Programming the Demirci-Selçuk Meet-in-the-Middle Attack with Constraints

Danping Shi[1] Siwei Sun[1] Patrick Derbez[2] Yosuke Todo[3] Bing Sun[4] Lei Hu[1]

[1]Institute of Information Engineering, Chinese Academy of Sciences, China

[2]Univ Rennes, CNRS, IRISA, France

[3]NTT Secure Platform Laboratories, Japan

[4]College of Liberal Arts and Sciences, National University of Defense Technology, China

Asiacrypt 2018
2018.12.4

Outlines

Outline

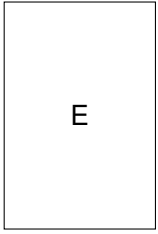
Demirci-Selçuk MITM Attack

- Demirci-Selçuk MITM, FSE 2008 [DS08].
- Various Creative Techniques:
  Differential Enumeration, Key Bridging, Key Dependent Sieve,. . . ,
  [DKS10, DFJ13, DF13, DF16, LJ16]
- General Model, Dedicated Search Algorithm [LWWZ13, DF13, DF16]

Automatic Searching methods

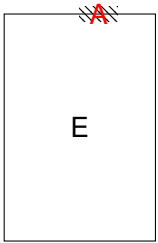
- MILP,CP,SAT,SMT
- Differential, Linear, Integral, 3-subset MITM ...
  [KLT15, SHW+14, ST17, CJF+16, XZBL16, GMS16, Sas18]

MITM Distinguisher



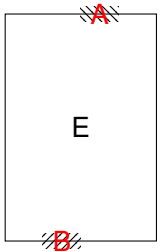
MITM Distinguisher

$\delta(A)$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



MITM Distinguisher

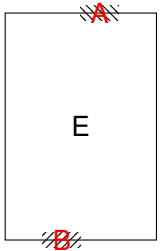
$\delta(A)$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



$\{C^0, C^1, \ldots, C^{N-1}\}$

MITM Distinguisher

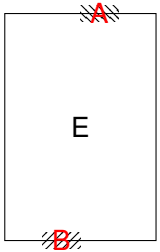
$\delta(A)$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



$\{C^0, C^1, \ldots, C^{N-1}\}$

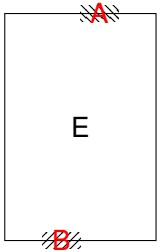
$\Delta_{\mathrm{E}}(A, B)$: $\{C^0[B] \oplus C^1[B], C^0[B] \oplus C^2[B], \ldots, C^0[B] \oplus C^{N-1}[B]\}$

Distinguisher of MITM



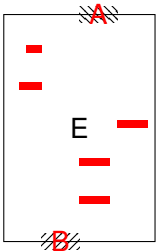
Distinguisher of MITM

- Random: $\mathcal{N}_R$



Distinguisher of MITM

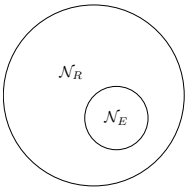
- Random: $\mathcal{N}_R$
- Block Cipher : $\mathcal{N}_E$ (saved into a hash table)

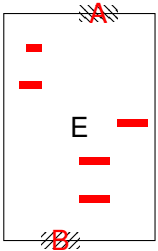


Distinguisher of MITM

- Random: $\mathcal{N}_R$
- Block Cipher : $\mathcal{N}_E$ (saved into a hash table)

Condition $\mathcal{N}_E < \mathcal{N}_R$

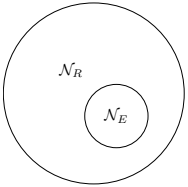


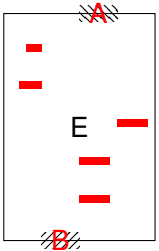


Distinguisher of MITM

- Random: $\mathcal{N}_R$
- Block Cipher : $\mathcal{N}_E$ (saved into a hash table)

Condition $\mathcal{N}_E < \mathcal{N}_R$

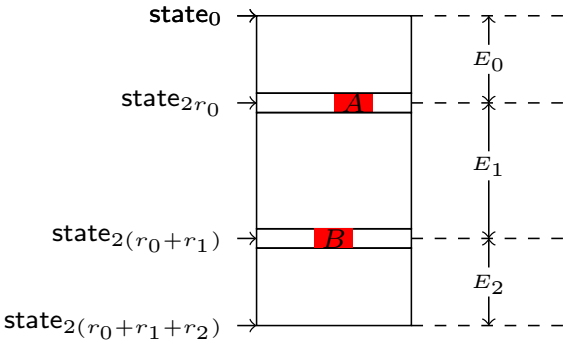




Distinguisher:$(A, B, \mathcal{N}_E)$

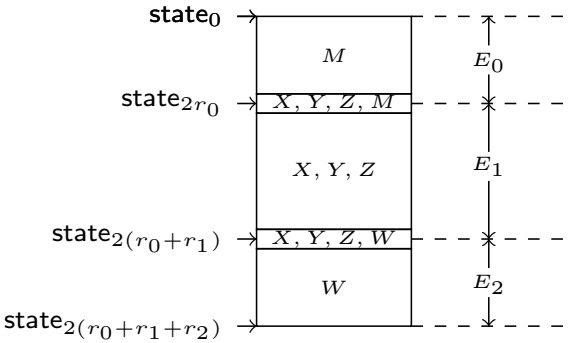
Key Recovery Attack of MITM

- A cipher is divided in three keyed permutations: E_0, E_1, E_2
- Construct distinguisher $(A, B, \mathcal{N}_E)$ at E_1



Outline

Variables



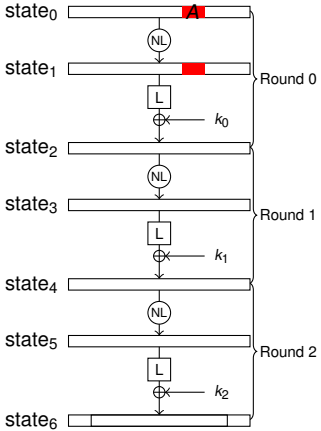
- `Var(X)` describe the forward differential
- `Var(Y)` describe the backward determination
- `Var(Z)` model the relation between `Var(X)` and `Var(Y)`

