A Practical-Time Related-Key Boomerang Attack on MMB

Tomer Ashur Orr Dunkelman

29/10/2013

Overview

1. Quick description of the MMB block cipher.

Overview

1. Quick description of the MMB block cipher.
2. Short Explanation about cryptanalytic techniques used in this paper.

Overview

1. Quick description of the MMB block cipher.
2. Short Explanation about cryptanalytic techniques used in this paper.
3. A related-key boomerang attack that recovers 62 key bits for MMB.

Overview

1. Quick description of the MMB block cipher.
2. Short Explanation about cryptanalytic techniques used in this paper.
3. A related-key boomerang attack that recovers 62 key bits for MMB.
4. Using the previously recovered 62 bits to recover another 31 bits of the key.

Overview

1. Quick description of the MMB block cipher.
2. Short Explanation about cryptanalytic techniques used in this paper.
3. A related-key boomerang attack that recovers 62 key bits for MMB.
4. Using the previously recovered 62 bits to recover another 31 bits of the key.
5. Recovering the last bits.

Overview

1. Quick description of the MMB block cipher.
2. Short Explanation about cryptanalytic techniques used in this paper.
3. A related-key boomerang attack that recovers 62 key bits for MMB.
4. Using the previously recovered 62 bits to recover another 31 bits of the key.
5. Recovering the last bits.
6. Results of experimental verification.

Overview

1. Quick description of the MMB block cipher.
2. Short Explanation about cryptanalytic techniques used in this paper.
3. A related-key boomerang attack that recovers 62 key bits for MMB.
4. Using the previously recovered 62 bits to recover another 31 bits of the key.
5. Recovering the last bits.
6. Results of experimental verification.
7. Possible extenstions of the attack.

The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.

The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.
- Block and key size of 128-bit.

The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.
- Block and key size of 128-bit.
- Six rounds, 4 operations:

The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.
- Block and key size of 128-bit.
- Six rounds, 4 operations:
  - σ - key injection $(x_i \oplus k_i^j)$.

The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.
- Block and key size of 128-bit.
- Six rounds, 4 operations:
  - σ - key injection $(x_i \oplus k_i^j)$.
  - γ - modular multiplication $((x_i * G_i)\ mod\ (2^{32} - 1))$.

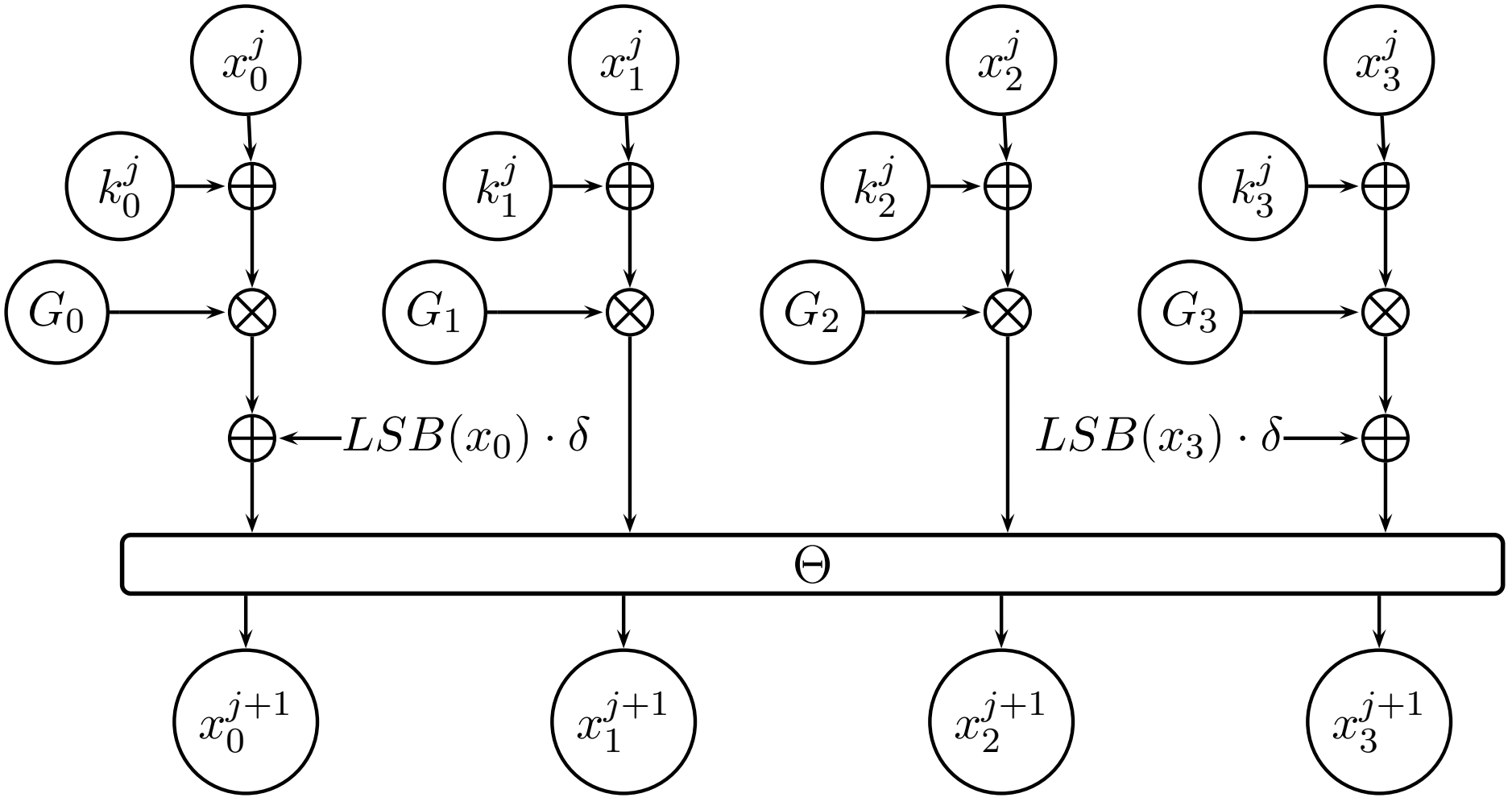
The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.
- Block and key size of 128-bit.
- Six rounds, 4 operations:
  - σ - key injection $(x_i \oplus k_i^j)$.
  - γ - modular multiplication $((x_i * G_i)\ mod\ (2^{32} - 1))$.
  - η - data-dependent operation $((x_i\ mod\ 2)\ ?\ (\delta \oplus x_i) : x_i)$.

