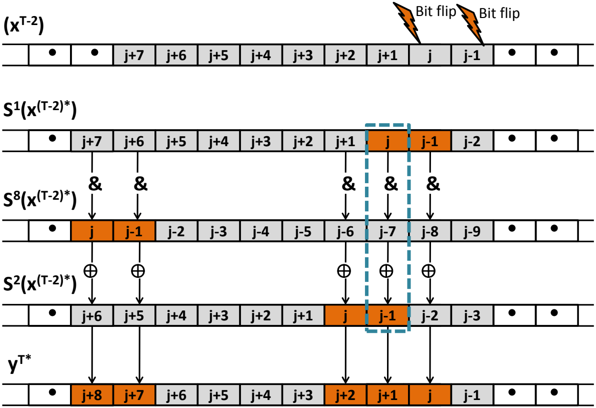
A Random-Byte Fault Attack on SIMON: Case 1

$$y^T = (x_j^{T-2} \,\&\, x_{(j-7)\%n}^{T-2}) \oplus RemainingTerms$$
$$y^{T^*} = ((x_j^{T-2} \oplus 1) \,\&\, (x_{(j-7)\%n}^{T-2} \oplus 1)) \oplus RemainingTerms$$

x_j^{T-2}	$x_j^{T-2} \oplus 1$	$x_{(j-7)\%n}^{T-2}$	$x_{(j-7)\%n}^{T-2} \oplus 1$	$(y^T \oplus y^{T^*})_{(j+1)\%n}$
0	1	1	0	0
1	0	0	1	0
0	1	0	1	1
1	0	1	0	1

Table: Relation between the Secret Values $x_{(j)\%n}^{T-2}$ and $x_{(j-7)\%n}^{T-2}$

A Random-Byte Fault Attack on SIMON: Case 2



A Random-Byte Fault Attack on SIMON: Case 2

$$y^{T} = (x_j^{T-2} \,\&\, x_{(j-7)\%n}^{T-2}) \oplus RemainingTerms$$
$$y^{T^*} = ((x_j^{T-2} \oplus 1) \,\&\, x_{(j-7)\%n}^{T-2}) \oplus 1 \oplus RemainingTerms$$

x_j^{T-2}	$x_j^{T-2} \oplus 1$	$x_{(j-7)\%n}^{T-2}$	$(y^{T} \oplus y^{T^*})_{(j+1)\%n}$
0	1	0	1
1	0	0	1
0	1	1	0
1	0	1	0

Table: Secret Value $x_{(j-7)\%n}^{T-2}$ obtained from $(y^{T} \oplus y^{T^*})_{(j+1)\%n}$

Attack Complexity

Attack Complexity

- If the least and most significant bits of the byte fault having Hamming weight z are 1, then $2z - 2$ key bits are retrieved. There are 64 such faults.

Attack Complexity

- If the least and most significant bits of the byte fault having Hamming weight z are 1, then $2z - 2$ key bits are retrieved. There are 64 such faults.
- Otherwise a byte fault of Hamming weight z in x^{T-2} retrieves $2z$ bits of the last round key k^{T-1}. The number of possible byte faults having Hamming weight z is $\binom{8}{z}$.

Attack Complexity

- If the least and most significant bits of the byte fault having Hamming weight z are 1, then $2z - 2$ key bits are retrieved. There are 64 such faults.
- Otherwise a byte fault of Hamming weight z in x^{T-2} retrieves $2z$ bits of the last round key k^{T-1}. The number of possible byte faults having Hamming weight z is $\binom{8}{z}$.
- Therefore, the expected number of key bits that can be retrieved by a random byte fault is:

$$\frac{1}{255} * \left(\left(\sum_{z=1}^{8} 2z * \binom{8}{z} \right) - 128 \right) \approx 8$$

