New Cryptanalytic Results on IDEA

Eli Biham, Orr Dunkelman, Nathan Keller

Computer Science Dept., Technion
Dept. of Electrical Engineering ESAT-SCD/COSIC, KUL
Einstein Institute of Mathematics, Hebrew University

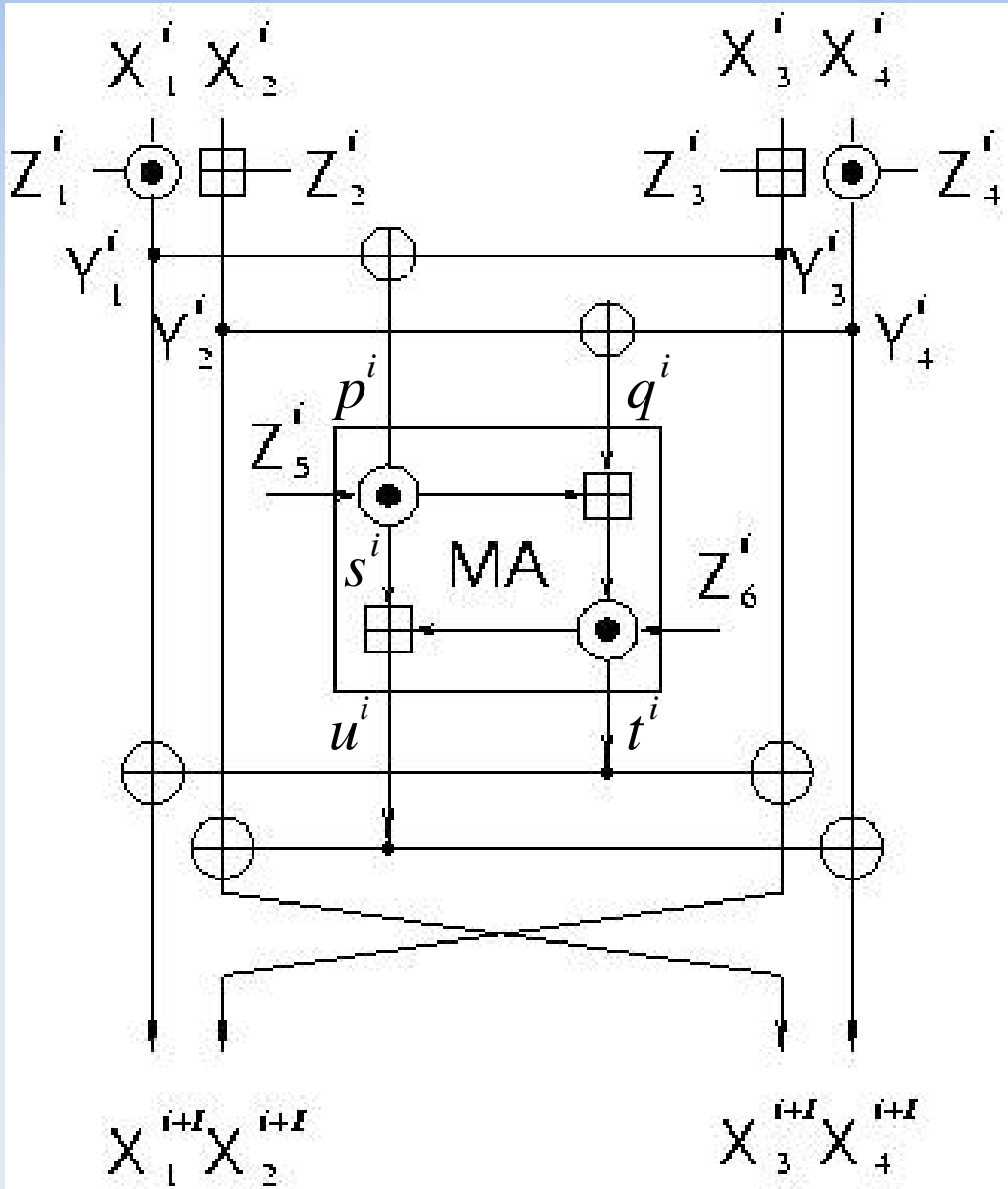
KATHOLIEKE UNIVERSITEIT LEUVEN

IDEA

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications

- A "red cape" for cryptanalysts – 15 years later – best attack is on 5/8.5 rounds (before our results)

