Rethinking IDEA

Orr Dunkelman

Department of Computer Science, University of Haifa
Faculty of Mathematics and Computer Science
Weizmann Institute of Science

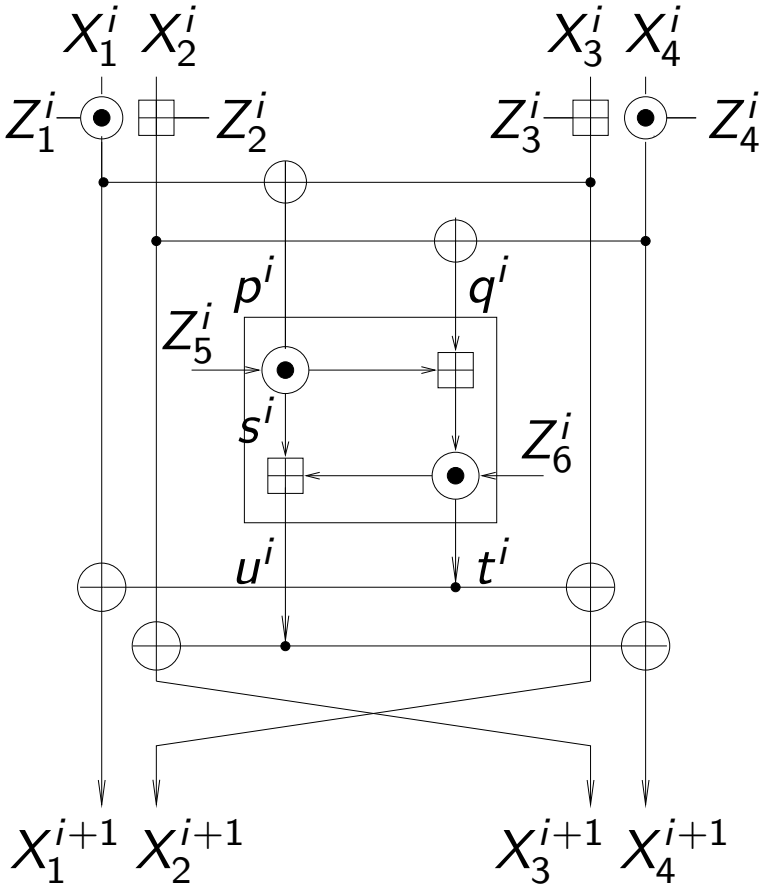
8 August, 2011

Joint work with Eli Biham, Nathan Keller, and Adi Shamir

Outline

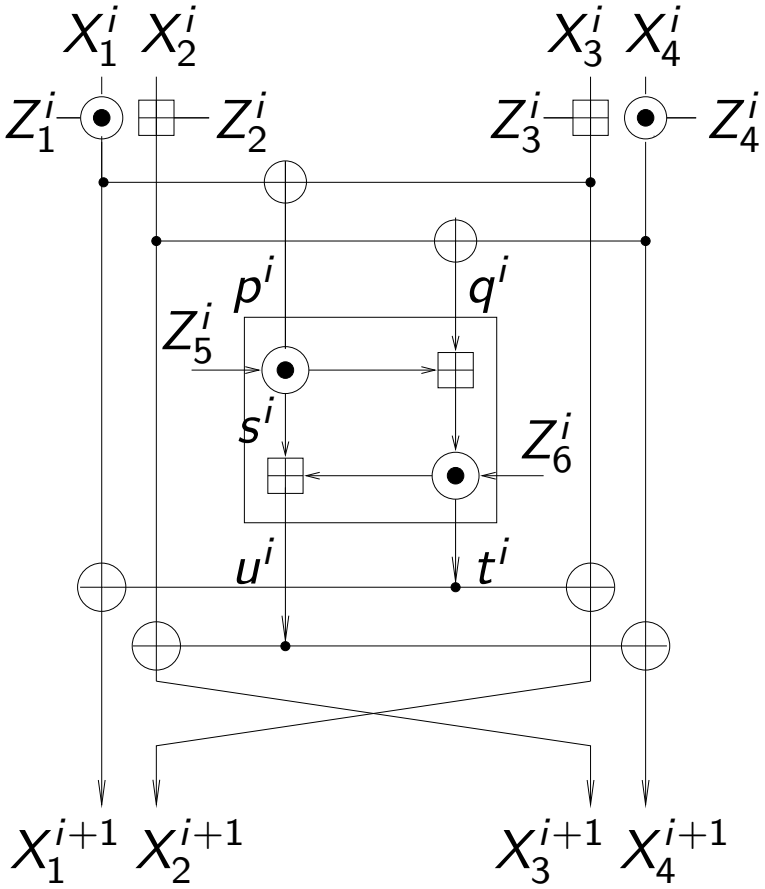
IDEA

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications
- Has 8.5 rounds
- A "red cape" for cryptanalysts — more than 20 research papers.



IDEA

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications
- Has 8.5 rounds
- A "red cape" for cryptanalysts — more than 20 research papers.