Attack Complexity

- If the least and most significant bits of the byte fault having Hamming weight z are 1, then $2z - 2$ key bits are retrieved. There are 64 such faults.
- Otherwise a byte fault of Hamming weight z in x^{T-2} retrieves $2z$ bits of the last round key k^{T-1}. The number of possible byte faults having Hamming weight z is $\binom{8}{z}$.
- Therefore, the expected number of key bits that can be retrieved by a random byte fault is:

$$\frac{1}{255} * \left(\left(\sum_{z=1}^{8} 2z * \binom{8}{z} \right) - 128 \right) \approx 8$$

- Hence $(n/8)$ byte faults required to recover n bit secret key

Simulation Results

n bits	k^{T-1}	Avg. No. of Faulty Encryptions
16	0xfa 0x24	6
24	0x26 0x53 0xaf	9
32	0x87 0x46 0x09 0x1a	13
48	0x22 0x4d 0xe9 0xcf 0x51 0xdd	21
64	0x19 0x26 0x5a 0xc7 0x4f 0xf2 0x90 0x01	30

Table: Random Byte Fault Attack on SIMON Assuming no Control Over the Fault Position

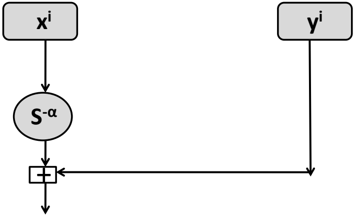
Fault Attack on SPECK

Round Function of SPECK cipher

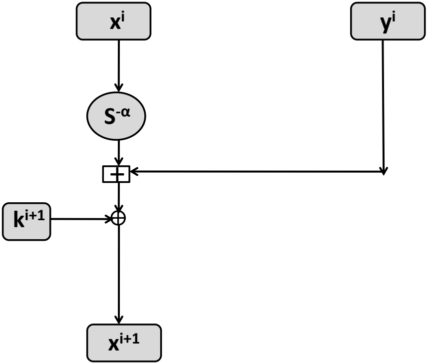
Round Function of SPECK cipher

$S^{-\alpha}x$: Circular right shift of x by α bits

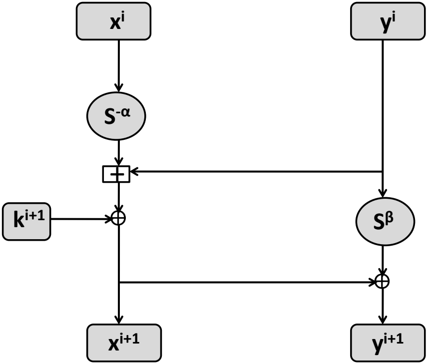
Round Function of SPECK cipher



Round Function of SPECK cipher

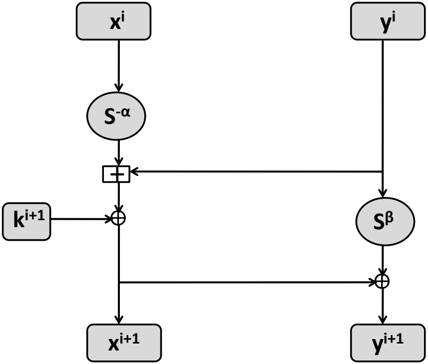


Round Function of SPECK cipher



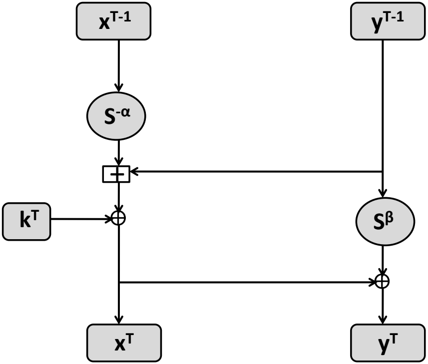
$S^{\beta}y$: Circular left shift of y by β bits