IDEA's Round Function



Past Cryptanalytic Attempts

Attack	*Rounds*	*Complexity*	
		Data	*Time*
Differential [$M93$]	2.5	2^{10} CP	2^{106}
Differential-Linear [$BKR97$]	3	2^{29} CP	2^{44}
Linear [$NPV04$]	4	114 KP	2^{114}
Square [$J05$]	4	2^{23} CP	2^{98}
Impossible Differential [$BBS99$]	4.5	2^{64} CP	2^{112}
Meet in the Middle [$AS06$]	5	$2^{24.6}$ CP	2^{125}

Related-Key Attacks on IDEA

Related-Key Attack	*Rounds*	*Keys*	*Complexity*	
		Data	*Time*	
Rectangle [*BDK*05]	6.5	4	$2^{59.8}$ *CP*	$2^{88.1}$

Differential Cryptanalysis

- Introduced by Biham and Shamir in **1990**
- Studies the development of differences through the encryption function
- A differential $\alpha \rightarrow \beta$ with probability p predicts that two plaintexts $(P_1, P_2 = P_1 \oplus \alpha)$ are encrypted to $(C_1, C_2 = C_1 \oplus \beta)$ with probability p
- Requires $O(p^{-1})$ chosen plaintexts

DC and IDEA

- XOR-differences propagate well through XORs
- Some XOR-differences propagate well through addition (with low haming weight, in most significant bits, etc.)
- They do pass multiplication with probability different than for a random 16-bit to 16-bit transformation.

DC and IDEA (2)

- Additive-differences propagate well through Additions
- Some additive-differences propagate well through XOR (with low haming weight, in most significant bits, etc.)
- They do pass multiplication with probability different than for a random 16-bit to 16-bit transformation. (due to the unknown keys)

DC and IDEA (3) [B+02]

- Multiplicative-differences propagate well through multiplication
- Some multiplicative-differences propagate well through XOR (mostly ± 1)
- They do pass addition with probability different than for a random 16-bit to 16-bit transformation.

Linear Cryptanalysis

- Introduced by Matsui in **1993**
- Studies linear approximations of the encryption function
- A linear approximation $\lambda_P \rightarrow \lambda_C$ with probability $1/2 + q$: $\lambda_P \cdot P \oplus \lambda_C \cdot C = \lambda_K \cdot K$ for $1/2 + q$ of the pairs (P, C)
- The sign of the bias q is less important
- Requires about $O(q^{-2})$ known plaintexts

LC and IDEA

- Linear approximations propagate well through XORs
- Some approximations propagate well through addition (with low hamming weight, in least significant bits, etc.)
- They do pass multiplication with bias different than for a random 16-bit to 16-bit transformation.

Partial Solution

- As for most of differential and linear attacks, the multiplication is very problematic
- Observation **1**: multiplication by **1** is linear
- Observation **2**: multiplication by **0 (-1)** is also linear
- So let's consider cases where the key is **0/1**, leading to a linear multiplication!

Weak Key Classes of IDEA

Attack	*Keys*	*Complexity*	
		Data	*Time*
Linear $[DGV93]$	2^{23}	$8\ KP$	1
Higher-Order Differential-Linear $[BDK05]$			
	2^{32}	$2^{19}\ KP$	2^{19}
Differential $[DGV93]$	2^{51}	$2\ CP$	2^{12}
Differential-Linear $[H98]$	2^{63}	$20\ CP$	4
Boomerang $[BNVP02]$	2^{64}	$2^{16}\ ACPC$	2^{16}

The SQUARE Attack

- Introduced by Daemen, Knudsen and Rijmen in **1997**
- Other names: the saturation attack, the multi-set attack, integral cryptanalysis
- Studies the developing encryption of a structured set of plaintexts
  - For example, consider a set of **256** plaintexts which have the same first **15** bytes and obtain all possible values for the last byte
  - After two rounds of AES, for each of the **16** bytes, each value is achieved once by some ciphertext (though the relation between the various bytes is not necessarily known)

