SKINNY Cipher

Walkie_Talkie

Department of EECS
Indian Institute of Technology Bhilai

November 28, 2020

Outline

Introduction

We Observed.

Following

- Classes of ciphers

Introduction

We Observed.

Following

- Classes of ciphers
- SIMON and SPECK

Introduction

We Observed.

Following

- Classes of ciphers
- SIMON and SPECK
- Lightweight Tweakable Block ciphers and side-channel protected Impletations

Introduction

We Observed.

Following

- Classes of ciphers
- SIMON and SPECK
- Lightweight Tweakable Block ciphers and side-channel protected Impletations
- Low-Latency implementations for Memory Encryption

Outline

Specifications

Specifications of SKINNY Cipher.

Following

- Lightweight block ciphers of the SKINNY family

Specifications

Specifications of SKINNY Cipher.

Following

- Lightweight block ciphers of the SKINNY family
- It has two block versions

Specifications

Specifications of SKINNY Cipher.

Following

- Lightweight block ciphers of the SKINNY family
- It has two block versions
- 64-bit block size and 128-bit block size

Specifications

Specifications of SKINNY Cipher.

Following

- Lightweight block ciphers of the SKINNY family
- It has two block versions
- 64-bit block size and 128-bit block size
- SKINNY Follows tweakey framework

Specifications

Specifications of SKINNY Cipher.

Following

- Lightweight block ciphers of the SKINNY family
- It has two block versions
- 64-bit block size and 128-bit block size
- SKINNY Follows tweakey framework
- Variant MANTIS

Outline

Observations

We Observed.

Following

- Binary matrix used in Mix column

Observations

We Observed.

Following

- Binary matrix used in Mix column
- Very efficient implementations

Observations

We Observed.

Following

- Binary matrix used in Mix column
- Very efficient implementations
- both SW and HW

Observations

We Observed.

Following

- Binary matrix used in Mix column
- Very efficient implementations
- both SW and HW
- Almost as light as possible

Observations

Comparision.

Following

- Key alternating-cipher

Observations

Comparision.

Following

- Key alternating-cipher
- 4*4 internal state

Observations

Comparision.

Following

- Key alternating-cipher
- 4*4 internal state
- AES like SPN round

Observations

Comparision.

Following

- Key alternating-cipher
- 4*4 internal state
- AES like SPN round
- Diffusion achieved by SR+MC

Observations

Comparision.

Following

- Key alternating-cipher
- 4*4 internal state
- AES like SPN round
- Diffusion achieved by SR+MC
- added more rounds

Observations

Comparision.

Following

- Key alternating-cipher
- 4*4 internal state
- AES like SPN round
- Diffusion achieved by SR+MC
- added more rounds
- huge difference matrix

Outline

Brownie Point Nominations

Security Analysis for Skinny Cipher are based on related-key model.

Security Analysis

- Integral Attacks

Brownie Point Nominations

Security Analysis for Skinny Cipher are based on related-key model.

Security Analysis

- Integral Attacks
- Meet-In-The-Middle Attacks

Brownie Point Nominations

Security Analysis for Skinny Cipher are based on related-key model.

Security Analysis

- Integral Attacks
- Meet-In-The-Middle Attacks
- Impossible Differential Attacks

Brownie Point Nominations

Security Analysis for Skinny Cipher are based on related-key model.

Security Analysis

- Integral Attacks
- Meet-In-The-Middle Attacks
- Impossible Differential Attacks
- Differential/Linear Cryptanalysis

Brownie Point Nominations

Security Analysis for Skinny Cipher are based on related-key model.

Security Analysis

- Integral Attacks
- Meet-In-The-Middle Attacks
- Impossible Differential Attacks
- Differential/Linear Cryptanalysis
- Slide Attacks

Integral Attacks

- Cell size can be 4 or 8 bits.