Forward differential

Variables Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$

- Var(X) for $\texttt{state}_0$
  $X_0[j] = 1$ iff j in A.
- X_r propagate to X_{r+1} with probability 1

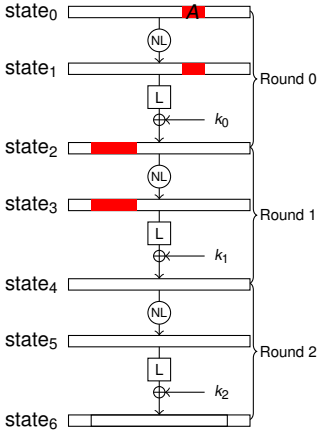


Forward differential

Variables Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$

- Var(X) for $\texttt{state}_0$
  $X_0[j] = 1$ iff j in A.
- X_r propagate to X_{r+1} with probability 1

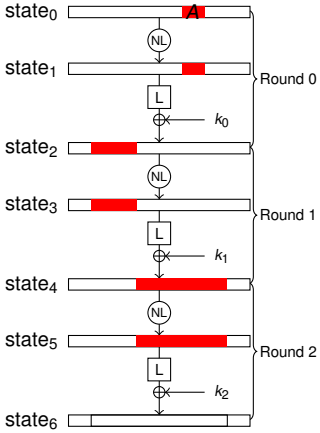


Forward differential

Variables Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$

- Var(X) for $\texttt{state}_0$
  $X_0[j] = 1$ iff j in A.
- X_r propagate to X_{r+1} with probability 1

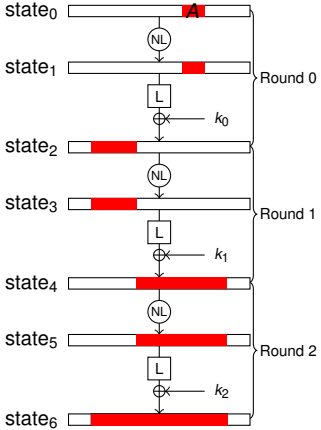


Forward differential

Variables Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$

- Var(X) for $\texttt{state}_0$
  $X_0[j] = 1$ iff j in A.
- X_r propagate to X_{r+1} with probability 1

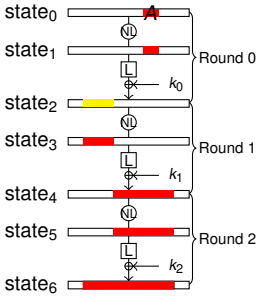


Property of forward differential

values of P^0 at the yellow states

$$\Downarrow$$

$$P_6^0 \oplus P_6^i,\ \forall i \in \{1, 2, \ldots, N-1\}$$



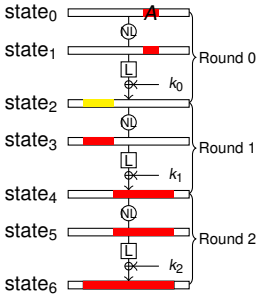
$\{P^0[A_{2r}]\}_{r\in 1,2}$ determine $P_6^0 \oplus P_6^i$

Property of forward differential

values of P^0 at the yellow states

$$\Downarrow$$

$$P_6^0 \oplus P_6^i,\ \forall i \in \{1, 2, \ldots, N-1\}$$



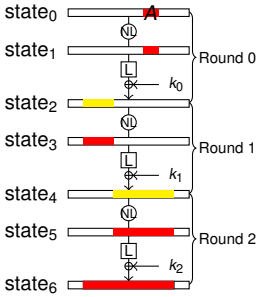
$\{P^0[A_{2r}]\}_{r\in 1,2}$ determine $P_6^0 \oplus P_6^i$

Property of forward differential

values of P^0 at the yellow states

$$\Downarrow$$

$$P_6^0 \oplus P_6^i,\ \forall i \in \{1, 2, \ldots, N-1\}$$

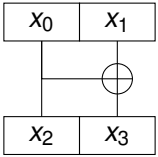


$\{P^0[A_{2r}]\}_{r\in 1,2}$ determine $P_6^0 \oplus P_6^i$

Forward Differential

Examples for Var(X)

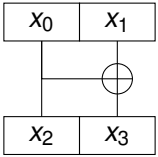
$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$



Forward Differential

Examples for Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$

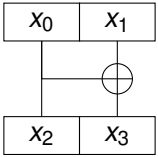


$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$

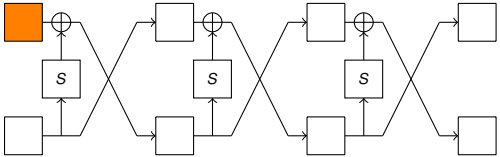
Forward Differential

Examples for Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$



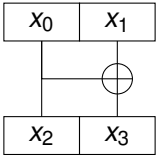
$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$

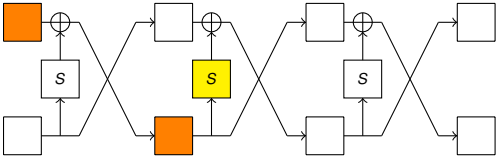


Forward Differential

Examples for Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$



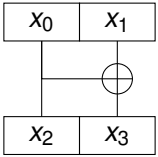


$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$

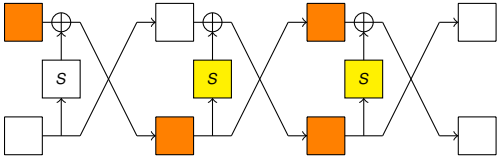
Forward Differential

Examples for Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$



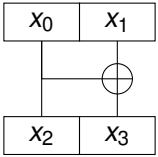
$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$