IDEA^2

- Due to the multiplication, the smallest set that can be used in most of the cases composes of at least one saturated word
- After **1.5-2** rounds, these properties arrive to the point where they do not predict too much
- For example: (C,C,C,P) -> (P,P,P,B) -> (?,?,?,?) such that the XOR of the first and second words (or the third and fourth) is balanced

Impossible Differentials

- Introduced by Biham, Biryukov, and Shamir in **1999**
- The main idea is to use differentials that are never satisifed
- In the case of IDEA these impossible differentials are constructed using a miss-in-the-middle approach:
  - A first differential $\alpha \rightarrow \beta$ which holds with probability **1** is found
  - A second differential $\gamma \rightarrow \delta$ which holds with probability **1** is also found
  - If β is incompatible with γ, then $\alpha \not\rightarrow \delta$

Imp. Diff. of IDEA

- First differential starts before the MA layer with difference $(a, 0, a, 0)$
- This difference propagates into $(a, a, 0, 0) \rightarrow (c, d, 0, 0)$ (so after one round $(a, 0, a, 0) \rightarrow (c, d, 0, 0)$)
- The second differential ends after the MA layer with difference $(b, b, 0, 0)$
- This means that the difference before is $(b, 0, b, 0) \rightarrow (b, 0, b, 0) \rightarrow (e, 0, f, 0)$
- Thus, $(a, 0, a, 0) \not\rightarrow (b, b, 0, 0)$ for **2.5** rounds of IDEA

The DST Attack [DST03]

- A specially crafted set of plaintexts that succeed to "push" a "SQUARE property" one and a half rounds
- The special set can be used to suggest a sequence of values for $lsb(p^{(2)})$
- The sequence can be reconstructed (up to XOR of all values with a fixed bit) from considering the sequence of $lsb(X_2^2 \oplus X_3^2)$
- This sequence can be reproduced using some other relations (which we present later) of more rounds
- The attack was improved in [AS06]

Our Results

- Finding a non-trivial differential for the MA layer.
- Computing the probability for boomerang attacks for a few cases for the MA layer.
- Identifying a weakness in the key schedule algorithm, which combined with the Biryukov-Demirci relation lead to attack on **5**-round IDEA.
- In the related-key model this attack can be extended to **7.5**-round attack.
- Related-key rectangle attack on **7**-round IDEA.
- Finally – a **6**-round Higher-Order Differential-Linear attack.

A Non-Trivial Differential

- The input difference $(0, x)$ "eliminates" the first multiplication of the MA
- Thus, there is only one multiplication
- ... and if its output difference is 8000_x then the addition does not cause probability for the differential

$$(0, x) \overset{MA}{\rightarrow} (8000_x, 8000_x)$$

with probability 2^{-16}, under the assumption that either x is non-zero or that there is a difference in Z_6

"Boomerang Probability"

- The boomerang attack deals with two pairs that need to satisfy some differential together
- Thus, we are sometimes interested in the probability $\sum_{\beta} \Pr^2[\alpha \rightarrow \beta]$ for some input difference α
- This predicts the probability that two pairs with input difference α have the same output difference
- For the MA layer and the input difference $(0, x)$

  $$\sum_{\beta} \Pr^2[(0, x) \rightarrow \beta] = 2^{-23.72}$$

  under the assumption that either x is non-zero or that there is a difference in Z_6

The Biryukov-Demirci Relation

- Let $P = (P_1, P_2, P_3, P_4)$ be a plaintext, and $C = (C_1, C_2, C_3, C_4)$ be the corresponding ciphertext
- Then

$$(((((((((((((((((P_2 \boxplus Z_2^1) \oplus u^1) \boxplus Z_3^2) \oplus t^2) \boxplus Z_2^3) \oplus u^3) \boxplus Z_3^4) \oplus t^4) \boxplus Z_2^5) \oplus u^5) \boxplus Z_3^6) \oplus t^6) \boxplus Z_2^7) \oplus u^7) \boxplus Z_3^8) \oplus t^8) \boxplus Z_2^9) = C_2$$

