Known and Chosen Key Differential Distinguishers for Block Ciphers

Josef Pieprzyk
joint work with
Ivica Nikolić, Przemysław Sokołowski, and Ron Steinfeld

ASK 2011, August 29-31, 2011

Outline

Block Ciphers

SP Network

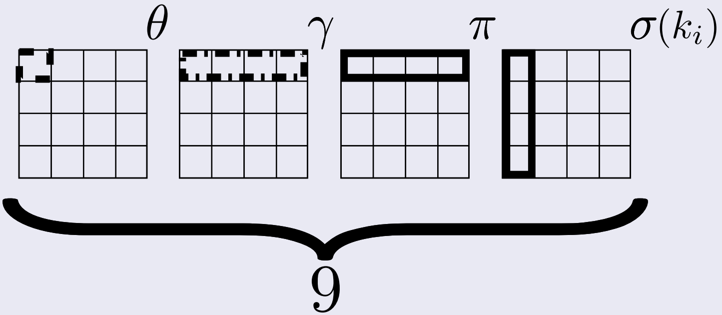
Our results are focused on **Substitution–Permutation Network** (SPN) based designs.

Block Ciphers

SP Network

Our results are focused on **Substitution–Permutation Network** (SPN) based designs.

Example: Square



Differential Distinguishers

Distinguisher for a cipher

A **Distinguisher** $\mathcal{D}$ for a block cipher is a randomized algorithm interacting with two primitives: an **Ideal Cipher** $\mathcal{IC}$ and **the analysed block cipher** E_K, and in polynomially bounded time decides which primitive is E_K, where K is an encryption key.

Differential Distinguishers

Distinguisher for a cipher

A **Distinguisher** $\mathcal{D}$ for a block cipher is a randomized algorithm interacting with two primitives: an **Ideal Cipher** $\mathcal{IC}$ and **the analysed block cipher** E_K, and in polynomially bounded time decides which primitive is E_K, where K is an encryption key.

Differential Distinguishers

Based on construction of differential trails $\Delta_P \to \Delta'$ for the block cipher E_K.

- **Standard Differential Distinguisher** — encryption key K is random,

Differential Distinguishers

Distinguisher for a cipher

A **Distinguisher** $\mathcal{D}$ for a block cipher is a randomized algorithm interacting with two primitives: an **Ideal Cipher** $\mathcal{IC}$ and **the analysed block cipher** E_K, and in polynomially bounded time decides which primitive is E_K, where K is an encryption key.

Differential Distinguishers

Based on construction of differential trails $\Delta_P \rightarrow \Delta'$ for the block cipher E_K.

- **Standard Differential Distinguisher** — encryption key K is random,
- **Open–key Differential Distinguishers** — encryption key K is known or chosen and we consider trails $(\Delta_P, \Delta_K) \rightarrow \Delta'$,

where $\Delta_P = P_1 \oplus P_2, \Delta_K = K_1 \oplus K_2$ for pairs of plain–texts P_1, P_2 and keys K_1, K_2 and $\Delta' = E_{K_1}(P_1) \oplus E_{K_2}(P_2)$.

Why Open–key Model For Block Cipher?

Cryptographic Hash Function

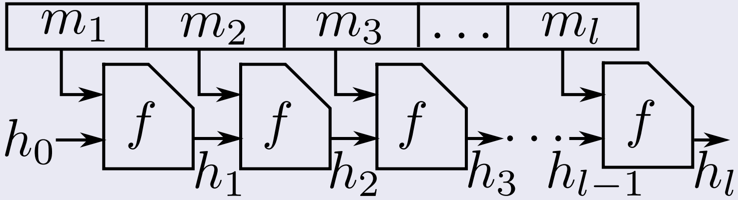
A **Cryptographic Hash Function** $F\colon \{0,1\}^* \to \{0,1\}^n$ is a transformation that maps arbitrary length input into fixed-length output and is designed to achieve certain security properties, such as: **preimage resistance**, **second preimage resistance**, **collision resistance**.

Why Open–key Model For Block Cipher?