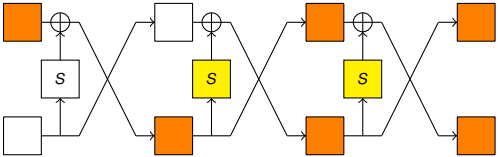


Forward Differential

Examples for Var(X)

$$X_r[j] = 0 \text{ iff } P_r^0[j] \oplus P_r^i[j] = 0, \forall i \in 1, \ldots, N-1.$$



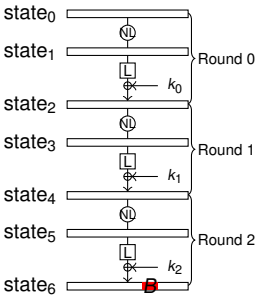


$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$

Backward determination

Variables Var(Y)

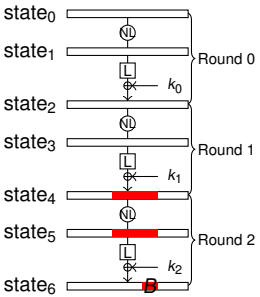
- Var(Y) for $\texttt{state}_6$
  $Y[j] = 1$ iff $j \in B$.
- Difference at B are determined by these colored positions



Backward determination

Variables Var(Y)

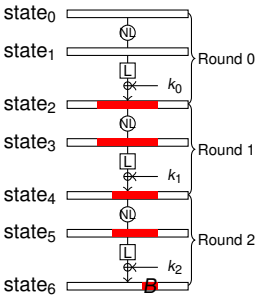
- Var(Y) for $\texttt{state}_6$
  $Y[j] = 1$ iff $j \in B$.
- Difference at B are determined by these colored positions



Backward determination

Variables Var(Y)

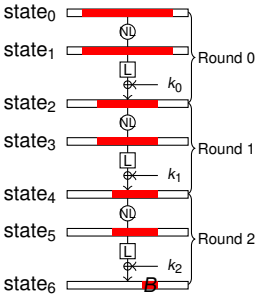
- Var(Y) for $\texttt{state}_6$
  $Y[j] = 1$ iff $j \in B$.
- Difference at B are determined by these colored positions



Backward determination

Variables Var(Y)

- Var(Y) for $\texttt{state}_6$
  $Y[j] = 1$ iff $j \in B$.
- Difference at B are determined by these colored positions

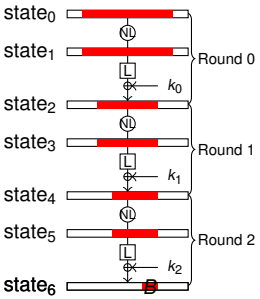


Property of backward determination

Values of P^0 at the yellow nibbles

$$\Downarrow$$

$$P_6^0 \oplus P_6^i[B], \forall i \in \{1, 2, \ldots, N\}$$



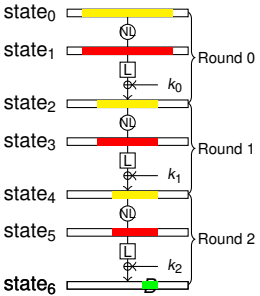
$\{P_{2r}^0[B_{2r}]\}_{r\in 0,1,2}$ determine $P_6^0[B] \oplus P_6^i[B]$

Property of backward determination

Values of P^0 at the yellow nibbles

$$\Downarrow$$

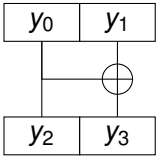
$$P_6^0 \oplus P_6^i[B], \forall i \in \{1, 2, \ldots, N\}$$



$\{P_{2r}^0[B_{2r}]\}_{r\in 0,1,2}$ determine $P_6^0[B] \oplus P_6^i[B]$

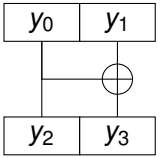
Backward determination

Examples for Var(Y)



Backward determination

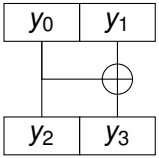
Examples for Var(Y)



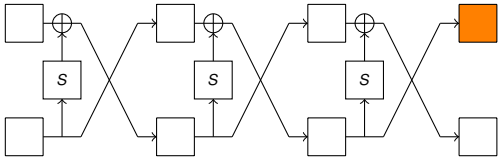
$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

Backward determination

Examples for Var(Y)

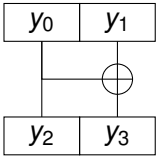


$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

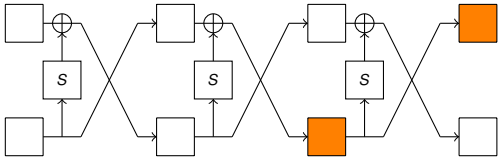


Backward determination

Examples for Var(Y)

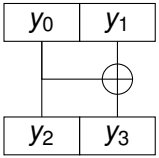


$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

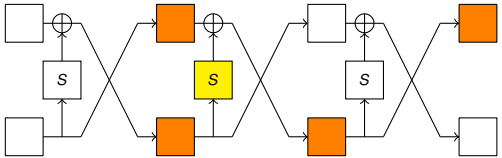


Backward determination

Examples for Var(Y)

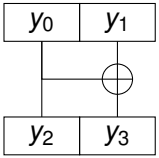


$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

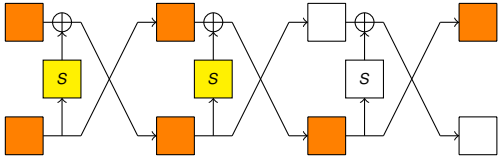


Backward determination

Examples for Var(Y)



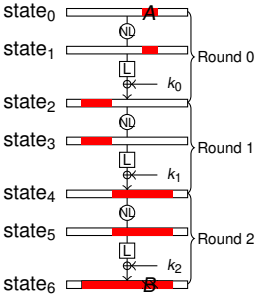
$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$



Constraints for Var(Z)