- When considering only the LSB:

$$LSB(P_2 \oplus Z_2^1 \oplus u^1 \oplus Z_3^2 \oplus t^2 \oplus Z_2^3 \oplus u^3 \oplus Z_3^4 \oplus t^4 \oplus Z_2^5 \oplus u^5 \oplus Z_3^6 \oplus t^6 \oplus Z_2^7 \oplus u^7 \oplus Z_3^8 \oplus t^8 \oplus Z_2^9) = LSB(C_2)$$

The Biryukov-Demirci Relation

- The same is true for P_3 and C_3:

$$(((((((((((((((((P_3 \boxplus Z_3^1) \oplus t^1) \boxplus Z_2^2) \oplus u^2) \boxplus Z_3^3) \oplus t^3) \boxplus Z_2^4) \oplus u^4) \boxplus Z_3^5) \oplus t^5) \boxplus Z_2^6) \oplus u^6) \boxplus Z_3^7) \oplus t^7) \boxplus Z_2^8) \oplus u^8) \boxplus Z_3^9) = C_3$$

- When considering only the LSB:

$$LSB(P_3 \oplus Z_3^1 \oplus t^1 \oplus Z_2^2 \oplus u^2 \oplus Z_3^3 \oplus t^3 \oplus Z_2^4 \oplus u^4 \oplus Z_3^5 \oplus t^5 \oplus Z_2^6 \oplus u^6 \oplus Z_3^7 \oplus t^7 \oplus Z_2^8 \oplus u^8 \oplus Z_3^9) = LSB(C_3)$$

The Biryukov-Demirci Relation

- Combining the above two relations:

$$LSB(P_2 \oplus P_3 \oplus Z_2^1 \oplus Z_3^1 \oplus s^1 \oplus Z_2^2 \oplus Z_3^2 \oplus s^2 \oplus Z_2^3 \oplus Z_3^3 \oplus s^3$$
$$\oplus Z_2^4 \oplus Z_3^4 \oplus s^4 \oplus Z_2^5 \oplus Z_3^5 \oplus s^5 \oplus Z_2^6 \oplus Z_3^6 \oplus s^6 \oplus Z_2^7 \oplus Z_3^7$$
$$\oplus s^7 \oplus Z_2^8 \oplus Z_3^8 \oplus s^8 \oplus Z_2^9 \oplus Z_3^9) = LSB(C_2 \oplus C_3)$$

Our Observation

- When dealing with two plaintexts (P^1, P^2), then the Biryukov-Demirci relation becomes:

$$LSB(P_2^1 \oplus P_3^1 \oplus P_2^2 \oplus P_3^2 \oplus \Delta s^1 \oplus \Delta s^2 \oplus \Delta s^3 \oplus \Delta s^4 \oplus \Delta s^5 \oplus \Delta s^6 \oplus \Delta s^7 \oplus \Delta s^8) = LSB(C_2^1 \oplus C_3^1 \oplus C_2^2 \oplus C_3^2)$$

Distinguishing 2.5-Round IDEA

- For 2.5-round IDEA, the basic relation is reduced to:

$$LSB(P_2^1 \oplus P_3^1 \oplus P_2^2 \oplus P_3^2 \oplus \Delta s^1 \oplus \Delta s^2) = LSB(C_2^1 \oplus C_3^1 \oplus C_2^2 \oplus C_3^2)$$

- If P^1 and P^2 have difference (0,x) before the first MA, then $\Delta s^1 = 0$
- If C^1 and C^2 have difference (0,y) after the second MA, then $\Delta s^2 = 0$

Distinguishing 2.5-Round IDEA

- Take 2^{18} plaintexts of the form (A,x,B,y) where A and B are fixed values
- Search for pairs of ciphertexts with output difference (0,0,β,γ)
- If the relation

$$LSB(P_2^1 \oplus P_3^1 \oplus P_2^2 \oplus P_3^2) = LSB(C_2^1 \oplus C_3^1 \oplus C_2^2 \oplus C_3^2)$$

is satisfied for all such pairs - then this is 2.5-round IDEA!