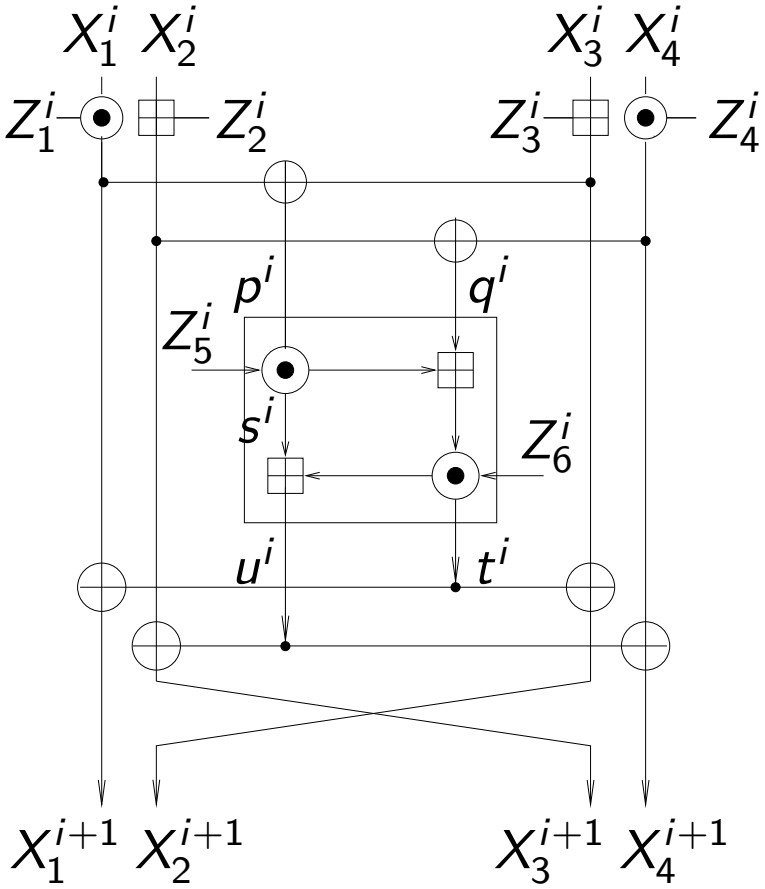


From the decryption operation:

$$X_1^{i+1} \oplus X_2^{i+1} = p^i$$

IDEA

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications
- Has 8.5 rounds
- A "red cape" for cryptanalysts — more than 20 research papers.

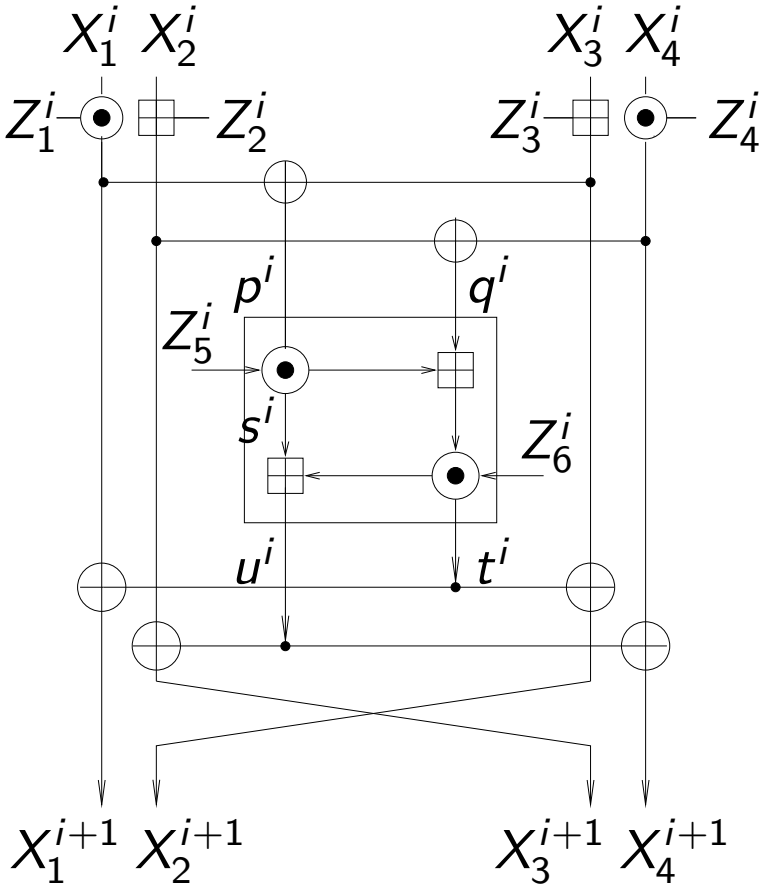


From the decryption operation:

$$X_1^{i+1} \oplus X_2^{i+1} = p^i = X_1^i \oplus X_3^i$$

IDEA

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications
- Has 8.5 rounds
- A "red cape" for cryptanalysts — more than 20 research papers.



