New Attacks against Reduced-Round Versions of IDEA

Pascal Junod

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

FSE'05 – Paris (France), February 23rd, 2005

Outline

Outline

The IDEA Block Cipher

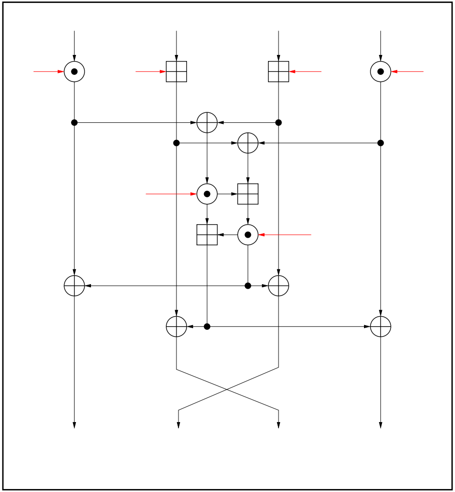
- $\longrightarrow$ Encrypts 64-bit blocks under a 128-bit key.
- $\longrightarrow$ Designed by Lai and Massey
- $\longrightarrow$ Tweak of PES (Proposed Encryption Standard)
- $\longrightarrow$ Design principles: mix three algebraically incompatible group operations
- $\longrightarrow$ Very popular cipher (still unbroken !!, building block of first versions of PGP)

The IDEA Block Cipher (2)

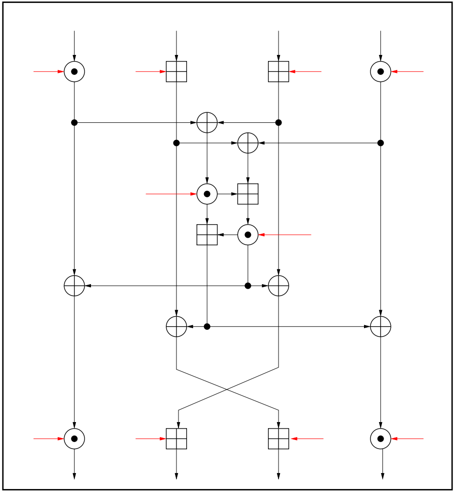
- Large cryptanalytical record (at least 10 papers from 1993 to 2004)
- Best attack: 5 rounds (out of 8.5) in $O(2^{126})$ operations and $O(2^{64})$ memory with help of 2^{24} chosen plaintexts by Demirci, Selçuk and Türe [SAC'03].
- Some papers break 8.5 rounds of IDEA, but the attacks work for a negligible portion of the keys.

Outline

A Round of IDEA



A Round of IDEA



IDEA operations

- $\longrightarrow$ Three group operations: $\oplus$, $\boxplus$, $\odot$
- $\longrightarrow$ $\oplus$: XOR on 16-bit values.
- $\longrightarrow$ $\boxplus$: addition modulo 2^{16}
- $\longrightarrow$ $\odot$: multiplication of $GF(2^{16}+1)^*$ (multiplication modulo $2^{16}+1$, where 0 is seen as 2^{16})

Full Cipher

- $\longrightarrow$ Full cipher made of 8.5 rounds
- $\longrightarrow$ Key-Schedule algorithm: produce 52 16-bit subkeys out of the 128-bit key
- $\longrightarrow$ Algorithm:
  - Partition Z into eight 16-bit blocks, and assign these blocks directly to the first eight subkeys.
  - Repeat the following until all remaining subkeys are assigned: rotate Z left 25 bits, partition the result, and assign these blocks to the next eight subkeys.