The Modular Multiplication Block (MMB) Cipher

- Invented in 1997, by Joan Daemen as an improvment for the IDEA cipher.
- Block and key size of 128-bit.
- Six rounds, 4 operations:
  - σ - key injection $(x_i \oplus k_i^j)$.
  - γ - modular multiplication $((x_i * G_i)\ mod\ (2^{32} - 1))$.
  - η - data-dependent operation $((x_i\ mod\ 2)\ ?\ (\delta \oplus x_i) : x_i)$.
  - θ - matrix multiplication $(x_{i-1} \oplus x_i \oplus x_{i+1})$.

MMB's Round Function



Differential Cryptanalysis and its Variants

- Differential cryptanalysis[BS91]

Differential Cryptanalysis and its Variants

- Differential cryptanalysis[BS91]
- Related-key differential cryptanalysis[KSW96]

Differential Cryptanalysis and its Variants

- Differential cryptanalysis[BS91]
- Related-key differential cryptanalysis[KSW96]
- Boomerang attack[W99]

Differential Cryptanalysis and its Variants

- Differential cryptanalysis[BS91]
- Related-key differential cryptanalysis[KSW96]
- Boomerang attack[W99]
- Related-key boomerang attack[K+04,K+05,BDK05]

Previous Work

- 2-round differential with probability 1 [WNS09]:

$$(0,\bar{0},\bar{0},0) \xrightarrow{\sigma[\mathrm{k}^0]} (0,\bar{0},\bar{0},0) \xrightarrow{\gamma} (0,\bar{0},\bar{0},0) \xrightarrow{\eta} (0,\bar{0},\bar{0},0) \xrightarrow{\theta} (\bar{0},0,0,\bar{0})$$
$$\xrightarrow{\sigma[\mathrm{k}^1]} (\bar{0},0,0,\bar{0}) \xrightarrow{\gamma} (\bar{0},0,0,\bar{0}) \xrightarrow{\eta} (\bar{\delta},0,0,\bar{\delta}) \xrightarrow{\theta} (0,\bar{\delta},\bar{\delta},0)$$

Previous Work

- 2-round differential with probability 1 [WNS09]:

$$(0,\bar{0},\bar{0},0) \xrightarrow{\sigma[\mathrm{k}^0]} (0,\bar{0},\bar{0},0) \xrightarrow{\gamma} (0,\bar{0},\bar{0},0) \xrightarrow{\eta} (0,\bar{0},\bar{0},0) \xrightarrow{\theta} (\bar{0},0,0,\bar{0})$$
$$\xrightarrow{\sigma[\mathrm{k}^1]} (\bar{0},0,0,\bar{0}) \xrightarrow{\gamma} (\bar{0},0,0,\bar{0}) \xrightarrow{\eta} (\bar{\delta},0,0,\bar{\delta}) \xrightarrow{\theta} (0,\bar{\delta},\bar{\delta},0)$$

- 5-round distinguisher with probability 2^{-110} [WNS09].
- Full key recovery with time complexity of 2^{118} [WNS09].

Previous Work

- 2-round differential with probability 1 [WNS09]:

$$(0,\bar{0},\bar{0},0) \xrightarrow{\sigma[\mathrm{k}^0]} (0,\bar{0},\bar{0},0) \xrightarrow{\gamma} (0,\bar{0},\bar{0},0) \xrightarrow{\eta} (0,\bar{0},\bar{0},0) \xrightarrow{\theta} (\bar{0},0,0,\bar{0})$$
$$\xrightarrow{\sigma[\mathrm{k}^1]} (\bar{0},0,0,\bar{0}) \xrightarrow{\gamma} (\bar{0},0,0,\bar{0}) \xrightarrow{\eta} (\bar{\delta},0,0,\bar{\delta}) \xrightarrow{\theta} (0,\bar{\delta},\bar{\delta},0)$$

- 5-round distinguisher with probability 2^{-110} [WNS09].
- Full key recovery with time complexity of 2^{118} [WNS09].
- 5-round sandwich distinguisher with probability 1 [J+11].
- Full key recovery with time complexity of 2^{40} [J+11].

Description of the Differential Characteristics

3-round related-key differential characteristic with probability 1:
$\triangle =$
$(0, 0, \bar{0}, \bar{0}) \xrightarrow{(0,0,\bar{0},\bar{0})}$
$(\delta, \bar{0}, \delta, \bar{\delta}) = \triangle^*.$

Full Description

One additional round can be prepended:
$(X, \bar{0}, 0, \bar{0}) \rightarrow \triangle$

4-round related-key differential characteristic with probability 1:
$\bigtriangledown^* =$
$(0, 0, \bar{0}, 0) \xrightarrow{(0,0,\bar{0},0)}$
$(\bar{\delta}, \bar{\delta}, 0, \bar{\delta}) = \bigtriangledown$

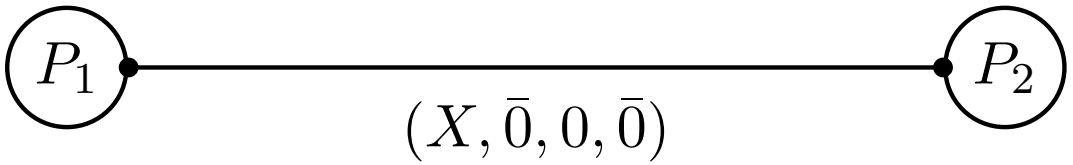
Full Description

One additional round can be prepended:
$(0, \bar{0}, \bar{0}, Y) \rightarrow \bigtriangledown^*$