Cryptographic Hash Function

A **Cryptographic Hash Function** $F\colon \{0,1\}^* \to \{0,1\}^n$ is a transformation that maps arbitrary length input into fixed-length output and is designed to achieve certain security properties, such as: **preimage resistance**, **second preimage resistance**, **collision resistance**.

Merkle-Damgård structure



Hash Modes

Single Block

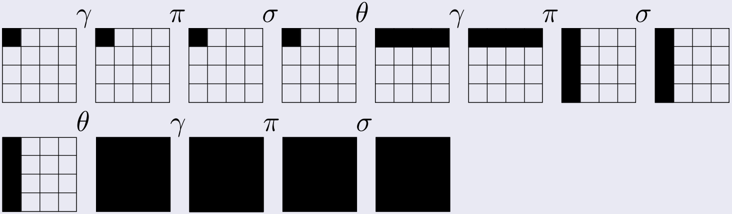
mode ($\imath$)	h'
1	$E_h(m) \oplus m$
2	$E_h(h \oplus m) \oplus h \oplus m$
3	$E_h(m) \oplus h \oplus m$
4	$E_h(h \oplus m) \oplus m$
5	$E_m(h) \oplus h$
6	$E_m(h \oplus m) \oplus h \oplus m$
7	$E_m(h) \oplus h \oplus m$
8	$E_m(h \oplus m) \oplus h$
9	$E_{h \oplus m}(m) \oplus m$
10	$E_{h \oplus m}(h) \oplus h$
11	$E_{h \oplus m}(m) \oplus h$
12	$E_{h \oplus m}(h) \oplus m$

Double Block

mode	(h', g')
A-DM	$h' = E_{g,m}(h) \oplus h$ $g' = E_{m,h}(\bar{g}) \oplus g$
T-DM	$h' = E_{g,m}(h) \oplus h$ $g' = E_{m,E_{g,m}(h)}(g) \oplus g$
DBL	$h' = E_{h\|m}(g \oplus c) \oplus g \oplus c$ $g' = E_{h\|m}(g) \oplus g$
MDC-2	$h' = (E_h(m) \oplus m)^L$ $\| (E_g(m) \oplus m)^R$ $g' = (E_g(m) \oplus m)^L$ $\| (E_h(m) \oplus m)^R$

