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]Universit Rennes 1 / IRISA

[3]NTT Secure Platform Laboratories

[4]College of Science, National University of Defense Technology,China

ASK2017 2017.12.11

Outlines

Outline

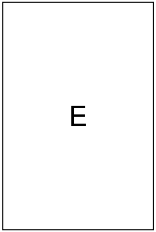
Automatic Cryptanalysis

- Dedicated search
- MILP,CP,SAT,SMT

Searching methods for MITM

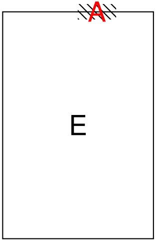
- Demirci-Selçuk MITM, FSE 2008.
- Derbez and Fouque: Dedicated search algorithm
- Li Lin, Wenling Wu: General model based on MILP

MITM Distinguisher



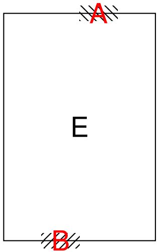
MITM Distinguisher

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



MITM Distinguisher

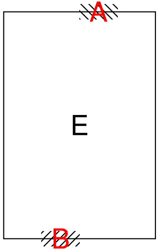
$\delta(A)$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



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

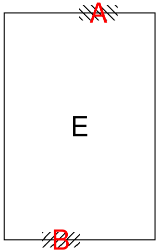
MITM Distinguisher

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

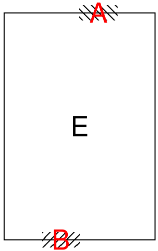


$\{C^0, C^1, \ldots, C^{N-1}\}$

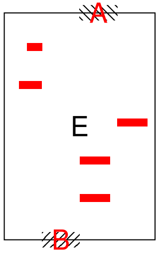
$\Delta_{\mathtt{E}}(A, B)$: $\{C^0[B] \oplus C^1[B], C^0[B] \oplus C^2[B], \ldots, C^0[B] \oplus C^{N-1}[B]\}$


A
E
B

- Random Cipher: $\mathcal{N}_R$

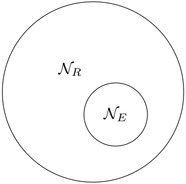


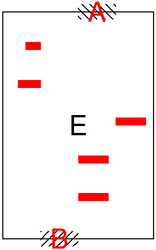
- Random Cipher: $\mathcal{N}_R$
- Block Cipher : $\mathcal{N}_E$ (save into a hash table)



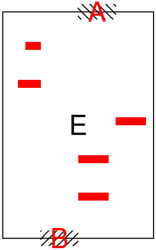
- Random Cipher: $\mathcal{N}_R$
- Block Cipher : $\mathcal{N}_E$ (save into a hash table)

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

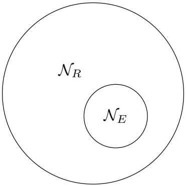




- Random Cipher: $\mathcal{N}_R$
- Block Cipher : $\mathcal{N}_E$ (save into a hash table)



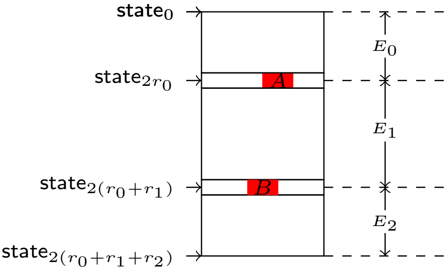
Condition $\mathcal{N}_E < \mathcal{N}_R$



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

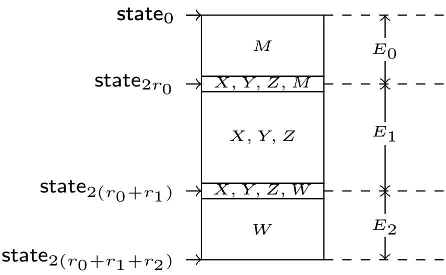
Structure of the attack

- 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

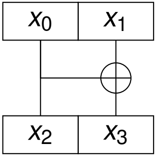


- `Var(X)` describe the forward differential
- `Var(Y)` describe the backward determination
- `Var(Z)` models the relation between `Var(X)` and `Var(Y)`