Round Function of SPECK cipher

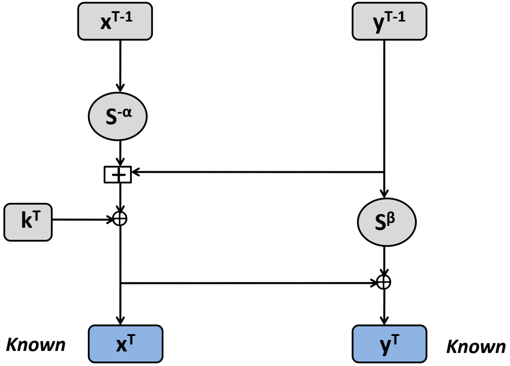


$$(x^{i+1}, y^{i+1}) = ((S^{-\alpha}x^i + y^i) \oplus k^{i+1}, S^{\beta}y^i \oplus x^{i+1}), i \in \{0, \dots, T-1\}$$

Equation of Last Round Key

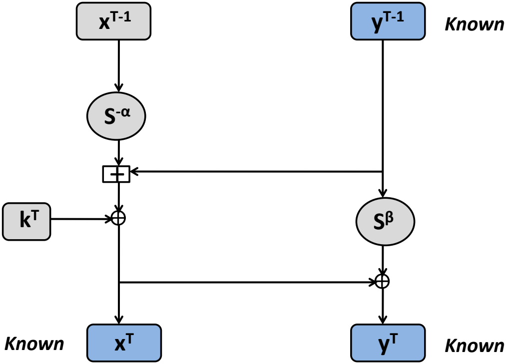


Equation of Last Round Key



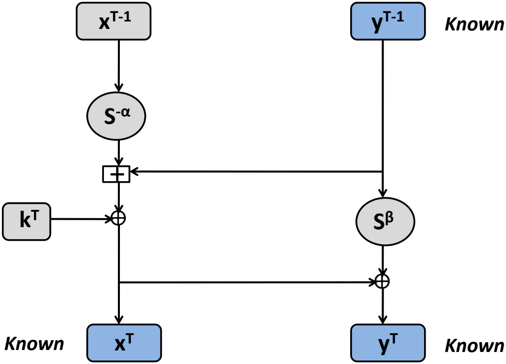
(x^T, y^T): Correct Ciphertext

Equation of Last Round Key



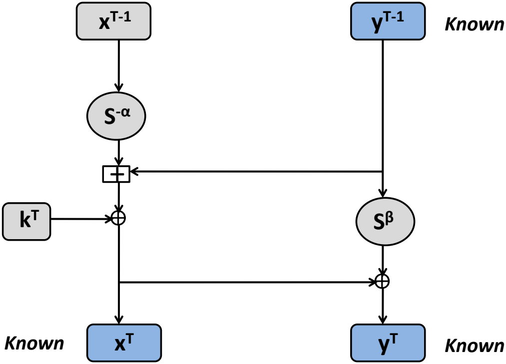
$$y^{T-1} = x^{T} \oplus S^{-\beta}(y^{T})$$

Equation of Last Round Key



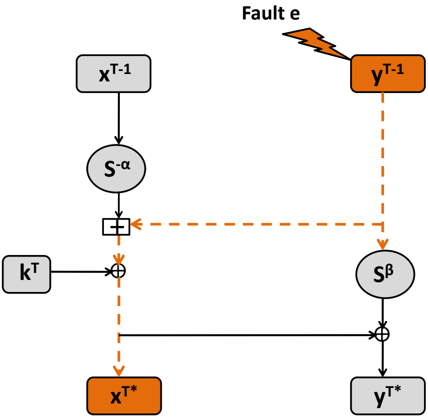
$$k^T = (S^{-\alpha}x^{T-1} + S^{-\beta}(y^T \oplus x^T)) \oplus x^T$$

Equation of Last Round Key



$$k_j^T = (x_{j+\alpha}^{T-1} \oplus (y^T \oplus x^T)_j \oplus c_j) \oplus x_j^T$$