Differential Trail

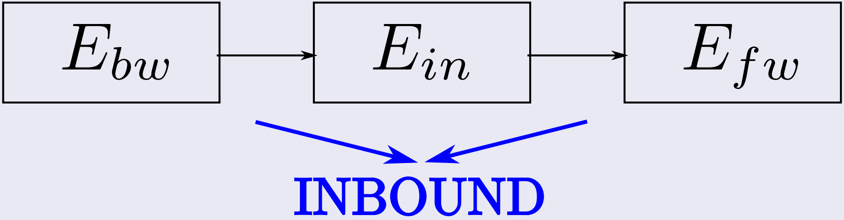
Example of a differential trail: Square



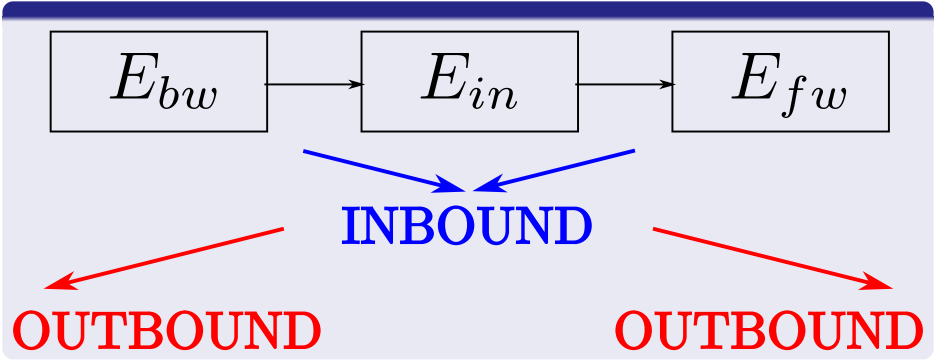
Rebound Attack

$$\boxed{E_{bw}} \longrightarrow \boxed{E_{in}} \longrightarrow \boxed{E_{fw}}$$

Rebound Attack



Rebound Attack

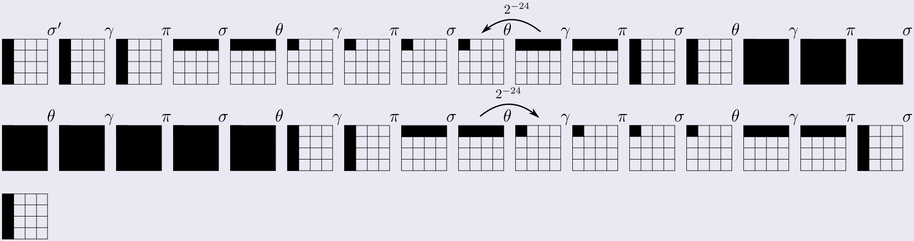


Results

Truncated differential trails

Crypton, Hierocript-3, Square

Example: Square



The total probability of the differential trail is 2^{-48}.

Results

Standard differential trail for 6.5 rounds of SAFER++ for chosen-key distinguisher and 128-bit key with probability 2^{-112}

2^{-14} 2^{-28} 2^{-28} 2^{-14} 2^{-28}

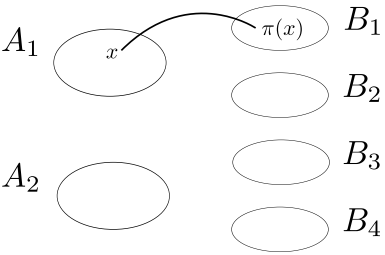
4-PHT S 4-PHT S 4-PHT S 4-PHT S 4-PHT S 4-PHT S 4-PHT Last subkey addition

					*	*			01	80			80	80
	01	80	80	*	*	*	*	ff						
			80	*	*	*					80	80	80	80
					*	*	*	01						
			80	*	*	*								
					*	*								
ff					*	*								
01					*	*								
					*	*	*	01					80	80
					*	*								
					*	*					80	80		
					*	*	*	ff					80	80
			80	*	*	*					80	80	80	80
01					*	*			ff	80	80	80	80	80
	ff	80			*	*							80	80
ff					*	*							80	80

Results

Lemma

Let D_I, D_O denote subsets of $\{0,1\}^n$, which are closed under $\oplus$, i.e. $x \oplus y \in D_I$ (respectively D_O) for $x, y \in D_I$ (resp. D_O). For any attacker making queries to a random n-bit permutation π and its inverse π^{-1}, the complexity (measured in expected number of oracle queries) of finding a pair of inputs (x, y), where $x \oplus y \in D_I, |D_I| = 2^{c_I}$, such that $\pi(x) \oplus \pi(y) \in D_O, |D_O| = 2^{c_O}$, is lower bounded as $Q \geq \min(2^{\frac{n}{2}-2}, 2^{n-(c_I+c_O)-3})$.

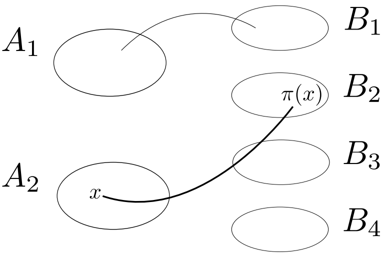


$|A_1| = |A_2| = |D_I|$
$|B_1| = |B_2| = |B_3| = |B_4| = |D_O|$
$A_1 \cup A_2 = B_1 \cup \cdots \cup B_4 = \{0,1\}^n$

Results

Lemma

Let D_I, D_O denote subsets of $\{0,1\}^n$, which are closed under $\oplus$, i.e. $x \oplus y \in D_I$ (respectively D_O) for $x, y \in D_I$ (resp. D_O). For any attacker making queries to a random n-bit permutation π and its inverse π^{-1}, the complexity (measured in expected number of oracle queries) of finding a pair of inputs (x, y), where $x \oplus y \in D_I, |D_I| = 2^{c_I}$, such that $\pi(x) \oplus \pi(y) \in D_O, |D_O| = 2^{c_O}$, is lower bounded as $Q \geq \min(2^{\frac{n}{2}-2}, 2^{n-(c_I+c_O)-3})$.