Integral Attacks

- AII(A)

Integral Attacks

- Balance(B)

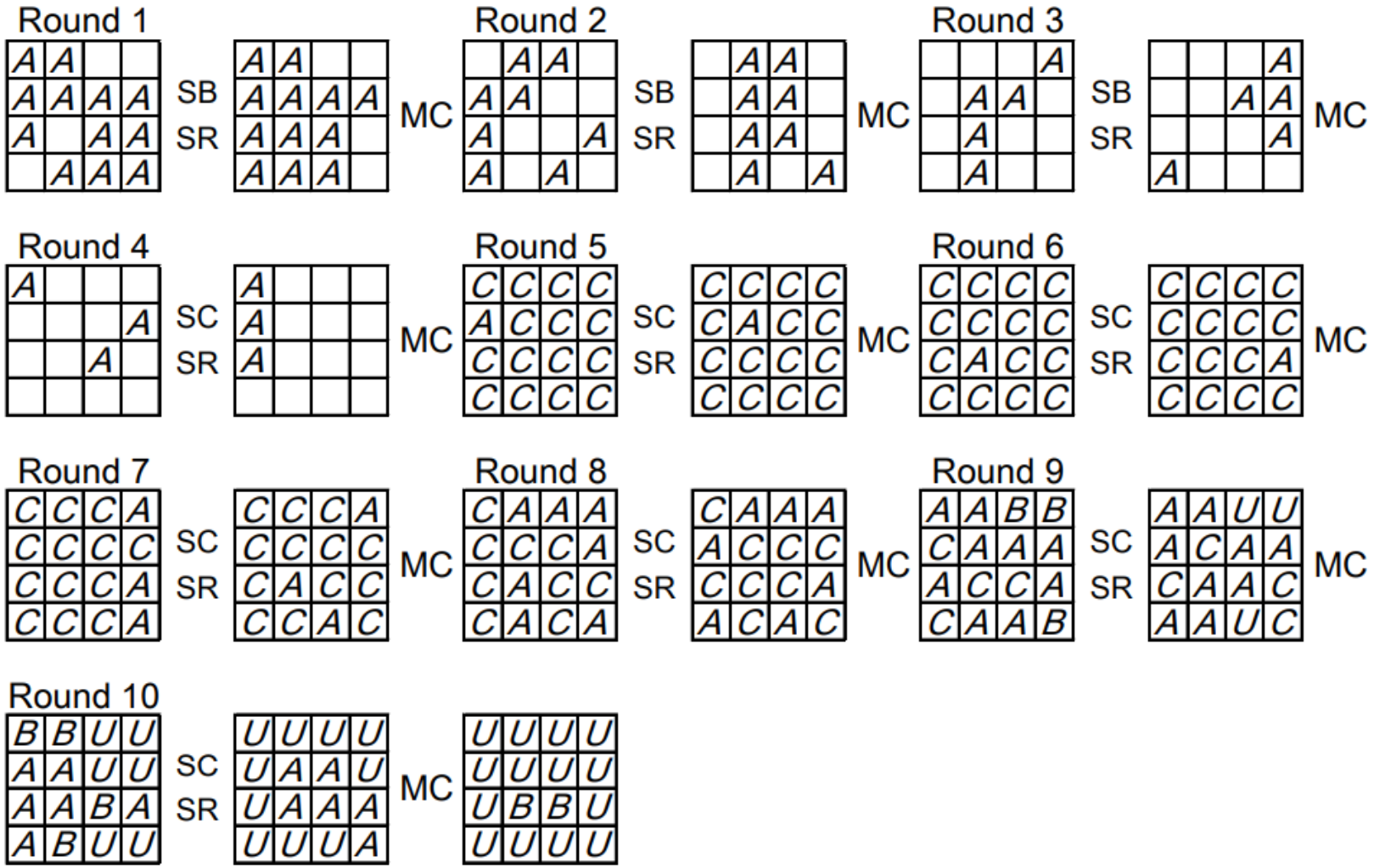
Integral Attacks

- Constant(C)