Key Recovery for 3 Rounds

- Take 2^{19} plaintexts of the form (A,x,B,y)
- For each guess of the subkey for the last MA layer:
  - Partially decrypt all ciphertexts
  - Apply the 2.5-round distinguisher
  - If the distinguisher fails – try another subkey
- Data complexity: 2^{19} CP
- Time complexity: $2^{48.5}$ encryptions

The 5-Round Attack

- The attack starts before the MA layer of round **3**
- The attack uses the Biryukov-Demirci relation for rounds **4,5,6,7**, and the KA layer of round **8**:

$$LSB(P_2^1 \oplus P_3^1 \oplus P_2^2 \oplus P_3^2 \oplus \Delta s^4 \oplus \Delta s^5 \oplus \Delta s^6 \oplus \Delta s^7) = LSB(C_2^1 \oplus C_3^1 \oplus C_2^2 \oplus C_3^2)$$

- We need to obtain the four values

$$\Delta s^4, \Delta s^5, \Delta s^6, \Delta s^7$$

IDEA's Key Schedule

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 1$	0–15	16–31	32–47	48–63	64–79	80–95
$i = 2$	96–111	112–127	25–40	41–56	57–72	73–88
$i = 3$	89–104	105–120	121–8	9–24	50–65	66–81
$i = 4$	82–97	98–113	114–1	2–17	18–33	34–49
$i = 5$	75–90	91–106	107–122	123–10	11–26	27–42
$i = 6$	43–58	59–74	100–115	116–3	4–19	20–35
$i = 7$	36–51	52–67	68–83	84–99	125–12	13–28
$i = 8$	29–44	45–60	61–76	77–92	93–108	109–124
$i = 9$	22–37	38–53	54–69	70–85		

The 5-Round Attack (cont.)

Key observation:

- In order to know $\Delta s^5, \Delta s^6, \Delta s^7$ it is sufficient to know subkeys:

  $$Z_4^8, Z_3^8, Z_2^8, Z_1^8, Z_6^7, Z_5^7, Z_4^7, Z_3^7, Z_2^7, Z_1^7, Z_6^6, Z_5^6, Z_1^6, Z_2^6, Z_5^5$$

- **However, <u>these subkeys contain only 103 key bits.</u>**

The 5-Round Attack (cont.)

- Starting with 2^{19} KP before the MA of round **3**:
  - For each subkey guess, we get **32** pairs with input difference **(0,x,0,y)** to fourth round
  - Thus, $\Delta s^4 = 0$
  - And enough subkeys are known to determine $\Delta s^5, \Delta s^6, \Delta s^7$

The 5-Round Attack (cont.)

- For each subkey guess of Z_3^5, Z_3^6 :
  - Find the pairs that have the difference **(0,x,0,y)** before round **4**.
  - Take one of these pairs, and for each guess of the remaining **103-32=71** bits, check if the relation holds. If not, try another subkey guess.
  - Then, check for the remaining pairs whether the relation holds. In case of failure – move on to the next subkey guess.
- Exhaustively try the remaining possibilities for the key

1st Improvement

- Recall that we need an input difference to round 4 of the form (0,x,0,y)
- This is to ensure that $\Delta s^4 = 0$

But, this can be achieved using other pairs...

1st Improvement (cont.)

- The key Z_1^4 is among the **103** bits we guess
- If a pair of plaintexts has a difference 8000_x in the first word (after multiplication) and 8000_x in the third word (before the addition) then it satisfies $\Delta p^4 = 0 \Rightarrow \Delta s^4 = 0$
- Thus, data complexity can be improved by a factor of $\sqrt{2}$ without affecting the attack's time complexity

2nd Improvement

- There are **11** "unknown" bits in Z_3^4
- Guessing these bits allow to find the actual inputs to the multiplication with Z_5^4
- Also, we note that Z_5^4 is covered by the **103** bits we guessed
- Thus, the actual value of s^4 can be computed!

2nd Improvement (cont.)

- Take **16** known plaintexts, and guess the **114** required bits
- For each plaintext we compute the value of s^4
- Then, check for the **15** independent pairs whether the reduced Biryukov-Demirci relation holds. If not – the key guess is discarded

- The attack uses **16** known plaintexts, and has a time complexity of 2^{114} encryptions

A 7.5-Round Related-Key Attack

- A similar idea to the **5**-round attack
- The key difference is used to ensure the required difference **(0,x,0,y)** at the entrance to round **4**
- Let the key difference be in bit **34**, and any non-empty subset of bits {**41**, **42**, ..., **49**}