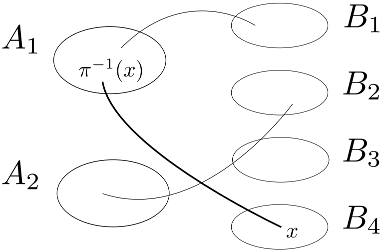


$|A_1| = |A_2| = |D_I|$
$|B_1| = |B_2| = |B_3| = |B_4| = |D_O|$
$A_1 \cup A_2 = B_1 \cup \cdots \cup B_4 = \{0,1\}^n$

Results

Lemma

Let D_I, D_O denote subsets of $\{0,1\}^n$, which are closed under $\oplus$, i.e. $x \oplus y \in D_I$ (respectively D_O) for $x, y \in D_I$ (resp. D_O). For any attacker making queries to a random n-bit permutation π and its inverse π^{-1}, the complexity (measured in expected number of oracle queries) of finding a pair of inputs (x, y), where $x \oplus y \in D_I, |D_I| = 2^{c_I}$, such that $\pi(x) \oplus \pi(y) \in D_O, |D_O| = 2^{c_O}$, is lower bounded as $Q \geq \min(2^{\frac{n}{2}-2}, 2^{n-(c_I+c_O)-3})$.

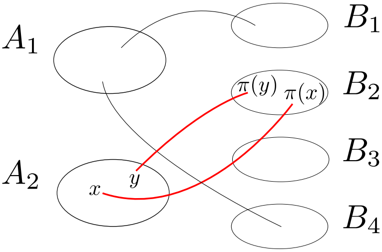


$|A_1| = |A_2| = |D_I|$
$|B_1| = |B_2| = |B_3| = |B_4| = |D_O|$
$A_1 \cup A_2 = B_1 \cup \cdots \cup B_4 = \{0,1\}^n$

Results

Lemma

Let D_I, D_O denote subsets of $\{0,1\}^n$, which are closed under $\oplus$, i.e. $x \oplus y \in D_I$ (respectively D_O) for $x, y \in D_I$ (resp. D_O). For any attacker making queries to a random n-bit permutation π and its inverse π^{-1}, the complexity (measured in expected number of oracle queries) of finding a pair of inputs (x, y), where $x \oplus y \in D_I, |D_I| = 2^{c_I}$, such that $\pi(x) \oplus \pi(y) \in D_O, |D_O| = 2^{c_O}$, is lower bounded as $Q \geq \min(2^{\frac{n}{2}-2}, 2^{n-(c_I+c_O)-3})$.



$|A_1| = |A_2| = |D_I|$
$|B_1| = |B_2| = |B_3| = |B_4| = |D_O|$
$A_1 \cup A_2 = B_1 \cup \cdots \cup B_4 = \{0,1\}^n$

Results

Cipher	Distinguisher	Rounds	Encryptions	Lower bound
Crypton	Known-key	7	2^{48}	2^{61}
	Chosen-key	9	2^{48}	2^{61}
Hierocrypt-3	Known-key	3.5	2^{48}	2^{61}
	Chosen-key	4.5	2^{48}	2^{61}
SAFER++	Known-key	6.5	2^{120}	2^{128}
	Chosen-key	6.5	2^{112}	2^{128}
Square	Known-key	7	2^{48}	2^{61}
	Chosen-key	8	2^{48}	2^{61}
n-bit Feistel with k-bit key	Diff. attack	r	2^c	
	Known-key	$r+2$	2^c	
	Chosen-key	$r+\lfloor\frac{2k}{n}\rfloor$	2^c	