Key Schedule

Round r	$Z_1^{(r)}$	$Z_2^{(r)}$	$Z_3^{(r)}$	$Z_4^{(r)}$	$Z_5^{(r)}$	$Z_6^{(r)}$
1	$Z_{[0\ldots15]}$	$Z_{[16\ldots31]}$	$Z_{[32\ldots47]}$	$Z_{[48\ldots63]}$	$Z_{[64\ldots79]}$	$Z_{[80\ldots95]}$
2	$Z_{[96\ldots111]}$	$Z_{[112\ldots127]}$	$Z_{[25\ldots40]}$	$Z_{[41\ldots56]}$	$Z_{[57\ldots72]}$	$Z_{[73\ldots88]}$
3	$Z_{[89\ldots104]}$	$Z_{[105\ldots120]}$	$Z_{[121\ldots8]}$	$Z_{[9\ldots24]}$	$Z_{[50\ldots65]}$	$Z_{[66\ldots81]}$
4	$Z_{[82\ldots97]}$	$Z_{[98\ldots113]}$	$Z_{[114\ldots1]}$	$Z_{[2\ldots17]}$	$Z_{[18\ldots33]}$	$Z_{[34\ldots49]}$
5	$Z_{[75\ldots90]}$	$Z_{[91\ldots106]}$	$Z_{[107\ldots122]}$	$Z_{[123\ldots10]}$	$Z_{[11\ldots26]}$	$Z_{[27\ldots42]}$
6	$Z_{[43\ldots58]}$	$Z_{[59\ldots74]}$	$Z_{[100\ldots115]}$	$Z_{[116\ldots3]}$	$Z_{[4\ldots19]}$	$Z_{[20\ldots35]}$
7	$Z_{[36\ldots51]}$	$Z_{[52\ldots67]}$	$Z_{[68\ldots83]}$	$Z_{[84\ldots99]}$	$Z_{[125\ldots12]}$	$Z_{[13\ldots28]}$
8	$Z_{[29\ldots44]}$	$Z_{[45\ldots60]}$	$Z_{[61\ldots76]}$	$Z_{[77\ldots92]}$	$Z_{[93\ldots108]}$	$Z_{[109\ldots124]}$
8.5	$Z_{[22\ldots37]}$	$Z_{[38\ldots53]}$	$Z_{[54\ldots69]}$	$Z_{[70\ldots85]}$		

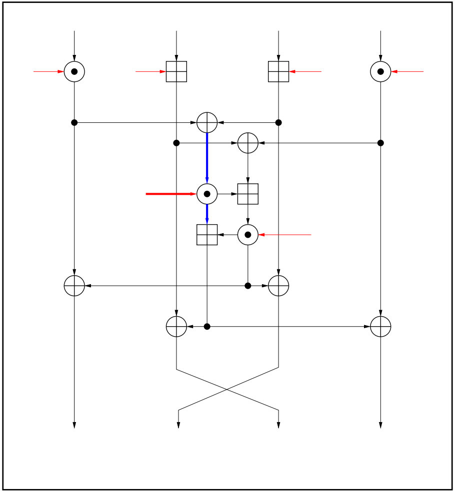
A First Observation

- $\longrightarrow$ $\alpha^{(r)}$ and $\beta^{(r)}$: two inputs of the MA-box
- $\longrightarrow$ $\gamma^{(r)}$ and $\delta^{(r)}$: two outputs of the MA-box
- $\longrightarrow$ Demirci, 2002: *For any round number* r,

$$\mathsf{lsb}\left(\gamma^{(r)} \oplus \delta^{(r)}\right) = \mathsf{lsb}\left(\alpha^{(r)} \odot Z_5^{(r)}\right)$$

where lsb(a) *denotes the least significant (rightmost) bit of* a.