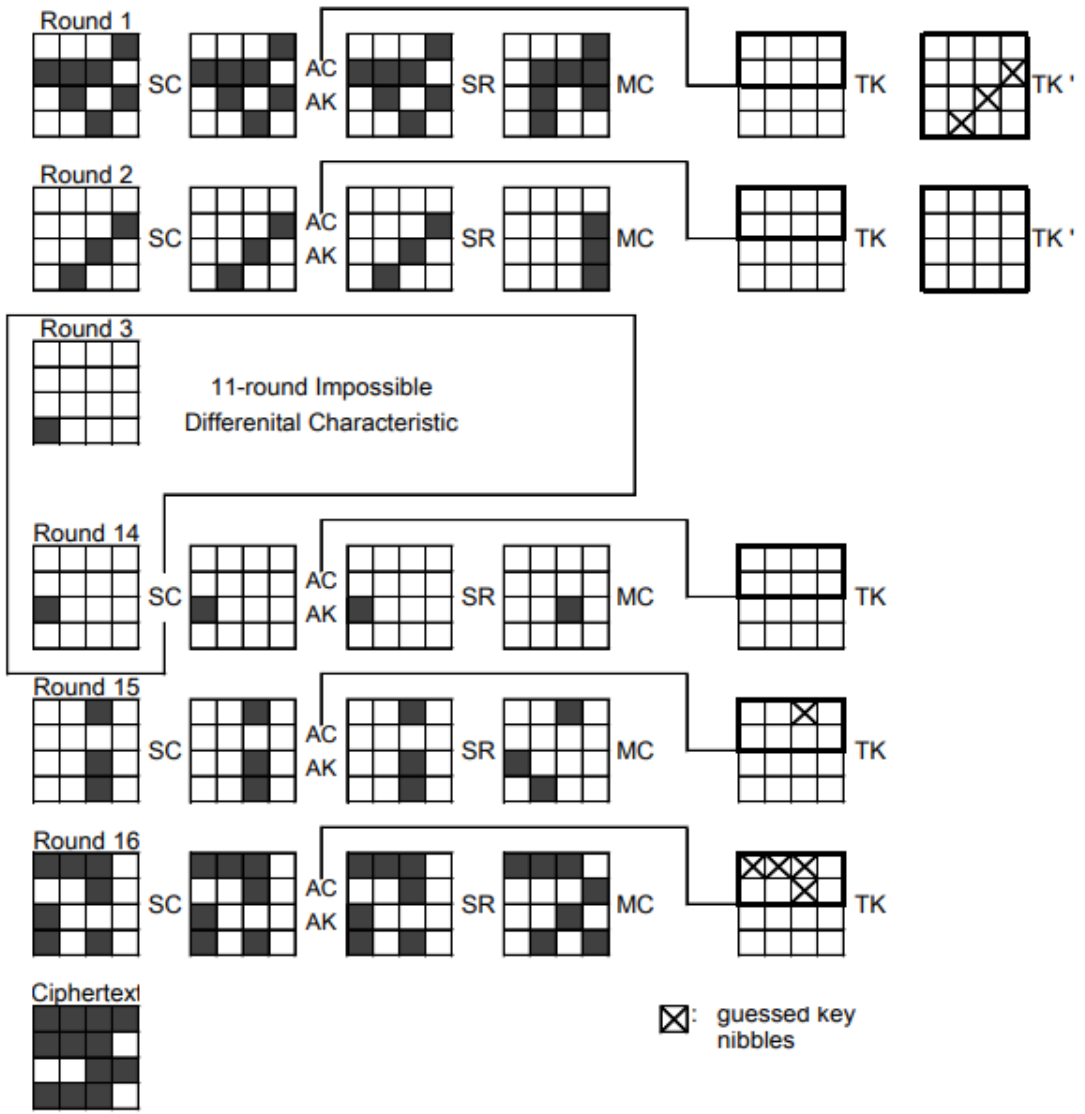
Integral Attacks

- Unknown(U)

10 round Encryption



16 round Encryption



key recovery

- prepares 2^{12c} plaintexts to form the integral distinguisher

key recovery

- prepares 2^{12c} plaintexts to form the integral distinguisher
- computes inverse MixColumns operation for each of the corresponding ciphertext,