Fault Injection in the Target Round



(x^{T^*}, y^{T^*}): Faulty Ciphertext

Determining Fault Position and Value

Using Correct Ciphertext:

$$y^{T-1} = S^{-\beta}(y^{T} \oplus x^{T}) \tag{3}$$

Determining Fault Position and Value

Using Correct Ciphertext:

$$y^{T-1} = S^{-\beta}(y^T \oplus x^T) \tag{3}$$

Using Faulty Ciphertext:

$$\begin{aligned} y^{(T-1)^*} &= S^{-\beta}(y^{T^*} \oplus x^{T^*}) \\ y^{(T-1)} \oplus e &= S^{-\beta}(y^{T^*} \oplus x^{T^*}) \end{aligned} \tag{4}$$

Determining Fault Position and Value

Using Correct Ciphertext:

$$y^{T-1} = S^{-\beta}(y^T \oplus x^T) \tag{3}$$

Using Faulty Ciphertext:

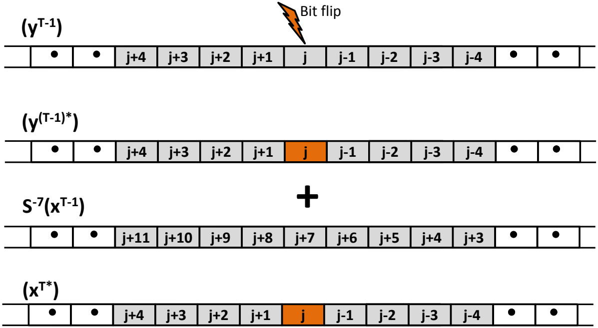
$$\begin{aligned} y^{(T-1)^*} &= S^{-\beta}(y^{T^*} \oplus x^{T^*}) \\ y^{(T-1)} \oplus e &= S^{-\beta}(y^{T^*} \oplus x^{T^*}) \end{aligned} \tag{4}$$

Using (3) and (4):

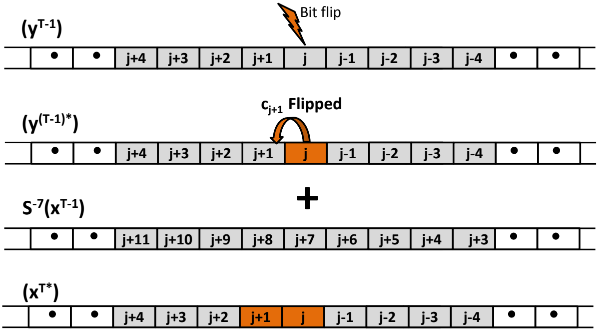
$$e = S^{-\beta}(y^T \oplus y^{T^*} \oplus x^T \oplus x^{T^*})$$