From the decryption operation:

$$X_3^{i+1} \oplus X_4^{i+1} = q^i = X_2^i \oplus X_4^i$$

Key Schedule of IDEA

- Subkeys are 16 consecutive bits of the key.
- A 128-bit register is initialized with the key. To generate the next subkey, the next 16 bits are taken. After 8 of these, the register is rotated to the left by 25 bits.

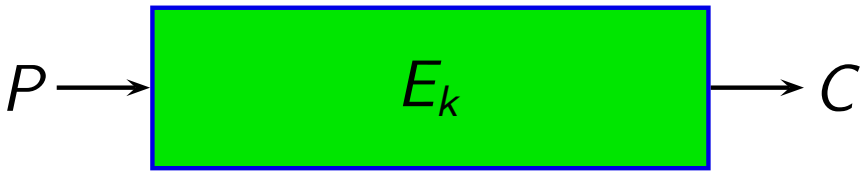
Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 1$	0–15	16–31	32–47	48–63	64–79	80–95
$i = 2$	96–111	112–127	25–40	41–56	57–72	73–88
$i = 3$	89–104	105–120	121–8	9–24	50–65	66–81
$i = 4$	82–97	98–113	114–1	2–17	18–33	34–49
$i = 5$	75–90	91–106	107–122	123–10	11–26	27–42
$i = 6$	43–58	59–74	100–115	116–3	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		

Previous Results on IDEA

Rounds	Attack Type	Data	Time	Source
2	Differential	2^{10} CP	2^{40}	[M93]
2.5	Differential	2^{10} CP	$2^{104.7}$	[M93]
3	Differential-Linear	2^{29} CP	2^{44}	[BKR97]
3.5	Differential	2^{56} CP	2^{67}	[BKR97]
4	Impossible Differential	$2^{36.6}$ CP	$2^{66.6}$	[BBS99]
4.5	Impossible Differential	2^{64} KP	$2^{110.4}$	[BBS99]
5	Demirci-Selçuk-Türe	$2^{24.6}$ CP	2^{124}	[AS06]
5.5	Key-dependent Linear	2^{21} CP	$2^{112.1}$	[SL09]
6	Key-dependent Linear	2^{49} CP	$2^{112.1}$	[SL09]
4.5	Zero-in-the-Middle BD-relation	16 CP	2^{103}	[BDK06]
5	Zero-in-the-Middle BD-relation	$2^{18.5}$ KP	2^{103}	[BDK07]
5	Zero-in-the-Middle BD-relation	16 KP	2^{114}	[BDK07]
5.5	Zero-in-the-Middle BD-relation	2^{32} CP	$2^{126.85}$	[BDK07]
6	Zero-in-the-Middle BD-relation	2^{64} KP	$2^{126.8}$	[BDK07]
4.5	Meet-in-the-Middle	2 KP	2^{103}	**New!**
6	Meet-in-the-Middle BD-relation	2 KP	$2^{123.4}$	**New!**
6	Meet-in-the-Middle BD-relation	16 KP	$2^{111.8}$	**New!**

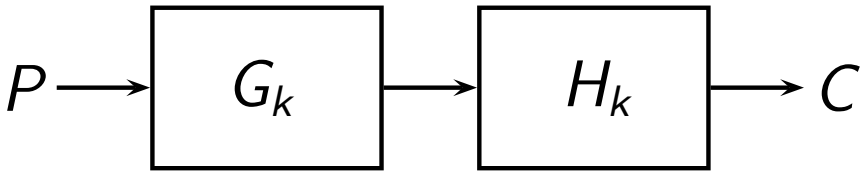
The Basics of Meet in the Middle (MitM) Attacks

- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$



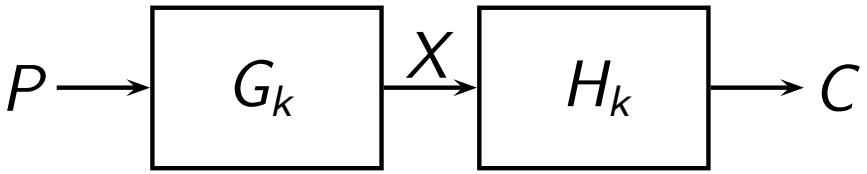
The Basics of Meet in the Middle (MitM) Attacks

- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$



The Basics of Meet in the Middle (MitM) Attacks

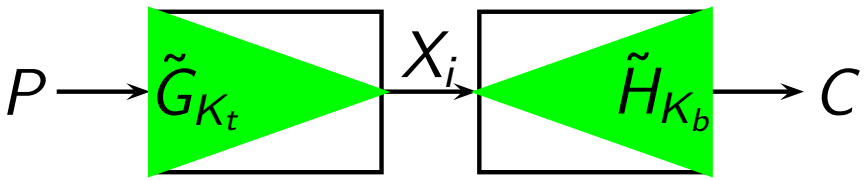
- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$
- Let $C = E_k(P)$, and let $G_k(P) = X = H_k^{-1}(C)$