Variables Var(Z) describe the relations between Var(X) and Var(Y):

$$Z_r[j] = 1 \text{ iff } X_r[j] = Y_r[j] = 1$$

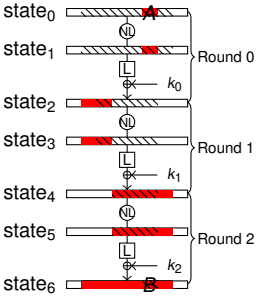


objective function: Minimize $\sum_{r=r_0+1}^{r_0+r_1-1} Z_{2r}$

Constraints for Var(Z)

Variables Var(Z) describe the relations between Var(X) and Var(Y):

$$Z_r[j] = 1 \text{ iff } X_r[j] = Y_r[j] = 1$$



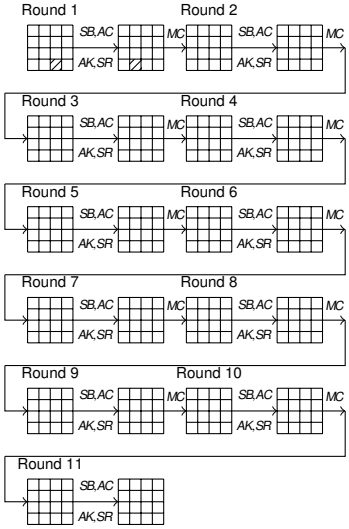
objective function: Minimize $\sum_{r=r_0+1}^{r_0+r_1-1} Z_{2r}$

Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{i,0}X_r[0]+MC_{i,1}X_r[1]+MC_{i,2}X_r[2]+MC_{i,3}X_r[3]-X_{r+1}[i] \geq 0$$

$$4X_{r+1}[i]-MC_{i,0}X_r[0]-MC_{i,1}X_r[1]-MC_{i,2}X_r[2]-MC_{i,3}X_r[3] \geq 0$$

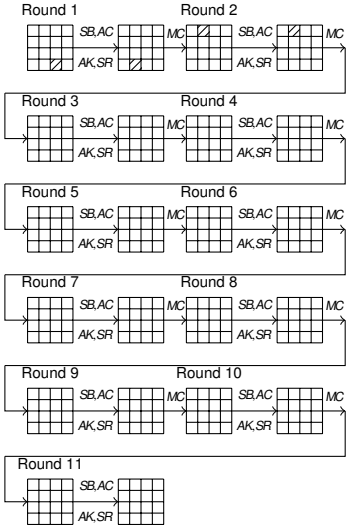


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{i,0}X_r[0]+MC_{i,1}X_r[1]+MC_{i,2}X_r[2]+MC_{i,3}X_r[3]-X_{r+1}[i] \geq 0$$

$$4X_{r+1}[i]-MC_{i,0}X_r[0]-MC_{i,1}X_r[1]-MC_{i,2}X_r[2]-MC_{i,3}X_r[3] \geq 0$$

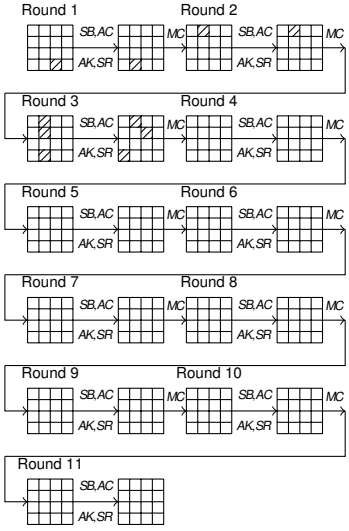


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{i,0}X_r[0]+MC_{i,1}X_r[1]+MC_{i,2}X_r[2]+MC_{i,3}X_r[3]-X_{r+1}[i] \geq 0$$

$$4X_{r+1}[i]-MC_{i,0}X_r[0]-MC_{i,1}X_r[1]-MC_{i,2}X_r[2]-MC_{i,3}X_r[3] \geq 0$$

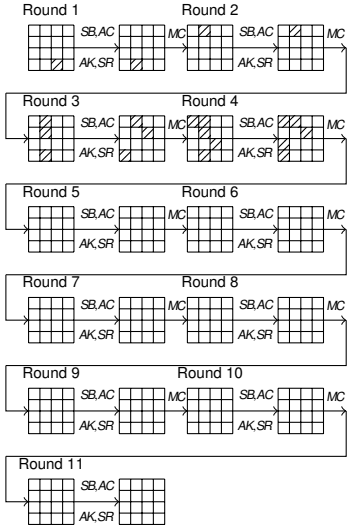


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{i,0}X_r[0]+MC_{i,1}X_r[1]+MC_{i,2}X_r[2]+MC_{i,3}X_r[3]-X_{r+1}[i] \geq 0$$

$$4X_{r+1}[i]-MC_{i,0}X_r[0]-MC_{i,1}X_r[1]-MC_{i,2}X_r[2]-MC_{i,3}X_r[3] \geq 0$$

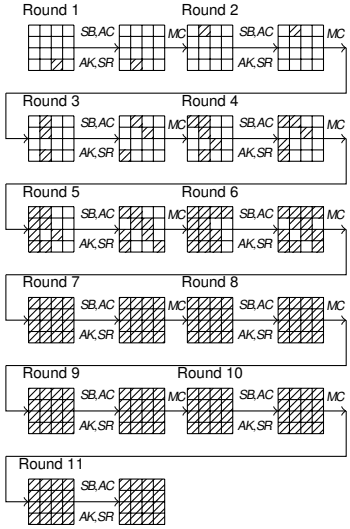


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{i,0}X_r[0]+MC_{i,1}X_r[1]+MC_{i,2}X_r[2]+MC_{i,3}X_r[3]-X_{r+1}[i] \geq 0$$

$$4X_{r+1}[i]-MC_{i,0}X_r[0]-MC_{i,1}X_r[1]-MC_{i,2}X_r[2]-MC_{i,3}X_r[3] \geq 0$$