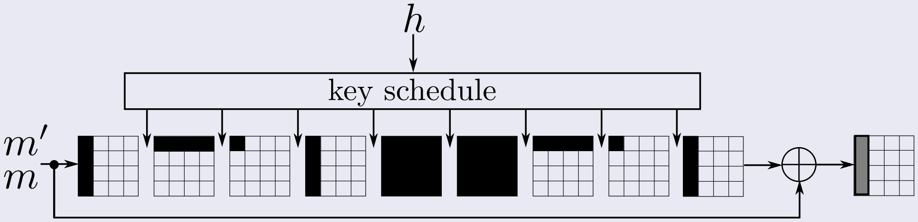
Cryptographic Hash Function

Collisions

1. **Collisions –** for a fixed chaining value H_0, the adversary tries to find two distinct messages M_1, M_2 such that $f(H_0, M_1) = f(H_0, M_2)$.
2. **Pseudo collisions –** for a message M, the adversary wishes to find two distinct chaining values H_1, H_2 such that $f(H_1, M) = f(H_2, M)$.
3. **Semi-free start collisions –** the adversary attempts to find two distinct messages M_1, M_2 and a chaining value H such that $f(H, M_1) = f(H, M_2)$.
4. **Free start collisions –** the adversary tries to find two distinct chaining values H_1, H_2, and two distinct messages M_1, M_2 such that $f(H_1, M_1) = f(H_2, M_2)$.

Semi–Free Start Collision For $E_h(m) \oplus m$

Example: Square



Results: Hash Modes

mode ($\imath$)	h'	plain–text	key	plain–text and key
1	$E_h(m) \oplus m$	C, SFSC	PC[a]	FSC
2	$E_h(h \oplus m) \oplus h \oplus m$	C, SFSC	PC	PC, FSC
3	$E_h(m) \oplus h \oplus m$	C, SFSC	PC	FSC
4	$E_h(h \oplus m) \oplus m$	C, SFSC	PC	PC, FSC
5	$E_m(h) \oplus h$	PC	C[a], SFSC[a]	FSC
6	$E_m(h \oplus m) \oplus h \oplus m$	PC	FSC	C, SFSC, FSC
7	$E_m(h) \oplus h \oplus m$	PC	C, SFSC	FSC
8	$E_m(h \oplus m) \oplus h$	PC	FSC	C, SFSC, FSC
9	$E_{h \oplus m}(m) \oplus m$	FSC	PC[a]	C, SFSC, FSC
10	$E_{h \oplus m}(h) \oplus h$	FSC	C[a], SFSC[a]	PC, FSC
11	$E_{h \oplus m}(m) \oplus h$	FSC	PC	C, SFSC, FSC
12	$E_{h \oplus m}(h) \oplus m$	FSC	C, SFSC	C, PC, FSC

[a] When key collisions exist in the cipher.

Results: Double Hash Modes

mode	(h', g')	plain–text	key	plain–text and key
A-DM	$h' = E_{g,m}(h) \oplus h$ $g' = E_{m,h}(\bar{g}) \oplus g$	FSC	C, SFSC	PC, FSC
T-DM	$h' = E_{g,m}(h) \oplus h$ $g' = E_{m,E_{g,m}(h)}(g) \oplus g$	FSC	C, SFSC	PC, FSC
DBL	$h' = E_{h\|m}(g \oplus c) \oplus g \oplus c$ $g' = E_{h\|m}(g) \oplus g$	PC	C, PC, SFSC, FSC	PC, FSC
MDC-2	$h' = (E_h(m) \oplus m)^L$ $\| (E_g(m) \oplus m)^R$ $g' = (E_g(m) \oplus m)^L$ $\| (E_h(m) \oplus m)^R$	C, SFSC	PC[a]	FSC

[a] When key collisions exist in the cipher.

Conclusions

Results

- We have presented differential distinguishers for Crypton, Hierocrypt-3, SAFER++, and Square,
- We have showed lower bound of constructing pair that follows a truncated trail in the case of a random permutation,
- We have examined the application of the differential trails in analysis of ciphers that are used for compression function constructions.

Open Problems

1. The area of open-key distinguishers is largely unexplored,
2. Finding similar distinguishers based on related-key differentials remains an open problem.

Questions