Hence, we know the flipped bit(s) of y^{T-1}

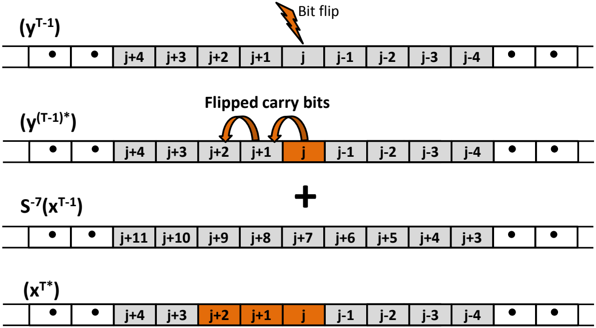
First Bit-Flip Fault Attack on SPECK



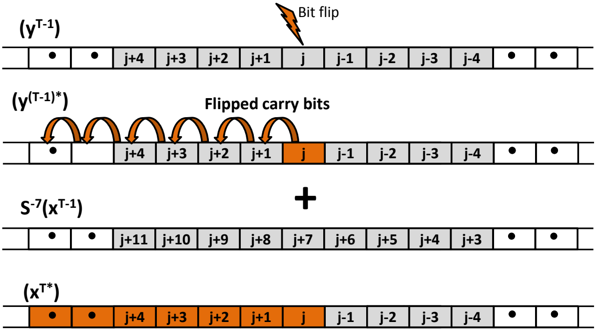
A Bit-Flip Fault Attack on SPECK



A Bit-Flip Fault Attack on SPECK



A Bit-Flip Fault Attack on SPECK



A Bit-Flip Fault Attack on SPECK

case 1 : $x_{j+\alpha} = c_j$

c_j	0	0
$x_{j+\alpha}$	0	0
y_j	0	1
$c_j + x_{j+\alpha} + y_j$	00	01

Table: Determining value of $x_{j+\alpha}$

A Bit-Flip Fault Attack on SPECK

case 1 : $x_{j+\alpha} = c_j$

c_j	1	1
$x_{j+\alpha}$	1	1
y_j	0	1
$c_j + x_{j+\alpha} + y_j$	10	11

Table: Determining value of $x_{j+\alpha}$

A Bit-Flip Fault Attack on SPECK

case 1 : $x_{j+\alpha} = c_j$

c_j	0	0	1	1
$x_{j+\alpha}$	0	0	1	1
y_j	0	1	0	1
$c_j + x_{j+\alpha} + y_j$	00	01	10	11

Table: Determining value of $x_{j+\alpha}$

A Bit-Flip Fault Attack on SPECK

case 2 : $x_{j+\alpha} \neq c_j$

c_j	1	1
$x_{j+\alpha}$	0	0
y_j	0	1
$c_j + x_{j+\alpha} + y_j$	01	10

Table: Determining value of $x_{j+\alpha}$

A Bit-Flip Fault Attack on SPECK

case 2 : $x_{j+\alpha} \neq c_j$

c_j	0	0
$x_{j+\alpha}$	1	1
y_j	0	1
$c_j + x_{j+\alpha} + y_j$	01	10

Table: Determining value of $x_{j+\alpha}$

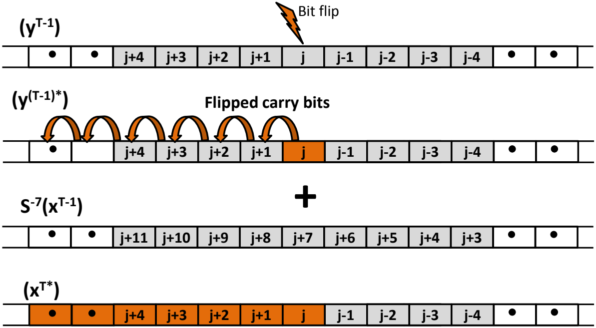
A Bit-Flip Fault Attack on SPECK

case 2 : $x_{j+\alpha} \neq c_j$

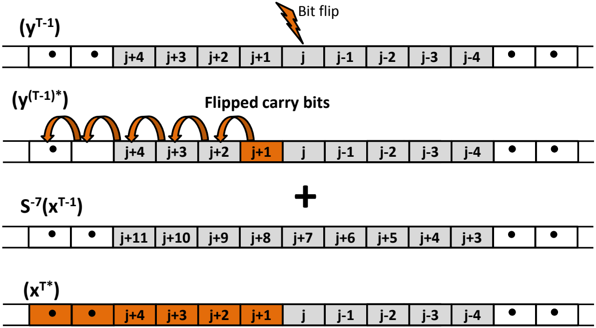
c_j	1	1	0	0
$x_{j+\alpha}$	0	0	1	1
y_j	0	1	0	1
$c_j + x_{j+\alpha} + y_j$	01	10	01	10

Table: Determining value of $x_{j+\alpha}$

A Bit-Flip Fault Attack on SPECK



A Bit-Flip Fault Attack on SPECK



Attack Complexity

Attack Complexity

- The probability of obtaining l more bits of x^{T-1} is equal to the probability of l carry bits getting flipped due to a single bit flip in y^{T-1}.