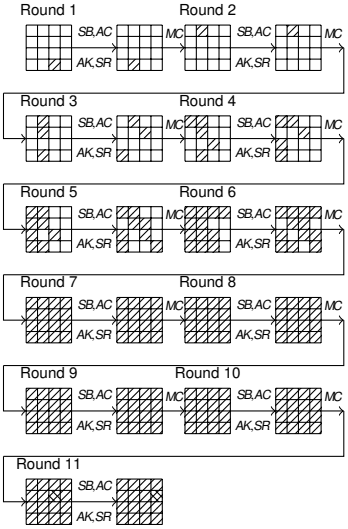


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{0,i}Y_{r+1}[0]+MC_{1,i}Y_{r+1}[1]+MC_{2,i}Y_{r+1}[2]+MC_{3,i}Y_{r+1}[3]-Y_r[i] \geq 0$$

$$4Y_r[i]-MC_{0,i}Y_{r+1}[0]-MC_{1,i}Y_{r+1}[1]-MC_{2,i}Y_{r+1}[2]-MC_{3,i}Y_{r+1}[3] \geq 0$$

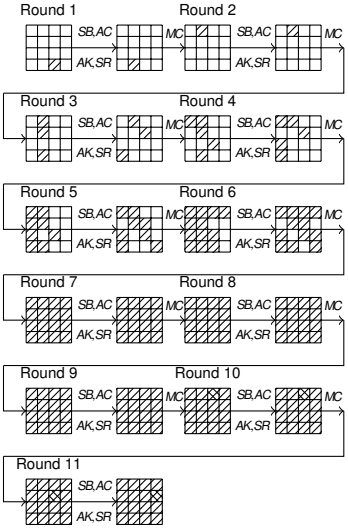


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{0,i}Y_{r+1}[0]+MC_{1,i}Y_{r+1}[1]+MC_{2,i}Y_{r+1}[2]+MC_{3,i}Y_{r+1}[3]-Y_r[i] \geq 0$$

$$4Y_r[i]-MC_{0,i}Y_{r+1}[0]-MC_{1,i}Y_{r+1}[1]-MC_{2,i}Y_{r+1}[2]-MC_{3,i}Y_{r+1}[3] \geq 0$$

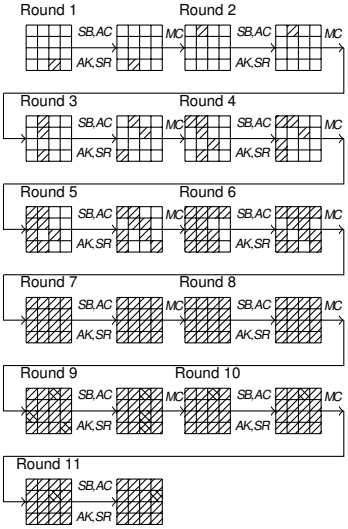


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{0,i}\,Y_{r+1}[0] + MC_{1,i}\,Y_{r+1}[1] + MC_{2,i}\,Y_{r+1}[2] + MC_{3,i}\,Y_{r+1}[3] - Y_r[i] \geq 0$$

$$4\,Y_r[i] - MC_{0,i}\,Y_{r+1}[0] - MC_{1,i}\,Y_{r+1}[1] - MC_{2,i}\,Y_{r+1}[2] - MC_{3,i}\,Y_{r+1}[3] \geq 0$$

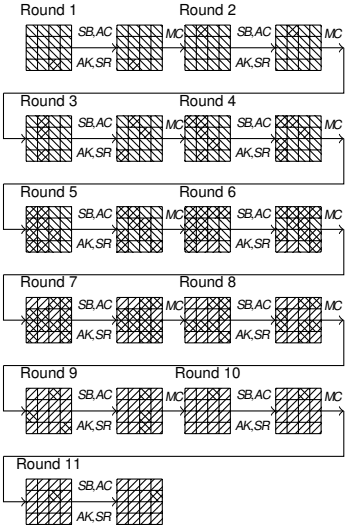


Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

$$MC_{0,i}Y_{r+1}[0]+MC_{1,i}Y_{r+1}[1]+MC_{2,i}Y_{r+1}[2]+MC_{3,i}Y_{r+1}[3]-Y_r[i] \geq 0$$

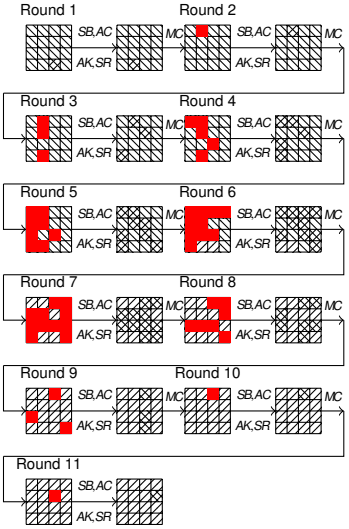
$$4Y_r[i]-MC_{0,i}Y_{r+1}[0]-MC_{1,i}Y_{r+1}[1]-MC_{2,i}Y_{r+1}[2]-MC_{3,i}Y_{r+1}[3] \geq 0$$



Application to SKINNY

- Proposed at CRYPTO 2016
- $MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

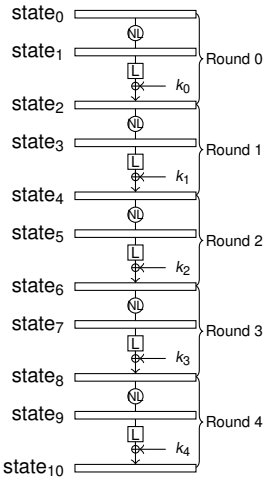
$$MC_{0,i}Y_{r+1}[0]+MC_{1,i}Y_{r+1}[1]+MC_{2,i}Y_{r+1}[2]+MC_{3,i}Y_{r+1}[3]-Y_r[i] \geq 0$$
$$4Y_r[i]-MC_{0,i}Y_{r+1}[0]-MC_{1,i}Y_{r+1}[1]-MC_{2,i}Y_{r+1}[2]-MC_{3,i}Y_{r+1}[3] \geq 0$$