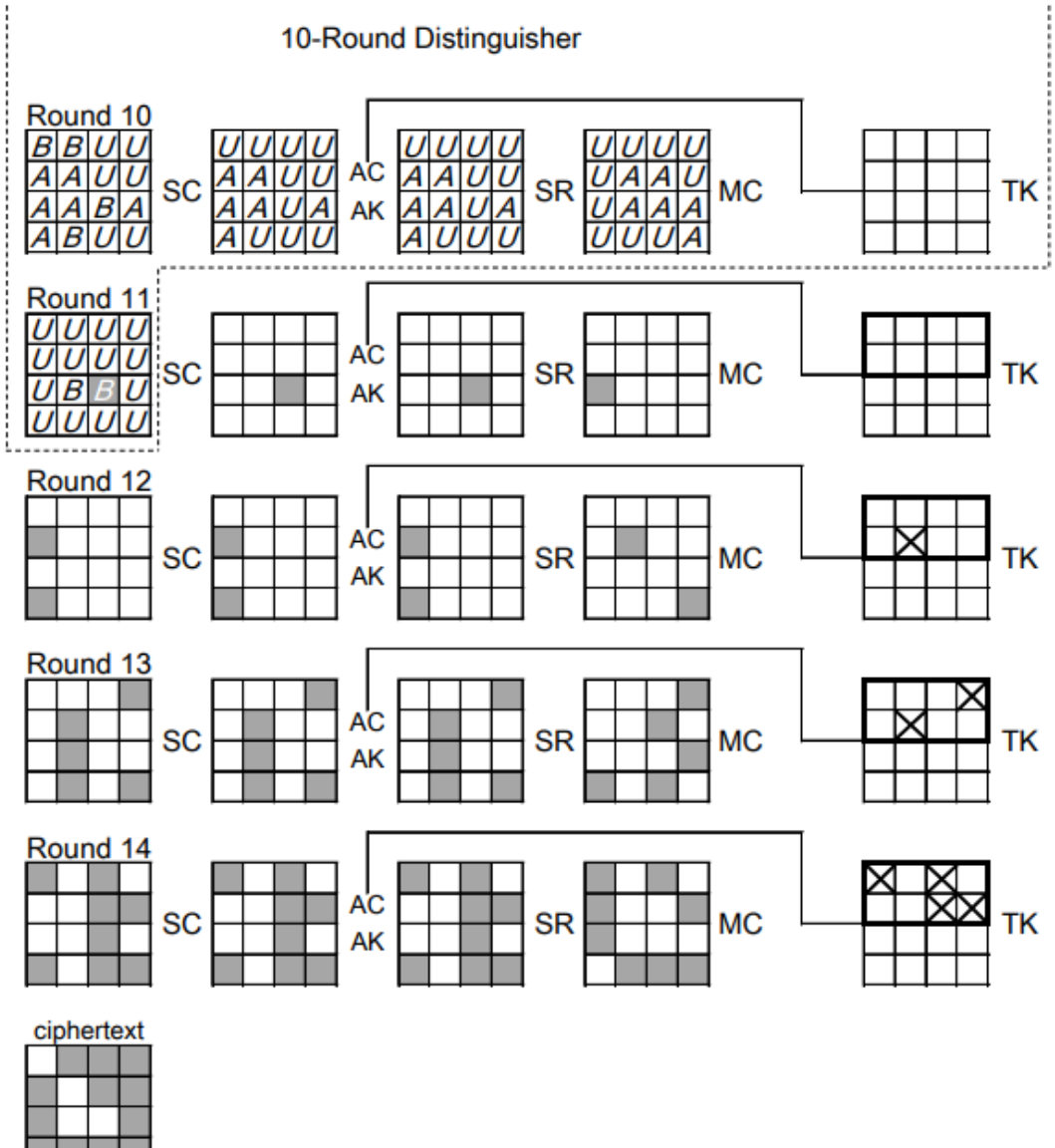
key recovery

- prepares 2^{12c} plaintexts to form the integral distinguisher
- computes inverse MixColumns operation for each of the corresponding ciphertext,
- takes parity of the 4-cell values, This reduces the remaining text size to 2^{8c} .

key recovery

- prepares 2^{12c} plaintexts to form the integral distinguisher
- computes inverse MixColumns operation for each of the corresponding ciphertext,
- takes parity of the 4-cell values, This reduces the remaining text size to 2^{8c} .
- We do this 4 time and we reach 14-round to 10-round by backward track.

key recovery



Meet-In-The-Middle Attacks

With the help of this,Number of attack rounds can be calculate by considering the maximum length of three features.Basically it work on SPN structure.

- Partial-Matching

Meet-In-The-Middle Attacks

With the help of this,Number of attack rounds can be calculate by considering the maximum length of three features.Basically it work on SPN structure.

- Initial structure

Meet-In-The-Middle Attacks

With the help of this,Number of attack rounds can be calculate by considering the maximum length of three features.Basically it work on SPN structure.

- Splice-and-cut .

Meet-In-The-Middle Attacks

With the help of this,Number of attack rounds can be calculate by considering the maximum length of three features.Basically it work on SPN structure.

- Partial-Matching
- Initial structure
- Splice-and-cut .

Outline

Conclusion

We Observed.

Following

- Rationale of SKINNY

Conclusion

We Observed.

Following

- Rationale of SKINNY
- Security analysis

Conclusion

We Observed.

Following

- Rationale of SKINNY
- Security analysis
- Implementations

Thanks

Team Members

- Ajay Tarole 11840090
- Ashish Kumar Suraj 11840230
- Vikash Vitthore 11841230

Implementation Info

- Github Link: https://github.com/ashishksuraj/Crypto-term_paper