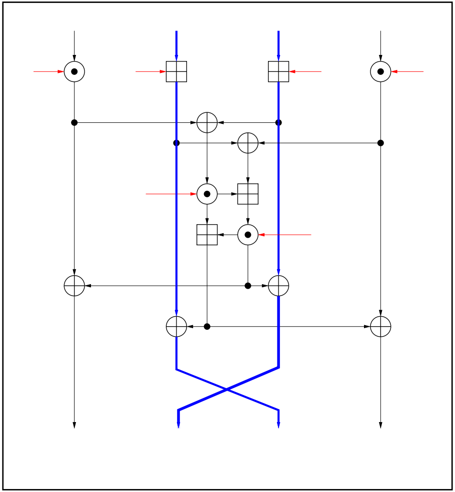
A First Observation (2)



A Second Observation

$\longrightarrow$ Biryukov: *The two middle words in a block are only combined, either with subkeys or internal cipher state, via two group operations which are linear in their least significant bit.*

A Second Observation (2)



The Biryukov-Demirci Relation

Nakahara *et al* (ACISP'04):

Theorem

For any number of rounds n in the IDEA block cipher, the following expression is true with probability one:

$$\mathrm{lsb}\left(\bigoplus_{i=1}^{n}\left(\gamma^{(i)} \oplus \delta^{(i)}\right) \oplus X_2^{(1)} \oplus X_3^{(1)} \oplus Y_2^{(n+1)} \oplus Y_3^{(n+1)}\right) = \mathrm{lsb}\left(\bigoplus_{j=1}^{n}\left(Z_2^{(j)} \oplus Z_3^{(j)}\right)\right)$$

Outline

Demirci-Biryukov Relation on 1.5-Round IDEA

→ Legend: known value / constant value / guessed value

$$\mathsf{lsb}\left(X_2^{(1)} \oplus X_3^{(1)} \oplus C_2^{(2)} \oplus C_3^{(2)} \oplus Z_2^{(1)} \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(2)} \oplus Z_5^{(1)} \odot \left(\left(X_1^{(1)} \odot Z_1^{(1)}\right) \oplus \left(X_3^{(1)} \boxplus Z_3^{(1)}\right)\right)\right) = 0$$

Demirci-Biryukov Relation on 1.5-Round IDEA

→ Legend: known value / constant value / guessed value

$$\mathsf{lsb}\left(X_2^{(1)} \oplus X_3^{(1)} \oplus C_2^{(2)} \oplus C_3^{(2)} \oplus Z_2^{(1)} \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(2)} \oplus Z_5^{(1)} \odot \left(\left(X_1^{(1)} \odot Z_1^{(1)}\right) \oplus \left(X_3^{(1)} \boxplus Z_3^{(1)}\right)\right)\right) = 0$$

Demirci-Biryukov Relation on 1.5-Round IDEA

→ Legend: known value / constant value / guessed value

$$\mathsf{lsb}\left(X_2^{(1)} \oplus X_3^{(1)} \oplus C_2^{(2)} \oplus C_3^{(2)} \oplus Z_2^{(1)} \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(2)} \oplus Z_5^{(1)} \odot \left(\left(X_1^{(1)} \odot Z_1^{(1)}\right) \oplus \left(X_3^{(1)} \boxplus Z_3^{(1)}\right)\right)\right) = 0$$

Demirci-Biryukov Relation on 1.5-Round IDEA

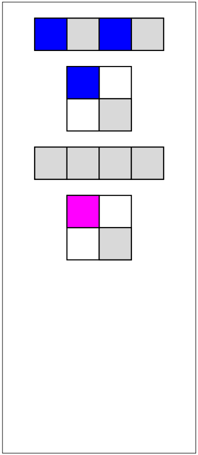
- $\longrightarrow$ Allows to get two 48-bit subkey candidates in less than $O(2^{50})$ operations using 55 known plaintexts.
- $\longrightarrow$ First trick: apply the Demirci-Biryukov relation in the decryption direction (à la Matsui)
- $\longrightarrow$ Allows to recover 48 other bits within the same complexity
- $\longrightarrow$ Other 32 unknown key bits: exhaustive search

Outline

Simple Chosen-Plaintext Attacks

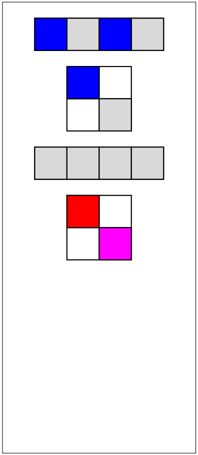
- $\longrightarrow$ Second trick: fix $X_1^{(1)}$ and $X_3^{(1)}$ to an arbitrary constant (à la Knudsen-Mathiassen).
- $\longrightarrow$ Guess appropriate subkeys and check the candidates with respect to the Demirci-Biryukov relation.