New 0-1 variables Var(M) for E_0

Var(M): Determine the plaintext structure

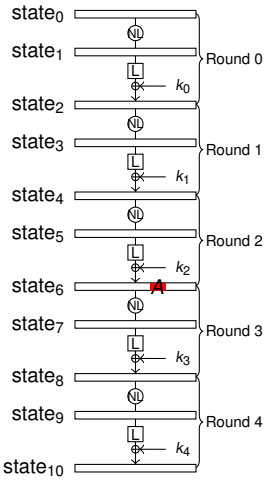
- $M_{2r_0} = X_{2r_0}$
- backward differential propagation with probability 1.
- forward differential through E_0^{-1}:



New 0-1 variables Var(M) for E_0

Var(M): Determine the plaintext structure

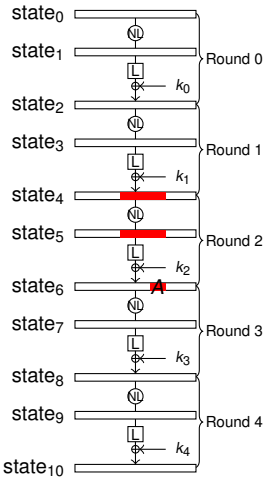
- $M_{2r_0} = X_{2r_0}$
- backward differential propagation with probability 1.
- forward differential through E_0^{-1}:



New 0-1 variables Var(M) for E_0

Var(M): Determine the plaintext structure

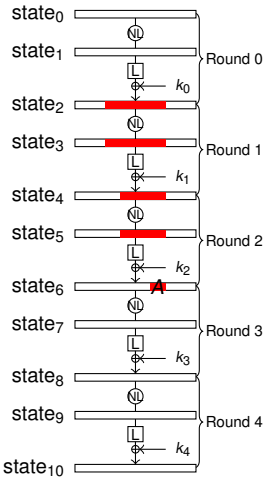
- $M_{2r_0} = X_{2r_0}$
- backward differential propagation with probability 1.
- forward differential through E_0^{-1}:



New 0-1 variables Var(M) for E_0

Var(M): Determine the plaintext structure

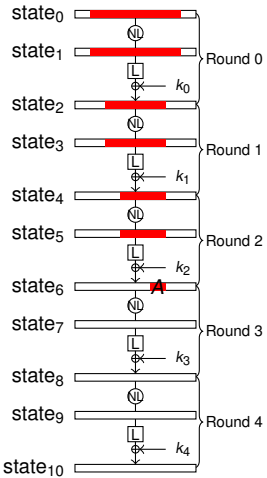
- $M_{2r_0} = X_{2r_0}$
- backward differential propagation with probability 1.
- forward differential through E_0^{-1}:



New 0-1 variables Var(M) for E_0

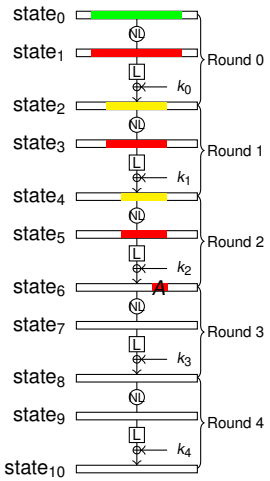
Var(M): Determine the plaintext structure

- $M_{2r_0} = X_{2r_0}$
- backward differential propagation with probability 1.
- forward differential through E_0^{-1}:



Property of backward differential

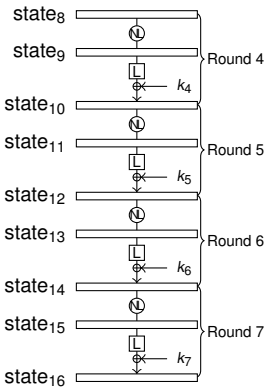
- Guess the values of P^0 at the yellow state
- obtain $\{P^0, P^1, \ldots, P^{N-1}\}$ s.t. $\{P_6^0, P_6^1, \ldots, P_6^{N-1}\}$ is $\delta(A)$-set



New 0-1 variables Var(W) for E_2

Var(W): forward determination process

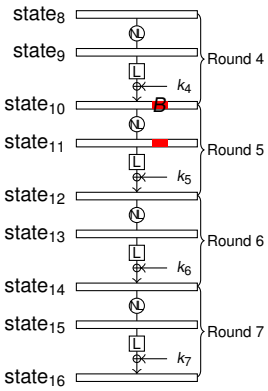
- $W_{10} = Y_{10}$
- backward determination through E_2^{-1}:



New 0-1 variables Var(W) for E_2

Var(W): forward determination process

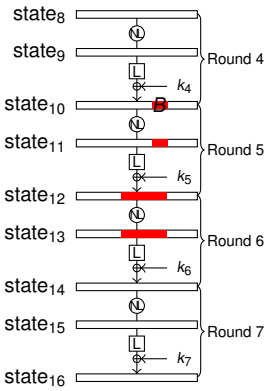
- $W_{10} = Y_{10}$
- backward determination through E_2^{-1}:



New 0-1 variables Var(W) for E_2

Var(W): forward determination process

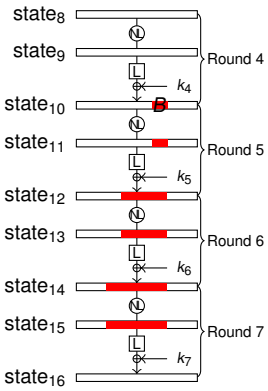
- $W_{10} = Y_{10}$
- backward determination through E_2^{-1}:



New 0-1 variables Var(W) for E_2

Var(W): forward determination process

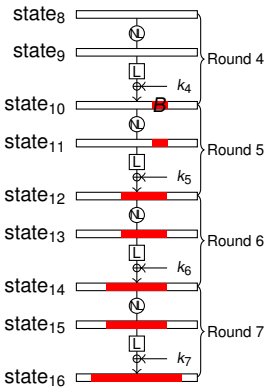
- $W_{10} = Y_{10}$
- backward determination through E_2^{-1}:



New 0-1 variables Var(W) for E_2

Var(W): forward determination process

- $W_{10} = Y_{10}$
- backward determination through E_2^{-1}:

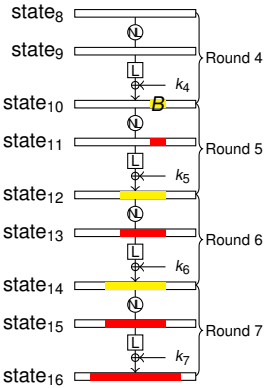


Property of Forward Determination

Guess the values of P^0 at yellow states

$\Downarrow$

Obtain sequence $\Delta_{\mathrm{E}}(A, B)$ at $\mathtt{state}_{10}$

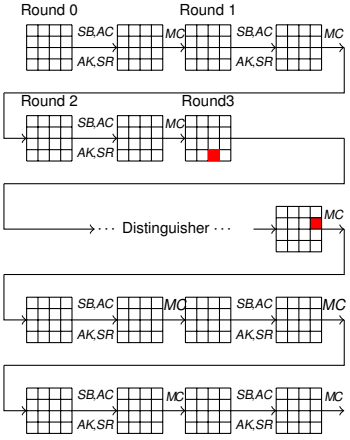


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

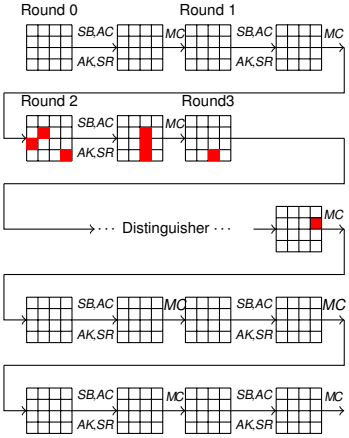


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

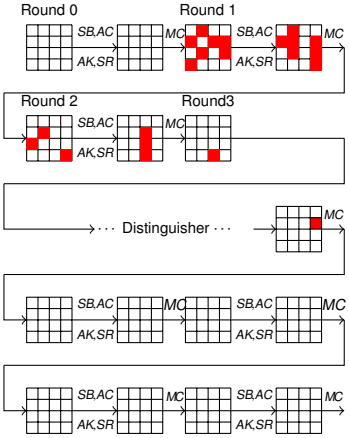


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

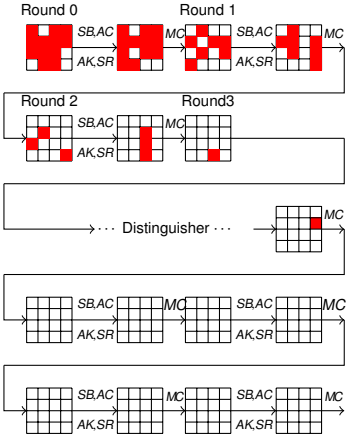


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

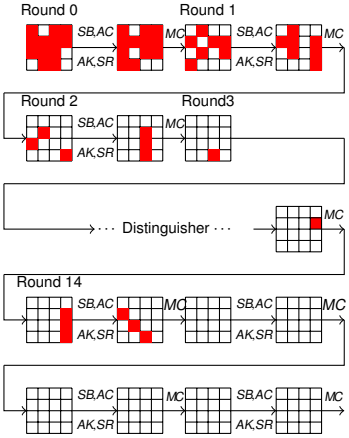


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

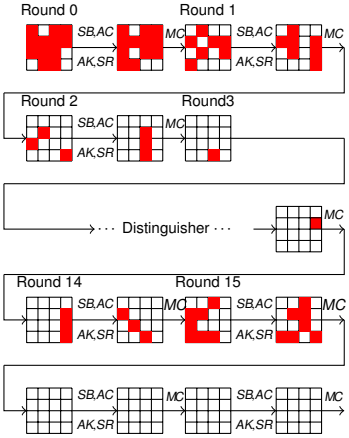


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

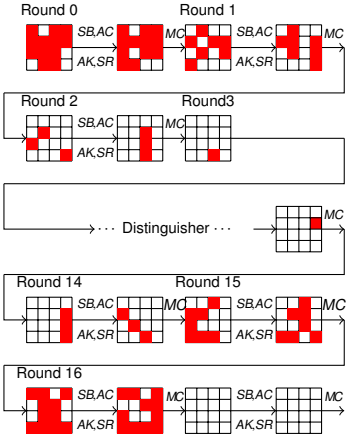


Examples for Var(M) and Var(W)

Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination

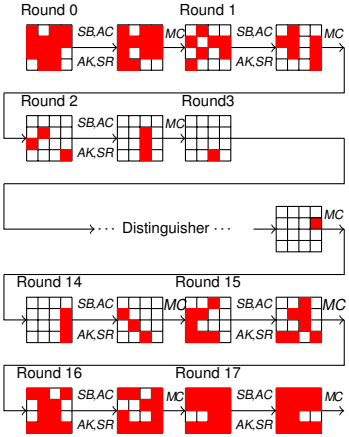


Examples for Var(M) and Var(W)

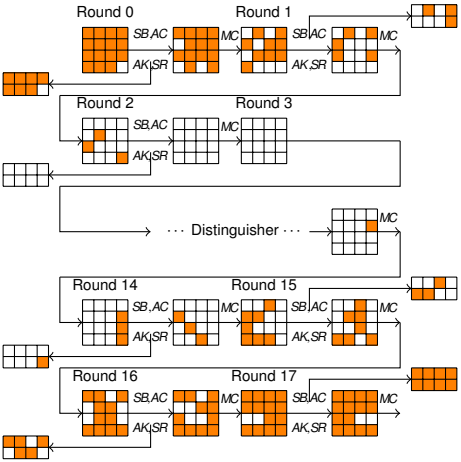
Var(M): Backward differential

$$MC^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Var(W): Forward determination