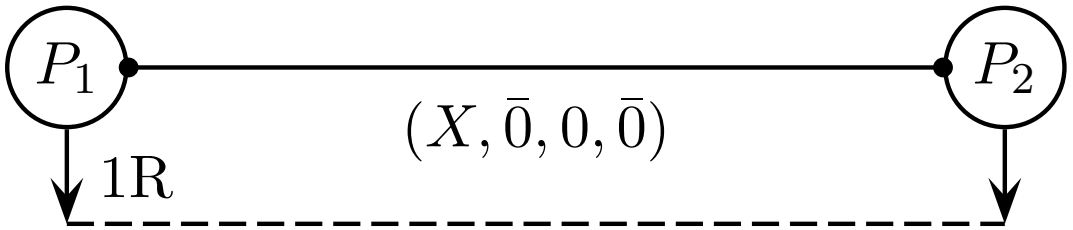
2-round related-key differential characteristic with probability 1:
$\tau =$
$(0, 0, 0, \bar{0}) \xrightarrow{(0,0,0,\bar{0})}$
$(0, \bar{0}, \bar{0}, \bar{0}) = \tau^*$

Full Description

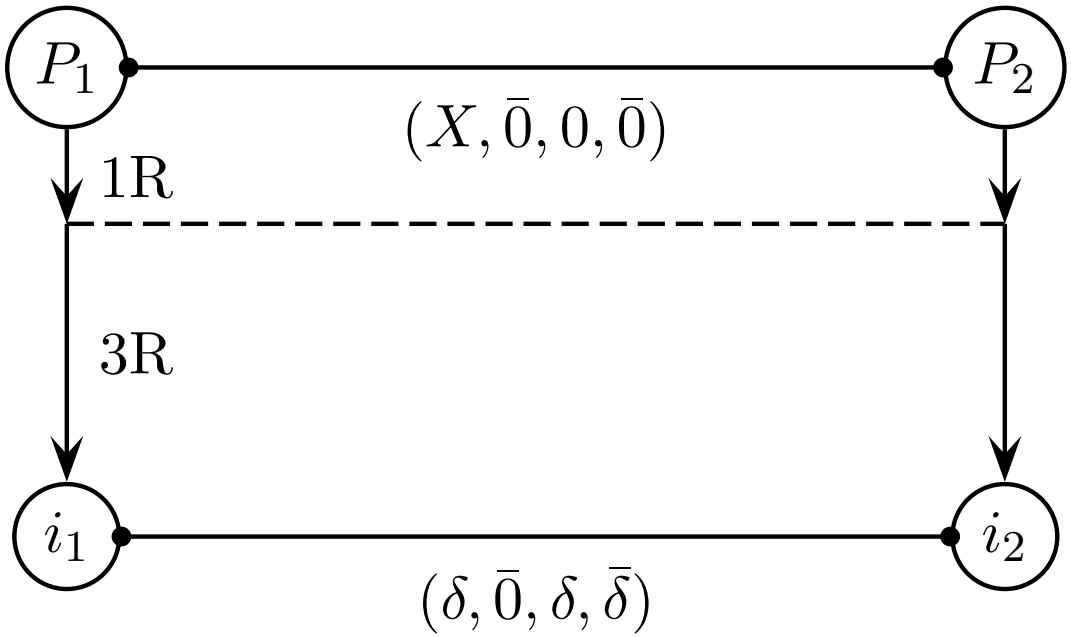
Description of B_0



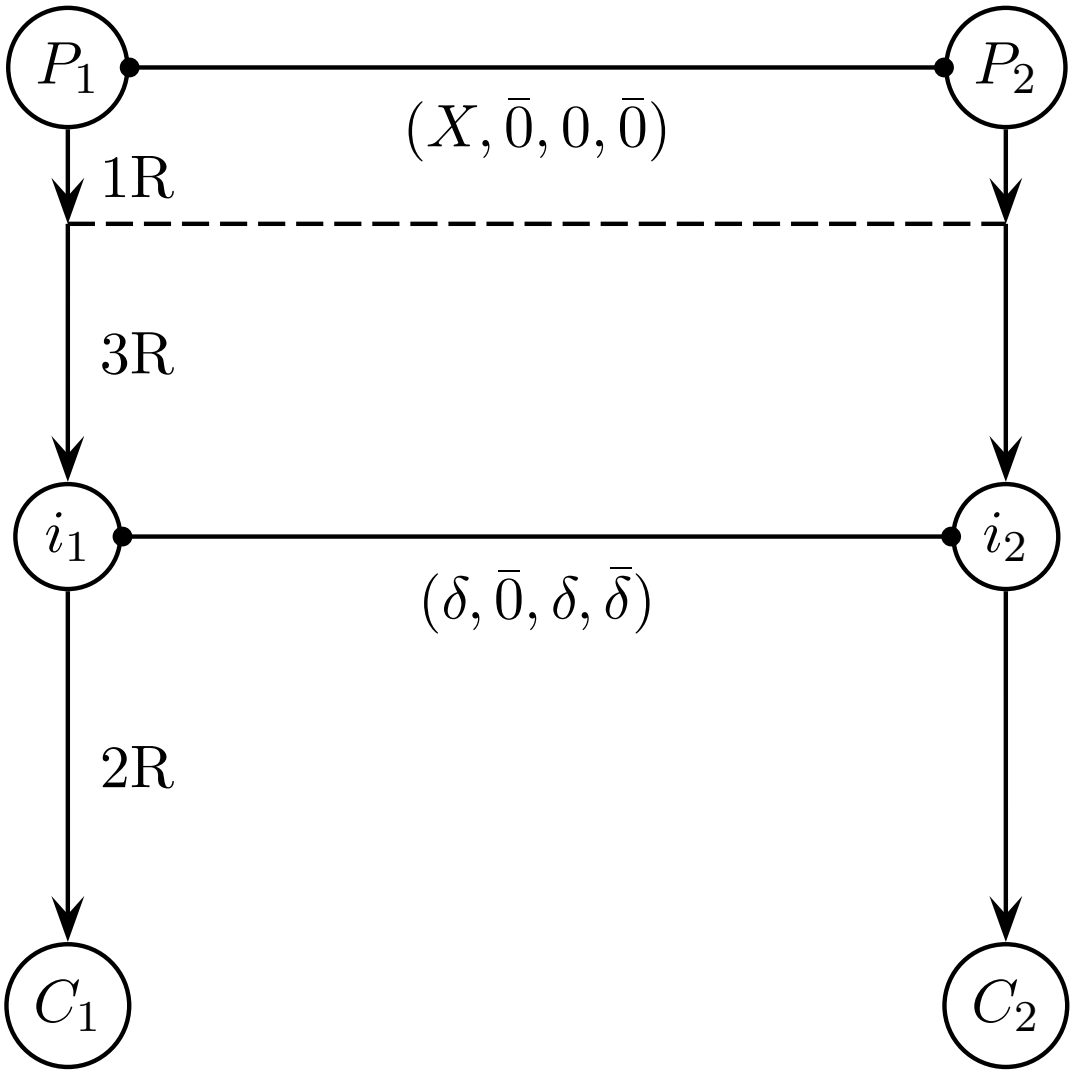
Description of B_0



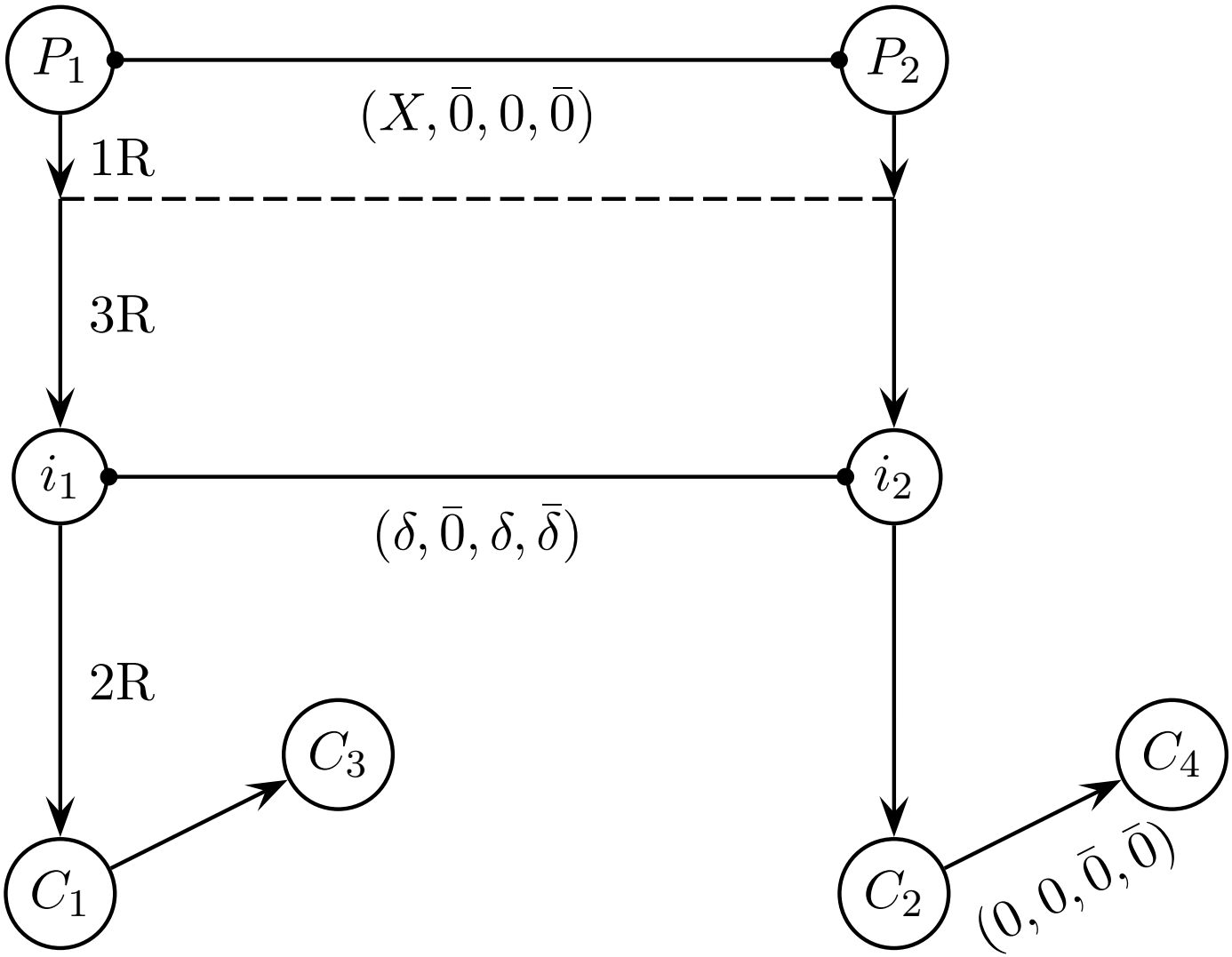
Description of B_0



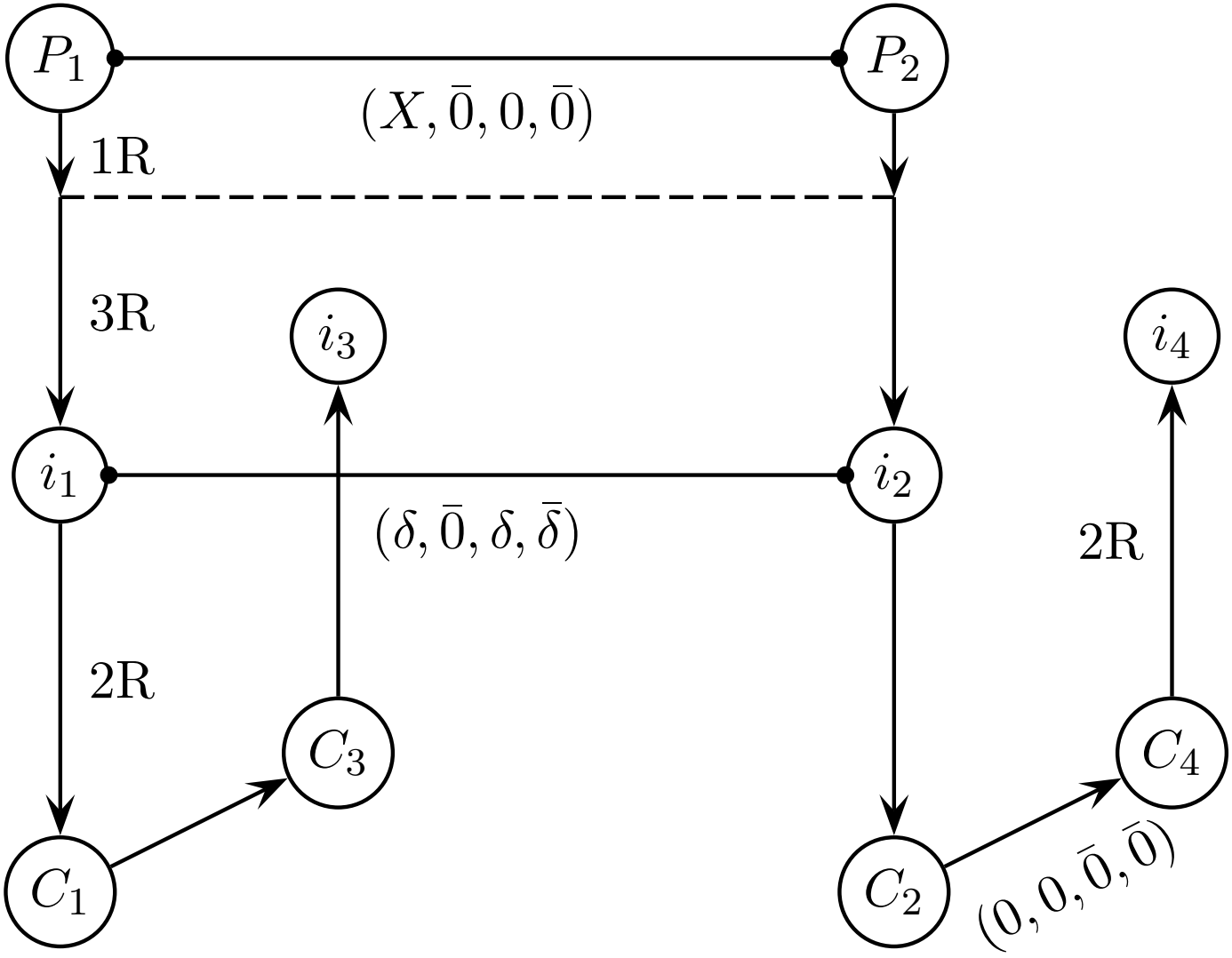
Description of B_0



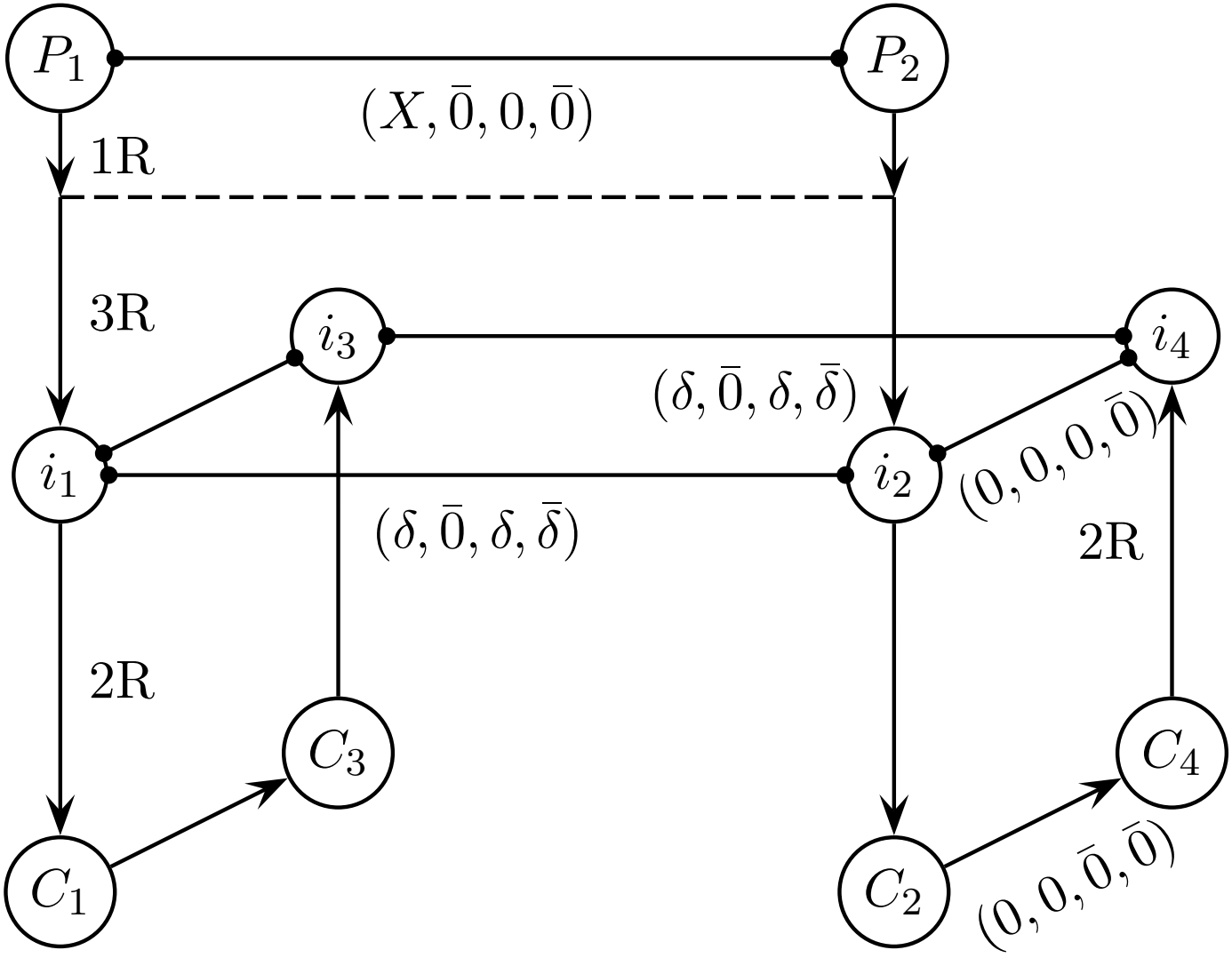
Description of B_0



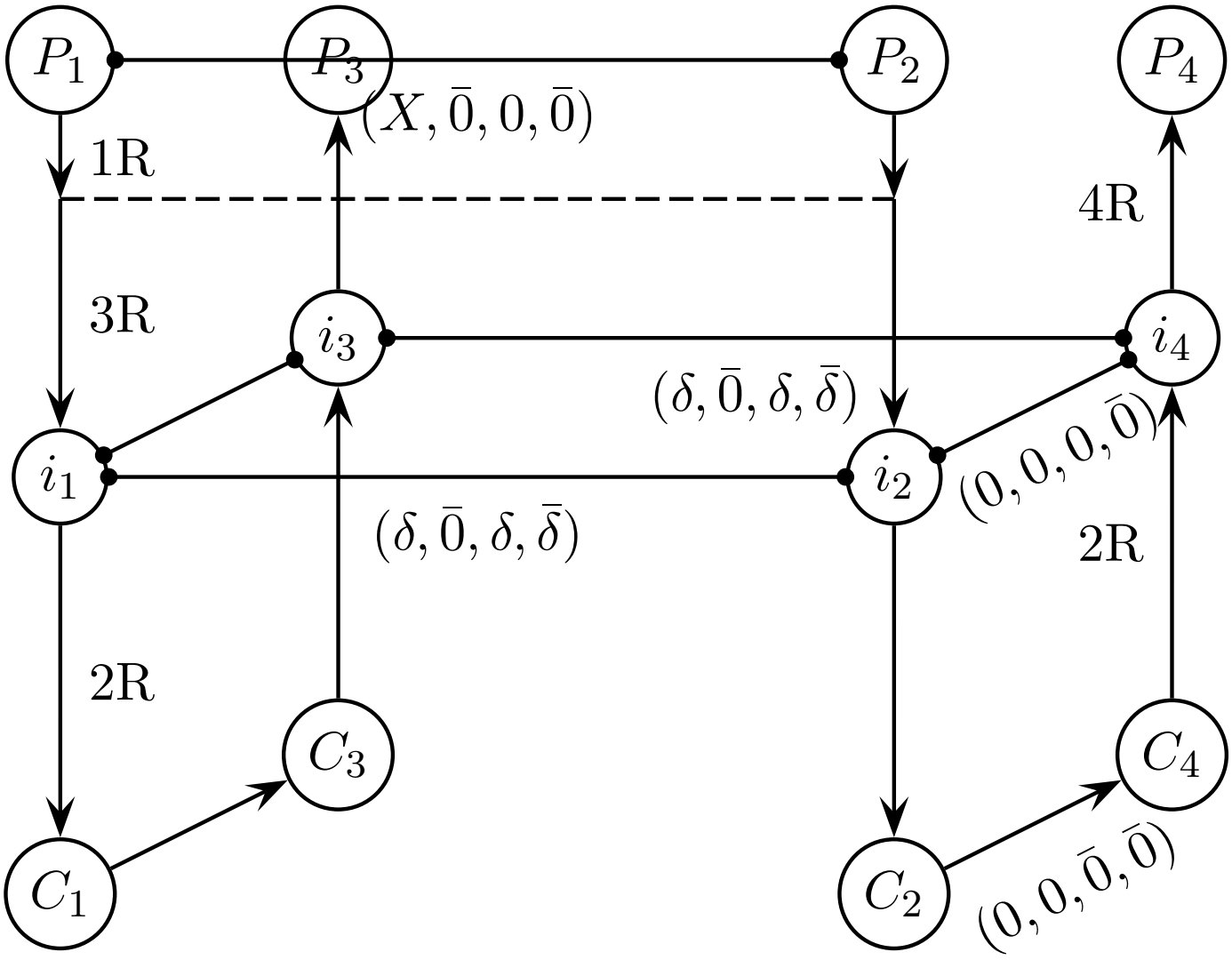
Description of B_0



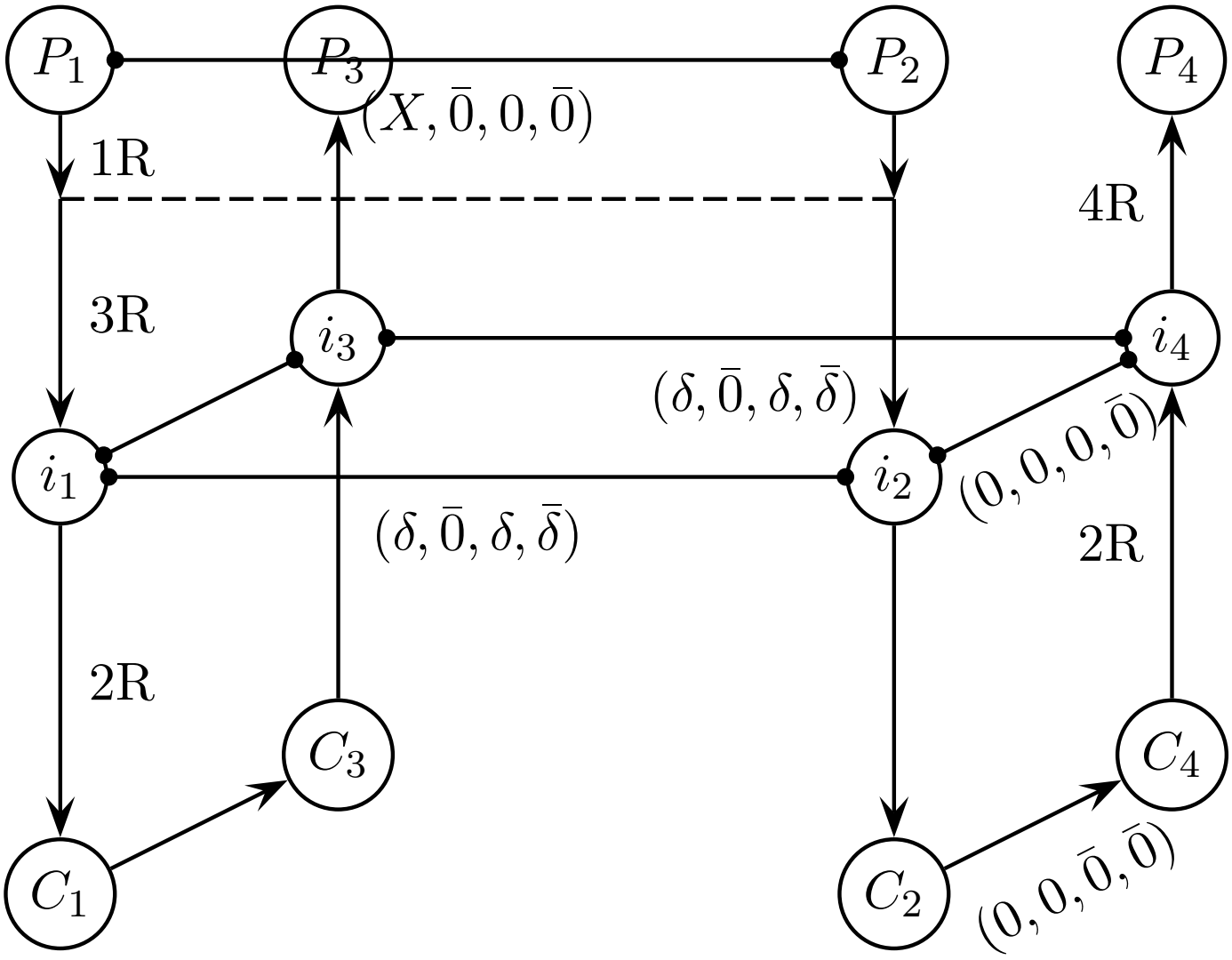
Description of B_0



Description of B_0



Description of B_0



Identifying right pairs

- Store all decrypted data in a hash-table