The Basics of Meet in the Middle (MitM) Attacks

- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$
- Let $C = E_k(P)$, and let $G_k(P) = X = H_k^{-1}(C)$
- Assume that a subset X_i of X can be written as

$$X_i = \tilde{G}_{K_t}(P)$$
$$X_i = \tilde{H}_{K_b}(C)$$



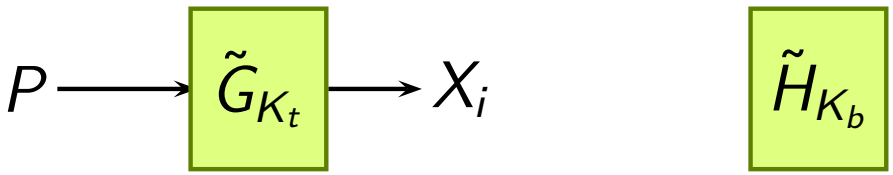
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, X_i, K_t$, and K_b

$\tilde{G}_{K_t}$ $\tilde{H}_{K_b}$

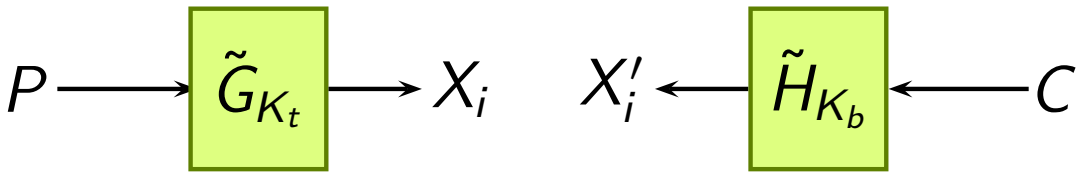
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, X_i, K_t$, and K_b
- Given a plaintext/ciphertext pair (P, C):
  1. For each K_t, compute $X_i = \tilde{G}_{K_t}(P)$ and store the value (X_i, K_t) in a hash table.



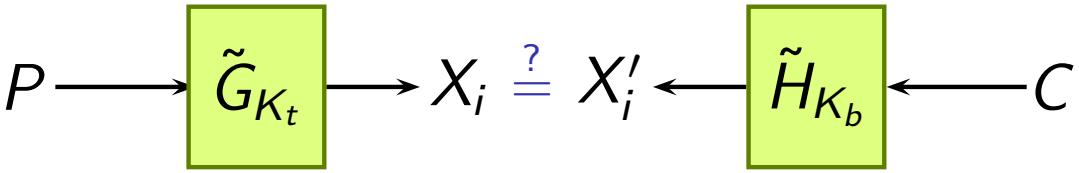
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, X_i, K_t$, and K_b
- Given a plaintext/ciphertext pair (P, C):
  1. For each K_t, compute $X_i = \tilde{G}_{K_t}(P)$ and store the value (X_i, K_t) in a hash table.
  2. For each K_b, compute $X_i' = \tilde{H}_{K_b}(C)$.



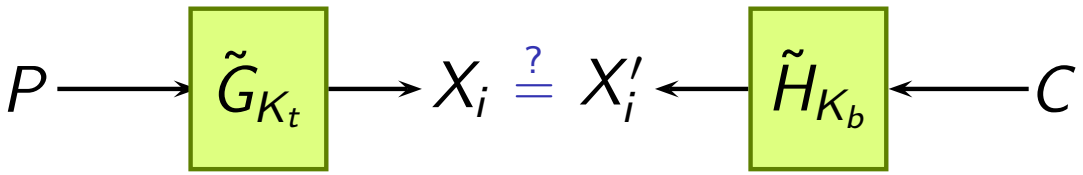
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, X_i, K_t$, and K_b
- Given a plaintext/ciphertext pair (P, C):
  1. For each K_t, compute $X_i = \tilde{G}_{K_t}(P)$ and store the value (X_i, K_t) in a hash table.
  2. For each K_b, compute $X_i' = \tilde{H}_{K_b}(C)$.
  3. For each X_i' if it is in the table, further analyze K_t, K_b



Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, X_i, K_t$, and K_b
- Given a plaintext/ciphertext pair (P, C):
  1. For each K_t, compute $X_i = \tilde{G}_{K_t}(P)$ and store the value (X_i, K_t) in a hash table.
  2. For each K_b, compute $X_i' = \tilde{H}_{K_b}(C)$.
  3. For each X_i' if it is in the table, further analyze K_t, K_b
- Further analyze may be: analyze another plaintext/ciphertext pair, exhaustively search remaining key bits, etc.



A Simple MitM Attack on 3.5-Round IDEA

- Consider the first 3.5 rounds of IDEA, and take two plaintexts.

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		

A Simple MitM Attack on 3.5-Round IDEA

- Consider the first 3.5 rounds of IDEA, and take two plaintexts.
- Bits 0–111 allows computing p^2 from the plaintext.

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		

A Simple MitM Attack on 3.5-Round IDEA

- Consider the first 3.5 rounds of IDEA, and take two plaintexts.
- Bits 0–111 allows computing p^2 from the plaintext.
- Bits 50–17 allows computing p^2 from the ciphertext.

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		

A Simple MitM Attack on 3.5-Round IDEA

- Consider the first 3.5 rounds of IDEA, and take two plaintexts.
- Bits 0–111 allows computing p^2 from the plaintext.
- Bits 50–17 allows computing p^2 from the ciphertext.