Simple Chosen-Plaintext Attacks (2)



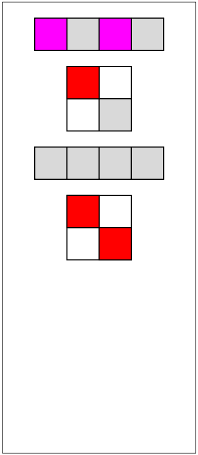
known value / constant value / guessed value

Simple Chosen-Plaintext Attacks (2)



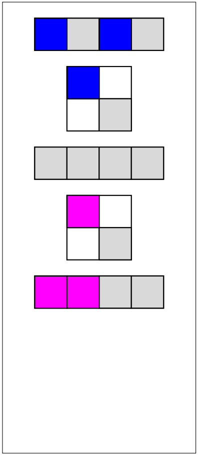
known value / constant value / guessed value

Simple Chosen-Plaintext Attacks (2)



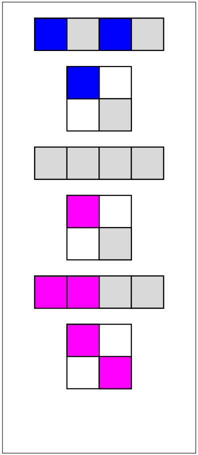
known value / constant value / guessed value

Simple Chosen-Plaintext Attacks (2)



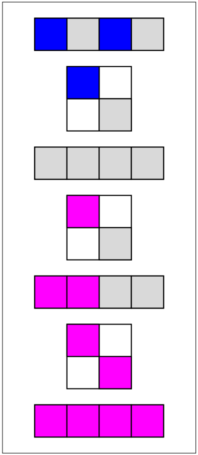
known value / constant value / guessed value

Simple Chosen-Plaintext Attacks (2)



known value / constant value / guessed value

Simple Chosen-Plaintext Attacks (2)



known value / constant value / guessed value

Outline

Time-Memory Tradeoff

- Trading time and memory allows to relax a chosen-plaintext oracle.
- Idea: for all possible values of $Z_1^{(1)}$, $Z_3^{(1)}$, and $Z_5^{(1)}$, compute the partial value of the Demirci-Biryukov relation. Store these values in a table.
- Guess the appropriate subkeys and partially decrypt a small set of known plaintext-ciphertext pairs until a match is found.

Outline

New Square-Like Distinguisher

Theorem (Square-Like Distinguisher on 2.5-Round IDEA)

Let 2^{16} different inputs of 2.5-round IDEA be defined as follows: $X_1^{(1)}$, $X_2^{(1)}$, and $X_3^{(1)}$ are fixed to arbitrary constants, and $X_4^{(1)}$ takes all possible values. Then the XOR of the 2^{16} values of the equation

$$\mathrm{lsb}\left(X_2^{(1)} \oplus X_3^{(1)} \oplus C_2^{(1)} \oplus C_3^{(1)} \oplus \right.$$
$$\left. Z_2^{(1)} \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_3^{(3)}\right) \oplus$$
$$\mathrm{lsb}\left(\gamma^{(1)} \oplus \delta^{(1)}\right) \oplus \mathrm{lsb}\left(\gamma^{(2)} \oplus \delta^{(2)}\right)$$

is equal to 0 with probability one.