Identifying right pairs

- Store all decrypted data in a hash-table
- Right pairs can be identified by their collision in the appropriate 96 bits.

Identifying right pairs

- Store all decrypted data in a hash-table
- Right pairs can be identified by their collision in the appropriate 96 bits.
- It is expected that 4 right pairs will be identified.

Key Recovery

- To recover k_0 and k_3 we iterate over all possible values for that key word.

Key Recovery

- To recover k_0 and k_3 we iterate over all possible values for that key word.
- It is enough to iterate over half of the space.

Key Recovery

- To recover k_0 and k_3 we iterate over all possible values for that key word.
- It is enough to iterate over half of the space.
- Using a right pair, calculate $\omega_i = (x_i \oplus k_i) \otimes G_i$ for $i \in \{1, 3\}$. if $\omega_i = \bar{\delta}$ suggest k_i and $\bar{k_i}$ as possible keys.

Key Recovery

- To recover k_0 and k_3 we iterate over all possible values for that key word.
- It is enough to iterate over half of the space.
- Using a right pair, calculate $\omega_i = (x_i \oplus k_i) \otimes G_i$ for $i \in \{1, 3\}$. if $\omega_i = \bar{\delta}$ suggest k_i and $\bar{k_i}$ as possible keys.
- Verify using another right pair.

Recovering More Key Bits

- Note that $\bigtriangledown^* \rightarrow \bigtriangledown$ can be extended to cover 5 rounds of MMB with probability 1, i.e., all right pairs with regards to B_1 are follow this path.

Recovering More Key Bits