Guessed Subkeys

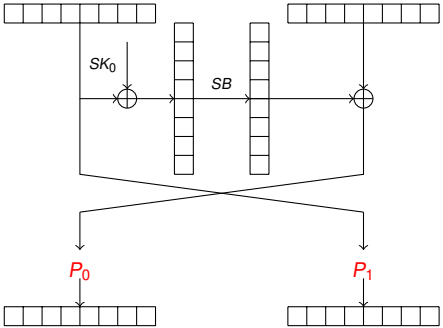


Results

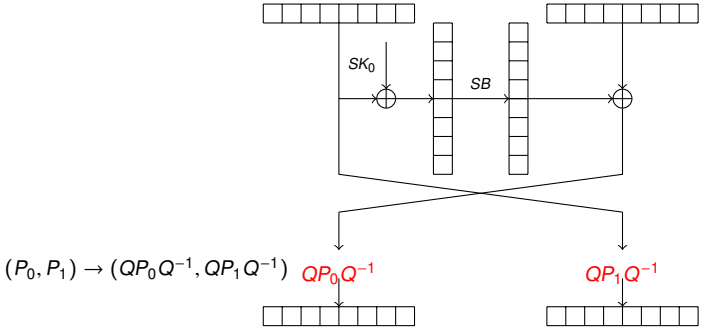
Target	Rounds	Time	Data	Memory	Method	Ref
LBlock	$11+10$	$2^{70.20}$	2^{48} CP	$2^{61.91}$	$\mathcal{DS}$-MITM	Sect. 7.2
	$9+0$	$2^{74.5}$	–	–	$\mathcal{DS}$-MITM Dist.	[43]
	23	$2^{74.5}$	$2^{59.5}$CP	$2^{74.3}$	ID	[47]
	23	$2^{75.36}$	2^{59}CP	2^{74}	ID	[48]
	23	2^{72}	$2^{62.1}$ Kp	2^{60}	MultiD ZC	[47]
	23	2^{76}	$2^{62.1}$ Kp	2^{60}	MultiD ZC	[49]
TWINE80	$11+9$	$2^{77.44}$	2^{32} CP	$2^{82.91}$	$\mathcal{DS}$-MITM	Sect. 7.3
	23	$2^{79.09}$	$2^{57.85}$ CP	$2^{84.06}$	ID	[50]
	23	2^{73}	$2^{62.1}$ KP	2^{60}	MultiD ZC	[47]
TWINE128	$11+14$	$2^{124.7}$	2^{48} CP	2^{109}	$\mathcal{DS}$-MITM*	[34]
	25	$2^{124.5}$	$2^{59.1}$ CP	$2^{78.1}$	ID	[34]
	25	2^{119}	$2^{62.1}$ KP	2^{60}	MultiD ZC	[47]
	25	$2^{122.12}$	$2^{62.1}$ KP	2^{60}	MultiD ZC	[49]
SKINNY-128-384	$10.5+11.5$	$2^{382.46}$	2^{96} CP	$2^{330.99}$	$\mathcal{DS}$-MITM	Sect. 7.1
	$11+11$	$2^{373.48}$	$2^{92.22}$ CP	$2^{147.22}$	ID	[51]

$\star$ We find the attacks with the same complexity.

Outline



Enumeration: $8! \cdot 8!$



Enumeration: $8! \cdot 8! \rightarrow 22 \cdot 8!$

Results

- 144 permutations: no 15-round IM Distinguisher.
- 12 permutations may be best: no 11-round `MITM` distinguisher

Outline

Conclusion

Conclusion

- modelling the `MITM` attack
- IM and `MITM` for variants cipher of LBlock and TWINE

Future Work

- Differential Enumeration
- Key Bridging
- ...

References I

Tingting Cui, Keting Jia, Kai Fu, Shiyao Chen, and Meiqin Wang.
New automatic search tool for impossible differentials and zero-correlation linear approximations.
IACR Cryptology ePrint Archive, 2016:689, 2016.

Patrick Derbez and Pierre-Alain Fouque.
Exhausting demirci-selçuk meet-in-the-middle attacks against reduced-round AES.
In *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, pages 541–560, 2013.

Patrick Derbez and Pierre-Alain Fouque.
Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks.
In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 157–184, 2016.

Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean.
Improved key recovery attacks on reduced-round AES in the single-key setting.
In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 371–387, 2013.

References II

Orr Dunkelman, Nathan Keller, and Adi Shamir.
Improved single-key attacks on 8-round AES-192 and AES-256.
In *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, pages 158–176, 2010.

Hüseyin Demirci and Ali Aydin Selçuk.
A meet-in-the-middle attack on 8-round AES.
In *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, pages 116–126, 2008.

David Gerault, Marine Minier, and Christine Solnon.
Constraint programming models for chosen key differential cryptanalysis.
In *Principles and Practice of Constraint Programming - 22nd International Conference, CP 2016, Toulouse, France, September 5-9, 2016, Proceedings*, pages 584–601, 2016.

Stefan Kölbl, Gregor Leander, and Tyge Tiessen.
Observations on the SIMON block cipher family.
In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 161–185, 2015.

References III

Rongjia Li and Chenhui Jin.
Meet-in-the-middle attacks on 10-round AES-256.
Des. Codes Cryptography, 80(3):459–471, 2016.

Li Lin, Wenling Wu, Yanfeng Wang, and Lei Zhang.
General model of the single-key meet-in-the-middle distinguisher on the word-oriented block cipher.
In *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, pages 203–223, 2013.

Yu Sasaki.
Integer linear programming for three-subset meet-in-the-middle attacks: Application to gift.
pages 227–243, 2018.

Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song.
Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers.
In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, pages 158–178, 2014.

References IV

Yu Sasaki and Yosuke Todo.
New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers.
In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, pages 185–215, 2017.

Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin.
Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers.
In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, pages 648–678, 2016.

Thanks for your attention.