MitM condition: 16 bits,
Number of key bits: 112 from top, 96 from bottom,
Data complexity: 13 KPs, Time complexity: 2^{112},
Memory complexity: 2^{96}.

Reducing Memory Complexity

- Take the required plaintext/ciphertext pairs.
- For each guess of the blue 112 bits, compute the p^2 values (for all pairs) and store the value $p^2, K[0–111]$ in a hash table.
- For each guess of the red 96 bits, compute the p^2 values, and check if they appear in the table.
- Once a collision is found, a key suggestion is made, and check its validity using exhaustive search.

Reducing Memory Complexity

- Take the required plaintext/ciphertext pairs.
- For each guess of the red 96 bits, compute the p^2 values (for all pairs) and store the value $p^2, K[50–17]$ in a hash table.
- For each guess of the blue 112 bits, compute the p^2 values, and check if they appear in the table.
- Once a collision is found, a key suggestion is made, and check its validity using exhaustive search.

Reducing Memory Complexity

- Take the required plaintext/ciphertext pairs.
- For each guess of the 80 bits which are shared among the red and the blue:
  - For each guess of the remaining red 16 bits, compute the p^2 values, and store them in a hash table.
  - For each guess of the remaining blue 32 bits, compute the p^2 values and check if they appear in the table.
- Once a collision is found, a key suggestion is made, and check its validity using exhaustive search.

Reducing Memory Complexity

- Take the required plaintext/ciphertext pairs.
- For each guess of the 80 bits which are shared among the red and the blue:
  - For each guess of the remaining red 16 bits, compute the p^2 values, and store them in a hash table.
  - For each guess of the remaining blue 32 bits, compute the p^2 values and check if they appear in the table.
- Once a collision is found, a key suggestion is made, and check its validity using exhaustive search.

Memory complexity: 2^{16}, Time complexity: 2^{112}, Data complexity: 8 KPs.

Reducing Memory Complexity

- Take the required plaintext/ciphertext pairs.
- For each guess of the 80 bits which are shared among the red and the blue:
  - For each guess of the remaining red 16 bits, compute the p^2 values, and store them in a hash table.
  - For each guess of the remaining blue 32 bits, compute the p^2 values and check if they appear in the table.
- Once a collision is found, a key suggestion is made, and check its validity using exhaustive search.

Memory complexity: 2^{16}, Time complexity: 2^{112}, Data complexity: 2 KPs.

Improved Attack

- We can further improve the time complexity of the attack.
- Consider MitM on q^2:

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		

- Now K_b is 103 bits long, and K_t is still 112 bits long.

A Few Improvements (cont.)

- The main observation is that bits 112–127 enter addition, and are used only in that addition.
- By guessing the k LSBs of these bits, we get the k LSBs of q^2.
- So we set $k = 7$, and then $|K_b| = |K_t| = 103$.
- Time complexity: 2^{103} (data complexity: 4 KPs, memory complexity: 2^{25}).

Extending the Attack to 4.5-Round IDEA

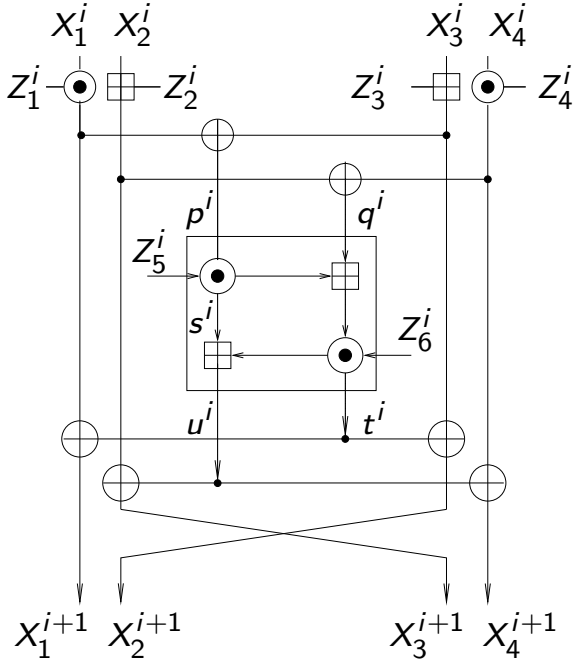
- IDEA's key schedule repeats key bits.
- Starting at the MA of round 2, we can extend the attack to 4.5 rounds.

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 2$	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

The MitM condition is on 16 bits.
Data complexity: 2KPs. Memory complexity: 2^{25}.
Time complexity: 2^{103}.

