A Block Cipher with Provable Security against Key Recovery

Tetsu Iwata, Yu Sasaki, Yosuke Todo, Kan Yasuda
Security from Industrial View
Security from Industrial View

• Distinguishing attacks are non-sense!!
Security from Industrial View

• Distinguishing attacks are non-sense!!

• There exists a better distinguishing attack than the one discussed in cryptographic community.
Reading Specification Attack (RSA)

- By reading specification, the implemented cipher can be distinguished easily.
Reading Specification Attack (RSA)

- By reading specification, the implemented cipher can be distinguished easily.
- For example, the cipher used in IPsec will be AES-GCM with non-negligible probability.
Reading Specification Attack (RSA)

- By reading specification, the implemented cipher can be distinguished easily.
- For example, the cipher used in IPsec will be AES-GCM with non-negligible probability.

Attack complexity

- Data:
- Time:
Reading Specification Attack (RSA)

• By reading specification, the implemented cipher can be distinguished easily.
• For example, the cipher used in IPsec will be AES-GCM with non-negligible probability

Attack complexity

• Data: 0 (no query)
• Time: 0 (no encryption, no decryption)
More on RSA

• Disadvantage

• Advantage
More on RSA

• Disadvantage
  useless if specification is unpublished

• Advantage
More on RSA

• Disadvantage
  useless if specification is unpublished

• Advantage
  always works if internationally standardized
More on RSA

• Disadvantage
  useless if specification is unpublished

• Advantage
  always works if internationally standardized
Our Goal

• Designing a new block cipher with provable security against key recovery
Our Goal

• Designing a new block cipher with provable security against key recovery

• Independent Identity Data-processing for Implementation Optimizing Transformation
Our Goal

• Designing a new block cipher with provable security against key recovery

• Independent Identity Data-processing for Implementation Optimizing Transformation
\[ K \in \{0,1\}^k \]

\[ P \xrightarrow{} E \xrightarrow{} C \]

\[ P - C \] is independent from \( K \)

\( E \) is identity mapping
DIOT: Specification

\[ K \in \{0,1\}^k \]

\[ P \rightarrow E \rightarrow C \]

\( P - C \) is independent from \( K \)

\( E \) is identity mapping

Independent-Identity Paradigm
IDIOT: Specification

\[ K \in \{0,1\}^k \]

\[ P \rightarrow E \rightarrow C \]

\( P - C \) is independent from \( K \)

\( E \) is identity mapping

Independent-Identity Paradigm

Extremely flexible interface
**IIDIOT: Specification**

\[ K \in \{0,1\}^k \]

\[ P \rightarrow E \rightarrow C \]

- \( P - C \) is independent from \( K \)
- \( E \) is identity mapping

**Independent-Identity Paradigm**

Extremely flexible interface

- Block size: chosen by the users
- Key size: chosen by the users (\( k \) bits)
Implementation
IIDIOT: Implementation

- $P = C$, the implementation cost is 0.
\( P = C \), the implementation cost is 0.

- Key register can be omitted if used in practice, but we need it for security proof.
Security
IIDIOT: Distinguisher

• Simple distinguisher
  1. Query $P$ to obtain $C$.
  2. Check if $P = C$.

Complexity: 1 KP

$K \in \{0,1\}^k$

$P \rightarrow E \rightarrow C$
IIDIOT: Distinguisher

- Simple distinguisher
  1. Query $P$ to obtain $C$.
  2. Check if $P = C$.
  Complexity: 1 KP

- This distinguisher is anyway worse than RSA (reading specification attack).

$$K \in \{0,1\}^k$$

\[ P \rightarrow E \rightarrow C \]
IIDIOT: Key Recover

• The game picks $k$ uniformly at random.  
  $$ k \leftarrow \mathcal{K} $$

• The game gives you the entire code book.  
  $$ \text{Adv} A^{P,C} $$

• Try to recover $k$.  

Comparison with AES

- Best attack against AES is exhaustive search.
- For each guess, check if $C = AES_{guess}(P)$
Comparison with AES

- Guess cannot be verified in IIDIOOT.

\[ \text{Success prob.} \]

\[ 2^{-k} \]

\[ 1 \]

\[ 0 \]

\[ 2^k \]

\[ \text{Offline comp.} \]

AES

IIDIOOT
Comparison with AES

- Guess cannot be verified in IIDIOOT.
- Provably secure against adversaries with infinite power of query and offline computation.
Concluding Remarks

• What is scientifically incorrect in IIDIOT?

• Make sure not to be as idiot as IIDIOT.

“Arigato” for your attention!!