- Note that $\bigtriangledown^* \rightarrow \bigtriangledown$ can be extended to cover 5 rounds of MMB with probability 1, i.e., all right pairs with regards to B_1 are follow this path.
- Let (p^1, p^2) be a right pair with respect to $\bigtriangledown^* \rightarrow \bigtriangledown$, and let (c^1, c^2) be their respective ciphertexts.

Recovering More Key Bits

- Note that $\bigtriangledown^* \rightarrow \bigtriangledown$ can be extended to cover 5 rounds of MMB with probability 1, i.e., all right pairs with regards to B_1 are follow this path.
- Let (p^1, p^2) be a right pair with respect to $\bigtriangledown^* \rightarrow \bigtriangledown$, and let (c^1, c^2) be their respective ciphertexts.
- Due to the differential characteristic, the values entering γ in the fifth round are known to be $(\overline{\delta}, \overline{\delta}, 0, \overline{\delta})$.

Recovering More Key Bits

- Note that $\bigtriangledown^* \rightarrow \bigtriangledown$ can be extended to cover 5 rounds of MMB with probability 1, i.e., all right pairs with regards to B_1 are follow this path.
- Let (p^1, p^2) be a right pair with respect to $\bigtriangledown^* \rightarrow \bigtriangledown$, and let (c^1, c^2) be their respective ciphertexts.
- Due to the differential characteristic, the values entering γ in the fifth round are known to be $(\overline{\delta}, \overline{\delta}, 0, \overline{\delta})$.
- By using the two known key words, and iterating the value of k_2^6 we can reverse the last encryption round. The right key word (and its inverse) will lead to $\overline{\delta}$ in the second word.