The Biryukov-Demirci Relation

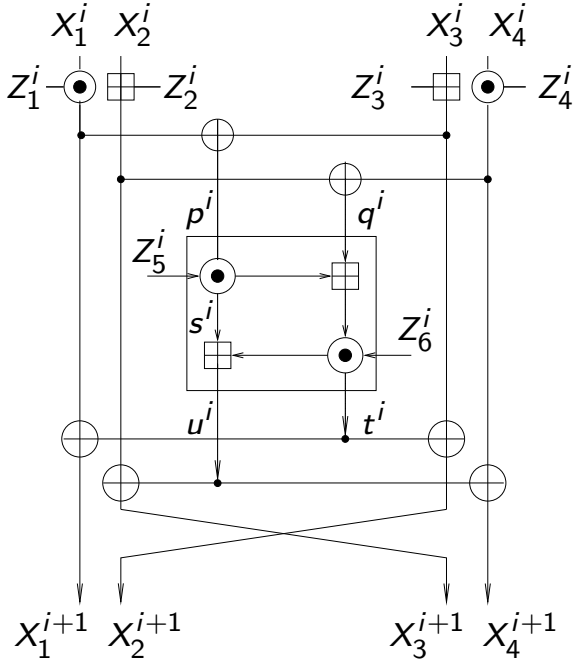
Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.



The Biryukov-Demirci Relation

Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.

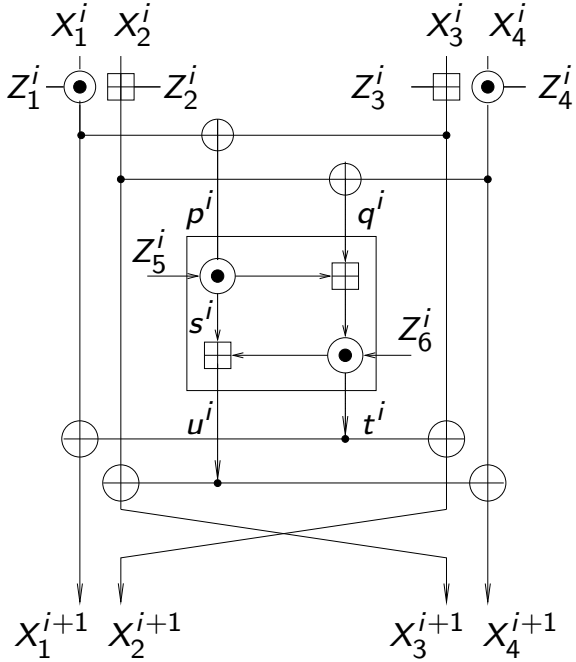
$$P_2 \boxplus Z_2^1$$



The Biryukov-Demirci Relation

Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.

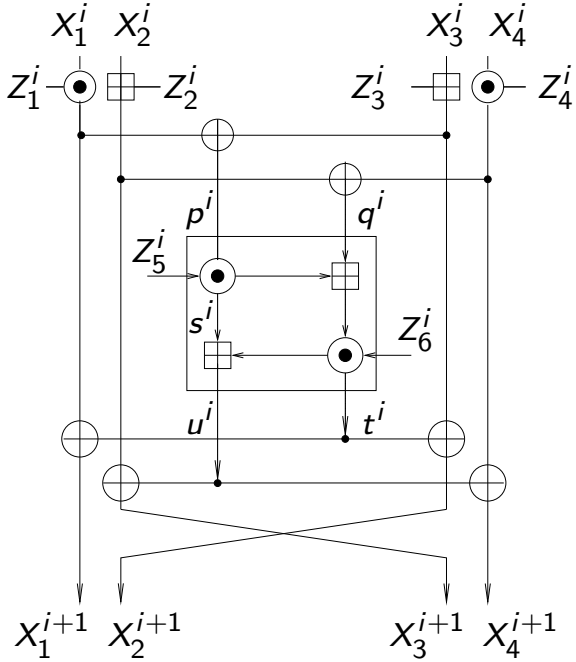
$$(P_2 \boxplus Z_2^1) \oplus u^1$$



The Biryukov-Demirci Relation

Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.

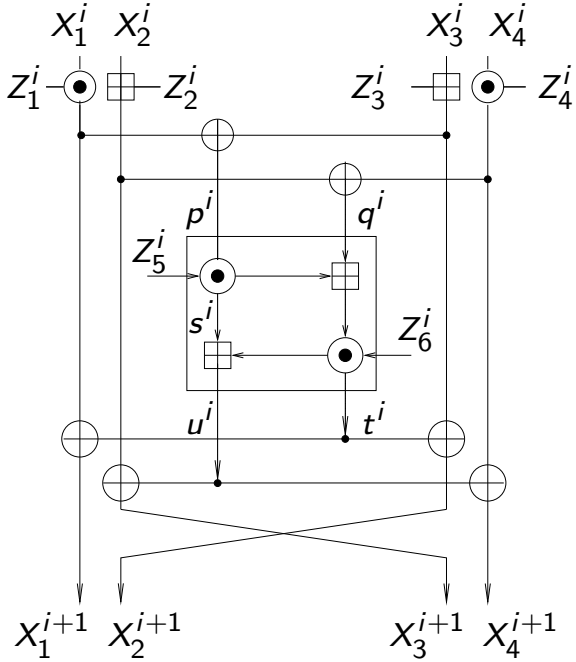
$$((P_2 \boxplus Z_2^1) \oplus u^1) \boxplus Z_3^2$$



The Biryukov-Demirci Relation

Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.