Attack Complexity

- The probability of obtaining l more bits of x^{T-1} is equal to the probability of l carry bits getting flipped due to a single bit flip in y^{T-1}.
- For l^{th} carry bit to be flipped all the lower $(l-1)$ carry bits should also be flipped. The probability of this event is $1/2^l$.

Attack Complexity

- The probability of obtaining l more bits of x^{T-1} is equal to the probability of l carry bits getting flipped due to a single bit flip in y^{T-1}.
- For l^{th} carry bit to be flipped all the lower $(l-1)$ carry bits should also be flipped. The probability of this event is $1/2^l$.
- Therefore the expected number of bits of last round key that can be retrieved using a single bit-flip is:

$$1 + \sum_{t=1}^{l} t * Pr[t] = 1 + \sum_{t=1}^{l} t * \frac{1}{2^t} \approx 3$$

Attack Complexity

- The probability of obtaining l more bits of x^{T-1} is equal to the probability of l carry bits getting flipped due to a single bit flip in y^{T-1}.
- For l^{th} carry bit to be flipped all the lower $(l-1)$ carry bits should also be flipped. The probability of this event is $1/2^l$.
- Therefore the expected number of bits of last round key that can be retrieved using a single bit-flip is:

$$1 + \sum_{t=1}^{l} t * Pr[t] = 1 + \sum_{t=1}^{l} t * \frac{1}{2^t} \approx 3$$

- Hence the number of bit faults required to recover all the n bits of last round key k^T is $(n/3)$.

Simulation Results

n bits	k^{T-1}	Avg. No. of Faulty Encryptions
16	0xfa 0x24	18
24	0x26 0x53 0xaf	25
32	0x87 0x46 0x09 0x1a	44
48	0x22 0x4d 0xe9 0xcf 0x51 0xdd	85
64	0x19 0x26 0x5a 0xc7 0x4f 0xf2 0x90 0x01	114

Table: Bit-flip Fault Attack on SPECK Assuming no Control Over the Fault Position

Conclusion & Summary

1. Fault Attack Susceptibility: Latest ciphers such as SIMON and SPECK vulnerable to fault attacks.

Conclusion & Summary

1. Fault Attack Susceptibility: Latest ciphers such as SIMON and SPECK vulnerable to fault attacks.
2. SIMON can be broken using (n/2) faults using a bit-flip fault model and (n/8) faulty ciphertexts using a random byte fault model.

Conclusion & Summary

1. Fault Attack Susceptibility: Latest ciphers such as SIMON and SPECK vulnerable to fault attacks.
2. SIMON can be broken using (n/2) faults using a bit-flip fault model and (n/8) faulty ciphertexts using a random byte fault model.
3. Using a bit-flip fault model, SPECK can be broken using (n/3) bit faults.

Thank You!

References

1. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. Available at http://eprint.iacr.org/
2. H. A. Alkhzaimi and M. M. Lauridsen. Cryptanalysis of the SIMON Family of Block Ciphers. Cryptology ePrint Archive, Report 2013/543, 2013. Avaliable at http://eprint.iacr.org/
3. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential Cryptanalysis of Reduced-Round Simon. Cryptology ePrint Archive, Report 2013/526, 2013. Available at http://eprint.iacr.org/.
4. Javad Alizadeh, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar and Somitra Kumar Sanadhya. Linear Cryptanalysis of Round Reduced SIMON. IACR Cryptology eprint Archive, Report 2013/663, 2013. Available at http://eprint.iacr.org/2013/663

References

5. D.Boneh, R.A.DeMillo, and R.J.Lipton. On the Importance of Checking Cryptographic Protocols for Faults (ExtendedAbstract). In W. Fumy, editor, Advances in Cryptology - EUROCRYPT 97, volume 1233 of Lecture Notes in Computer Science, pages 37-51. Springer, 1997.