Finding the last key word

- The last key word can be found by trying all possible key values for it, checking if some plaintext indeed leads to its ciphertext.

Finding the last key word

- The last key word can be found by trying all possible key values for it, checking if some plaintext indeed leads to its ciphertext.
- To distinguish the real key from its negation, this phase must try all possible assignments.

Complexity

- Time: $2 \cdot (4 \cdot 2^{17} + \frac{1}{6} \cdot 2^{31}) + \frac{1}{6} \cdot 2^{31} + 8 \cdot 2^{32} = 2^{35}$

Complexity

- Time: $2 \cdot (4 \cdot 2^{17} + \frac{1}{6} \cdot 2^{31}) + \frac{1}{6} \cdot 2^{31} + 8 \cdot 2^{32} = 2^{35}$
- Memory (bytes): $4 \cdot 4 \cdot 2^{17} + 4 \cdot 2^{17} = 2^{21.3}$

Complexity

- Time: $2 \cdot (4 \cdot 2^{17} + \frac{1}{6} \cdot 2^{31}) + \frac{1}{6} \cdot 2^{31} + 8 \cdot 2^{32} = 2^{35}$
- Memory (bytes): $4 \cdot 4 \cdot 2^{17} + 4 \cdot 2^{17} = 2^{21.3}$
- Data: $2 \cdot 2 \cdot 2 \cdot 2^{17} = 2^{20}$

Complexity

- Time: $2 \cdot (4 \cdot 2^{17} + \frac{1}{6} \cdot 2^{31}) + \frac{1}{6} \cdot 2^{31} + 8 \cdot 2^{32} = 2^{35}$
- Memory (bytes): $4 \cdot 4 \cdot 2^{17} + 4 \cdot 2^{17} = 2^{21.3}$
- Data: $2 \cdot 2 \cdot 2 \cdot 2^{17} = 2^{20}$
- Related-keys: 4

Experimental Verification

- All attacks has been verified using a hybrid C and Python code.
- The attack has a success rate of 98%.
- It takes less than 15 minutes on average to recover the full key of MMB.

Improvements

- Recovering 62 key bits for variants of MMB with 7 and 8 rounds.

Improvements

- Recovering 62 key bits for variants of MMB with 7 and 8 rounds.
- Recovering 31 key bits for a variant of MMB with 9 rounds.

Improvements

- Recovering 62 key bits for variants of MMB with 7 and 8 rounds.
- Recovering 31 key bits for a variant of MMB with 9 rounds.
- Time memory trade-off.

Thank you for your time. Questions?

Full Description of $\triangle \rightarrow \triangle^*$

$$\triangle =$$

$$(0,0,\bar{0},\bar{0}) \xrightarrow[(0,0,\bar{0},\bar{0})]{\sigma[\mathrm{k}^1]} (0,0,0,0) \xrightarrow{\gamma} (0,0,0,0) \xrightarrow{\eta} (0,0,0,0) \xrightarrow{\theta} (0,0,0,0)$$

$$\xrightarrow[(0,\bar{0},\bar{0},0)]{\sigma[\mathrm{k}^2]} (0,\bar{0},\bar{0},0) \xrightarrow{\gamma} (0,\bar{0},\bar{0},0) \xrightarrow{\eta} (0,\bar{0},\bar{0},0) \xrightarrow{\theta} (\bar{0},0,0,\bar{0})$$

$$\xrightarrow[(\bar{0},\bar{0},0,0)]{\sigma[\mathrm{k}^3]} (0,\bar{0},0,\bar{0}) \xrightarrow{\gamma} (0,\bar{0},0,\bar{0}) \xrightarrow{\eta} (0,\bar{0},0,\bar{\delta}) \xrightarrow{\theta} (\delta,\bar{0},\delta,\bar{\delta}) = \triangle^*$$

Back

Full Description of $\nabla^* \rightarrow \nabla$

$\nabla =$

$$(0,0,\bar{0},0) \xrightarrow[(0,0,\bar{0},0)]{\sigma[\mathrm{k}^1]} (0,0,0,0) \xrightarrow{\gamma} (0,0,0,0) \xrightarrow{\eta} (0,0,0,0) \xrightarrow{\theta} (0,0,0,0)$$

$$\xrightarrow[(0,\bar{0},0,0)]{\sigma[\mathrm{k}^2]} (0,\bar{0},0,0) \xrightarrow{\gamma} (0,\bar{0},0,0) \xrightarrow{\eta} (0,\bar{0},0,0) \xrightarrow{\theta} (\bar{0},\bar{0},\bar{0},0)$$

$$\xrightarrow[(\bar{0},0,0,0)]{\sigma[\mathrm{k}^3]} (0,\bar{0},\bar{0},0) \xrightarrow{\gamma} (0,\bar{0},\bar{0},0) \xrightarrow{\eta} (0,\bar{0},\bar{0},0) \xrightarrow{\theta} (\bar{0},0,0,\bar{0})$$

$$\xrightarrow[(0,0,0,\bar{0})]{\sigma[\mathrm{k}^4]} (\bar{0},0,0,0) \xrightarrow{\gamma} (\bar{0},0,0,0) \xrightarrow{\eta} (\bar{\delta},0,0,0) \xrightarrow{\theta} (\bar{\delta},\bar{\delta},0,\bar{\delta})$$

Back

Full Description of $\tau \rightarrow \tau^*$

$$\tau =$$

$$(0,0,0,\bar{0}) \xrightarrow[(0,0,0,\bar{0})]{\sigma[\mathrm{k}^4]} (0,0,0,0) \xrightarrow{\gamma} (0,0,0,0) \xrightarrow{\eta} (0,0,0,0) \xrightarrow{\theta} (0,0,0,0)$$

$$\xrightarrow[(0,0,\bar{0},0)]{\sigma[\mathrm{k}^5]} \xrightarrow{\gamma} (0,0,\bar{0},0) \xrightarrow{\eta} (0,0,\bar{0},0) \xrightarrow{\theta} (0,\bar{0},\bar{0},\bar{0}) = \tau^*$$

Back