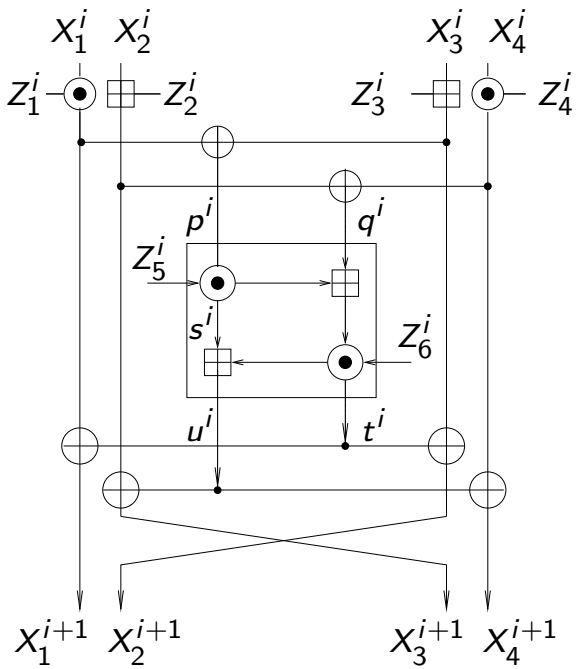
$$((((P_2 \boxplus Z_2^1) \oplus u^1) \boxplus Z_3^2) \oplus t^2$$



The Biryukov-Demirci Relation

Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.

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



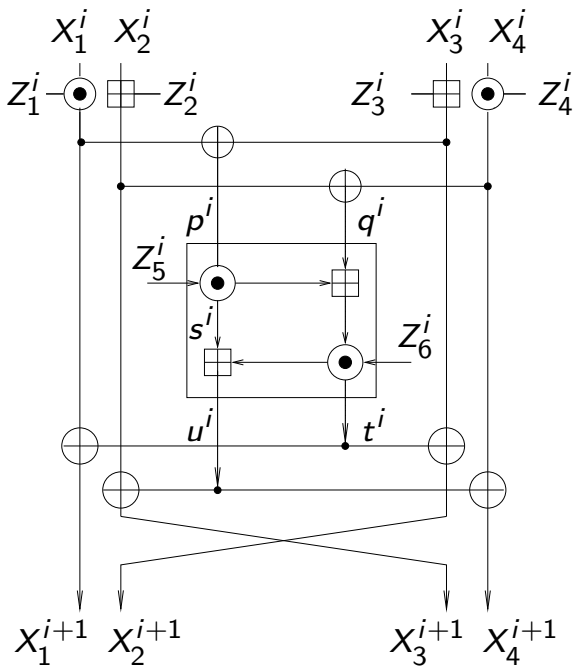
The Biryukov-Demirci Relation

Consider the encryption of the plaintext $P = (P_1, P_2, P_3, P_4)$ to the ciphertext $C = (C_1, C_2, C_3, C_4)$.

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

Similarly:

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



The Biryukov-Demirci Relation (cont.)

- Consider the LSB of both expressions, for which $\boxplus \equiv \oplus$:

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

and

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

The Biryukov-Demirci Relation (cont.)

- Consider the LSB of both expressions, for which $\boxplus \equiv \oplus$:

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

and

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

- XORing both equations (and using the fact that $u^i = t^i \boxplus s^i$ implies that $LSB(u^i) = LSB(t^i \oplus s^i)$):

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

The Biryukov-Demirci Relation (cont.)

- We can rearrange the above equation into any form we like...

$$LSB(P_2 \oplus P_3 \oplus C_2 \oplus C_3) =$$
$$LSB(Z_2^1 \oplus Z_3^1 \oplus Z_2^2 \oplus Z_3^2 \ldots \oplus Z_9^2 \oplus Z_9^3) \oplus$$
$$LSB(s^1 \oplus s^2 \ldots \oplus s^8)$$

The Keyless Biryukov-Demirci Relation

- Consider two plaintexts P^1, P^2.
- As for each of them the Biryukov-Demirci relation is satisfied we obtain that:

$$LSB(P_2^1 \oplus P_3^1 \oplus P_2^2 \oplus P_3^2 \oplus C_2^1 \oplus C_3^1 \oplus C_2^2 \oplus C_3^2) = LSB(\Delta s^1 \oplus \Delta s^2 \oplus \ldots \oplus \Delta s^8)$$

6-Round Meet-in-the-Middle Based on the BD Relation

- One can attack 6-round IDEA starting just after the second round's MA.
- The keyless Biryukov-Demirci relation in this case can be written as a MitM condition:

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

- The first part of the equation can be evaluated from the plaintext pair given 112 bits of the key (bits 50–33).
- The second part of the equation can be evaluated form the ciphertext pair given 103 bits of the key (bits 125–99).

Meet-in-the-Middle Based on the BD Relation (cont.)

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 2$	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

Meet-in-the-Middle Based on the BD Relation (cont.)

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 2$	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

- Note that the "partial encryption" and the "partial decryption" do not "meet" on the intermediate values.