New Square-Like Distinguisher (2)

- Idea: use a few saturated structures and mount the same type of attacks.
- Allows to attack up to 4 rounds

Complexities (2 rounds)

Rounds	Data	Time	Attack type	Ref.	Note
2	2^{10} CP	2^{42}	differential	[Meier, 1993]	
2	62 CP	2^{34}	*linear-like*	*this paper*	
2	23 CP	2^{64}	square-like	[Demirci, 2002]	

Complexities (2.5 rounds)

Rounds	Data	Time	Attack type	Ref.	Note
2.5	2^{10} CP	2^{106}	differential	[Meier, 1993]	Memory: 2^{96}
2.5	2^{10} CP	2^{32}	differential	[Daemen *et al*, 1993]	For one key out of 2^{77}
2.5	2^{18} CP	2^{58}	square	[Nakahara *et al*, 2002]	
2.5	2^{32} CP	2^{59}	square	[Nakahara *et al*, 2002]	
2.5	2^{48} CP	2^{79}	square	[Nakahara *et al*, 2002]	
2.5	2 CP	2^{37}	square	[Nakahara *et al*, 2002]	Under 2^{16} rel. keys
2.5	55 CP	2^{81}	square-like	[Demirci, 2002]	
2.5	101 CP	2^{48}	*linear-like*	*this paper*	
2.5	97 KP	2^{90}	linear-like	[Nakahara *et al*, 2003]	
2.5	55 KP	2^{54}	*linear-like*	*this paper*	*Memory:* 2^{48}

Complexities (3 rounds)

Rounds	Data	Time	Attack type	Ref.	Note
3	2^{29} CP	2^{44}	differential-linear	[Borst *et al*, 1997]	
3	71 CP	2^{71}	square-like	[Demirci, 2002]	
3	71 CP	2^{64}	*linear-like*	*this paper*	
3	2^{33} CP	2^{64}	collision	[Demirci *et al*, 2003]	Memory: 2^{64}
3	2^{33} CP	2^{50}	combination of attacks	*this paper + [Demirci, 2002]*	
3	2^{22} CP	2^{50}	*square-like*	*this paper*	
3	71 KP	2^{70}	*linear-like*	*this paper*	*Memory: 2^{48}*

Complexities (3.5 rounds)

Rounds	Data	Time	Attack type	Ref.	Note
3.5	2^{56} CP	2^{67}	truncated diff.	[Borst *et al*, 1997]	
3.5	$2^{38.5}$ CP	2^{53}	impossible diff.	[Biham *et al*, 1999]	Memory: 2^{48}
3.5	2^{34} CP	2^{82}	square-like	[Demirci, 2002]	
3.5	2^{24} CP	2^{73}	collision	[Demirci *et al*, 2003]	
3.5	2^{22} CP	2^{66}	*square-like*	*this paper*	
3.5	103 CP	2^{103}	square-like	[Demirci, 2002]	
3.5	103 CP	2^{97}	*linear-like*	*this paper*	
3.5	119 KP	2^{112}	linear-like	[Nakahara *et al*, 2003]	
3.5	103 KP	2^{97}	*linear-like*	*this paper*	*Memory:* 2^{48}

Complexities (4 rounds)

Rounds	Data	Time	Attack type	Ref.	Note
4	2^{37} CP	2^{70}	impossible diff.	[Biham *et al*, 1999]	Memory: 2^{48}
4	2^{34} CP	2^{114}	square-like	[Demirci, 2002]	
4	2^{24} CP	2^{89}	collision	[Demirci *et al*, 2003	Memory: 2^{64}
4	2^{23} CP	2^{98}	*square-like*	*this paper*	
4	121 KP	2^{114}	linear-like	[Nakahara *et al*, 2003]	

Complexities (4.5 and 5 rounds)

Rounds	Data	Time	Attack type	Ref.	Note
4.5	2^{64} CP	2^{112}	impossible diff.	[Biham *et al*, 1999]	
4.5	2^{24} CP	2^{121}	collision	[Demirci *et al*, 2003]	Memory: 2^{64}
5	2^{24} CP	2^{126}	collision	[Demirci *et al*, 2003]	Memory: 2^{64}

Thank You!