A 7.5-Round Related-Key Attack

- Take two plaintexts (P, P^*)
- If $Y_1^2 = Y_1^{2*}; \quad Y_2^2 = Y_2^{2*}; \quad Y_3^2 = Y_3^{2*}; \quad Y_4^2 = Y_4^{2*}$, then the equality holds till the fourth round, where the difference is introduced only in the subkey Z_6^4 , i.e., $\Delta s^4 = 0$
- The treatment of the rounds **5-7** is similar to the linear attack
- The treatment of the first round is a bit more complex due to the key difference

Treating the First Round

- The naïve approach of guessing the subkey would fail (too many subkey guesses)
- Different approach:
  - take enough known plaintexts under each of the two keys
  - Encrypt them through the KA of the 1st round
  - Examine pairs with difference $(0, 0040_x, 0, 0040_x)$
  - They have difference $(0, 0, 0040_x, 0040_x)$ at the entrance to the second round (independent of the 1st round MA layer)

Treating the First Round (cont.)

- Different approach (cont.):
  - such pairs have probability 2^{-17} to satisfy the difference zero after the second round KA layer
- So the attack is:
  - Guess the **64** bits of the first KA layer
  - Only for pairs with difference $(0, 0040_x, 0, 0040_x)$ guess the remaining bits
- Data complexity: $2^{43.5}$ known plaintexts
- Time complexity: $2^{115.1}$ encryptions

A 5.5-Round Attack

- Recall that in order to verify the Biryukov-Demirci relation for rounds **5,6,7** only **103** keys bits are to be guessed
- Maybe we can extend the Biryukov-Demirci relation more rounds towards the beginning?

A 5.5-Round Attack (cont.)

- Take a structure of 2^{16} plaintexts
- If after the KA layer of round **3** the following holds

$$Y_2^3, Y_4^3 = \text{Fixed}; Y_1^3 \oplus Y_3^3 = \text{Fixed}$$

then the input to the MA layer of round **3** is constant => which means that the input to round **4** is of the form **(P,P,C,C)**

- Which means that S^4 is permuted for all plaintexts in the structure

A 5.5-Round Attack (cont.)

- We use the Biryukov-Demirci relation for the **5** rounds starting at the middle of round **3**.
- The generation of the structures is a bit hard due to the KA layer.
- Take 2^{32} plaintexts of the form **(x,A,y,B)** where A and B are fixed.
- Guess the subkeys Z_1^3, Z_3^3 and you can find the required structure**(s)**.
- Luckily – most of these subkeys are covered in the **103** bits we have to guess!

A 5.5-Round Attack (cont.)

- Time complexity:
  - Finding the structures is easy.
  - For each 32-bit guess, we have to guess 80 additional bits (total of 112 bits) and partially decrypt 2^{16} values: 2^{128} partial decryptions
- Total: 0.43 * 2^{128} encryptions

An Improvement

- We note that in order to generate a set which satisfy the requirement, the MSB of Z_3^3 is not necessary.
- Thus, we do not need to guess it.

- Final time complexity: $0.43 * 2^{127} = 2^{126.85}$
- Data Complexity: 2^{32} CP

A 6-Round Attack (cont.)

- The additional half round prevents efficient structures.
- Thus, we have to take almost the entire code book
- For each subkey guess of Z_5^2, Z_6^2 find four structures for the **5.5**-round attack, and apply it
- Data Complexity: $2^{64} - 2^{52}$
- Time Complexity: $2^{126.8}$

Summary

Attack	*Rounds*	*Complexity*	
		Data	*Time*
Linear (Distinguishing)	2.5	2^{18} CP	2^{18}
Linear	3	2^{19} CP	$2^{48.5}$
Differential-Linear	5	2^{19} KP	2^{103}
Related-Key Linear	7.5	$2^{43.5}$ $RK-KP$	$2^{115.1}$
Related-Key Rectangle	7	2^{65} $RK-CP$	$2^{104.2}$
Differential-Linear	5	$2^{18.5}$ KP	2^{103}
Differential-Linear	5	16 KP	2^{114}
Higher-Order Diff.Lin.	5.5	2^{32} CP	$2^{126.85}$
Higher-Order Diff.Lin.	6	$2^{64}-2^{52}$ KP	$2^{126.8}$

Thank you!