Meet-in-the-Middle Based on the BD Relation (cont.)

- The data complexity of the attack is 16 KPs, which compose 15 pairs (each contributing a bit to the MitM condition).
- Time complexity: $2^{112} \cdot 16$ partial encryptions (about 2^{115} encryptions).
- Memory complexity: 2^{16}.

A Small Few Improvement

- 9 out of the 112 bits guessed from the top, are only needed to determine Δs^4.
- Hence, we compute all the intermediate values using the 103 bits, and then just perform the final $\odot$ operation 2^9.
- This saves time complexity ($2^{111.4}$ in total), but increases memory complexity, as these 9 bits are shared.
- Data complexity: 16 KPs, Memory complexity: 2^{25}, Time complexity: $2^{111.8}$.

A Small Few Improvement

- 9 out of the 112 bits guessed from the top, are only needed to determine Δs^4.
- Hence, we compute all the intermediate values using the 103 bits, and then just perform the final $\odot$ operation 2^9.
- This saves time complexity ($2^{111.4}$ in total), but increases memory complexity, as these 9 bits are shared.
- Data complexity: 16 KPs, Memory complexity: 2^{25}, Time complexity: $2^{111.8}$.
- A variant of the attack has data complexity of 2 KPs with time complexity of $2^{123.4}$ and about the same memory complexity.

A Zero-in-the-Middle Attack

- One can use the keyless Biryukov-Demirci relation in a different manner.

A Zero-in-the-Middle Attack

- One can use the keyless Biryukov-Demirci relation in a different manner.
- Assume we pick plaintexts such that $\Delta s^i = 0$, then one does not need to compute it. . . .

A Zero-in-the-Middle Attack

- One can use the keyless Biryukov-Demirci relation in a different manner.
- Assume we pick plaintexts such that $\Delta s^i = 0$, then one does not need to compute it. . . .
- This is used for an attack on 5-round of IDEA starting after the *KA* of round 3 (i.e., attacking rounds 3.5–8.5).
- For this case, the keyless Biryukov-Demirci relation is reduced to:

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

- The first two unknown are controlled by structures of plaintexts and key guessing (computing Δs^3, and fixing $\Delta s^4 = 0$.
- This leaves 3 unknowns — $\Delta s^5, \Delta s^6$, and Δs^7.

Key Observation

- Given a ciphertext pair, to determine $\Delta s^5, \Delta s^6, \Delta s^7$, we need to guess the following 15 subkeys:

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

Key Observation

- Given a ciphertext pair, to determine $\Delta s^5, \Delta s^6, \Delta s^7$, we need to guess the following 15 subkeys:

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

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 5$	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

Key Observation

- Given a ciphertext pair, to determine $\Delta s^5, \Delta s^6, \Delta s^7$, we need to guess the following 15 subkeys:

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

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 5$	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

- These are composed of only 103 key bits!

Attack Procedure

- Take 2^{19} known plaintexts.
- For each subkey guess at the first MA (these bits are part of the 103 bits), there are 32 pairs with difference $(0, x, 0, y)$ entering the fourth round.
- For these pairs, $\Delta s^4 = 0$.

Attack Procedure

- Take 2^{19} known plaintexts.
- For each subkey guess at the first MA (these bits are part of the 103 bits), there are 32 pairs with difference $(0, x, 0, y)$ entering the fourth round.
- For these pairs, $\Delta s^4 = 0$.
- Guess the remaining 71 bits, and try the 32 pairs. If all pairs satisfy the Biryukov-Demirci relation, exhaustively search the remaining key bits.
- Data complexity: 2^{19} known plaintexts, Time complexity: 2^{103}.

Several Improvements

- One can save a $\sqrt{2}$ in the data complexity by allowing differences of the form $(8000_x, x, 8000_x, y)$.
- By using the fact that Z_3^4 has 11 unknown bits (with respect to the 103) and that Z_5^4 is covered by all these 114 bits, one can drop the difference requirement. It is possible to actually compute Δs^4 for free.
- Data complexity: 16 known plaintexts. Time complexity: 2^{114}.

Attack on 6-Round IDEA

- One can control one extra round using a structure of 2^{16} plaintexts, rather than 2.
- Taking a structure of 2^{16} values for which $Y_1^3 \oplus Y_3^3, Y_2^3, Y_4^3$ is fixed, assures that

$$\bigoplus_{i=0}^{2^{16}-1} s_3 = 0 = \bigoplus_{i=0}^{2^{16}-1} s_4$$

  for all values in the structure.
- This can be used for attacks up to 6-round IDEA with data complexity of almost the entire codebook and $2^{126.8}$ time.

A Related-Key Attack on 7.5-Round IDEA

- Another possibility to control as many Δs^i as possible, is to use related-key differential.
- This allows attacking 7.5-round IDEA with either
  1. 2^{25} chosen plaintexts (and 2^{25} memory), or
  2. 2^{43} known plaintexts (and 2^{43} memory)

  with both attacks taking $2^{103.5}$ time.

Questions?

Available online at
http://eprint.iacr.org/2011/417

Thank you for you attention!