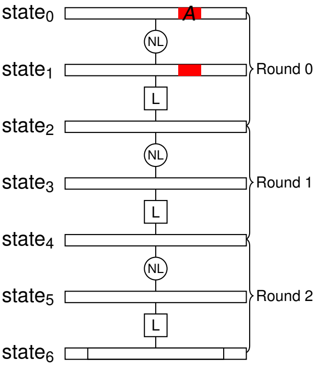
Forward differential

Variables `Var(X)`

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



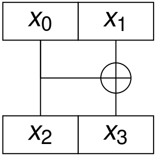
$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$



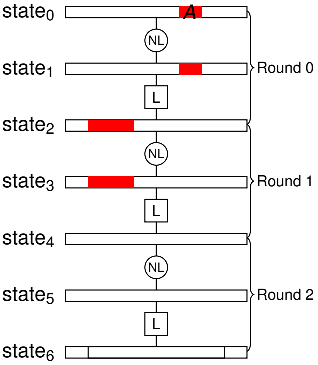
Forward differential

Variables Var(X)

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



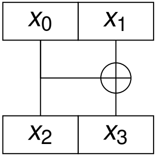
$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$



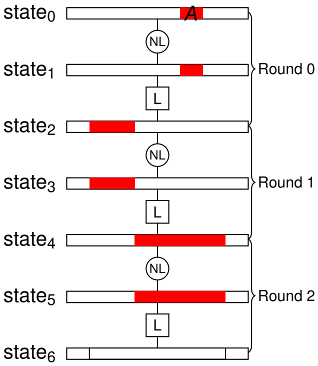
Forward differential

Variables `Var(X)`

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



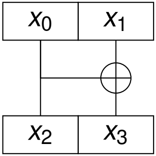
$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$



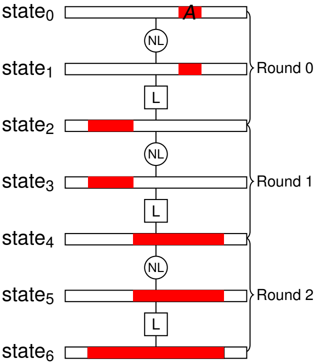
Forward differential

Variables Var(X)

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

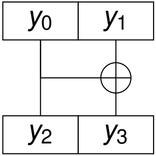


$$\begin{aligned} x_2 &= x_0 \\ 2x_3 &\geq x_0 + x_1 \\ x_3 &\leq x_0 + x_1 \end{aligned}$$

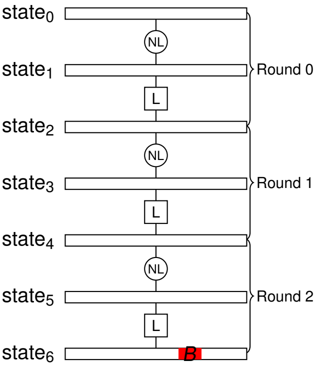


Backward determination

Variables Var(Y)

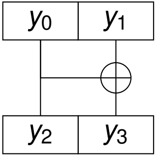


$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

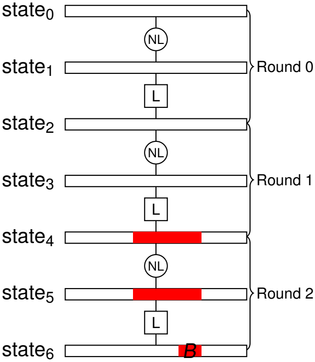


Backward determination

Variables `Var(Y)`

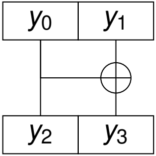


$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

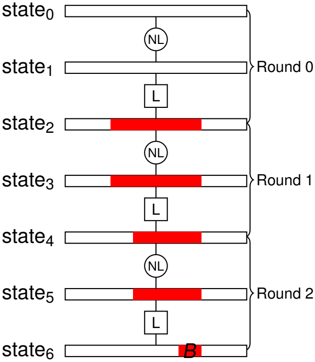


Backward determination

Variables Var(Y)

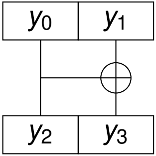


$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$

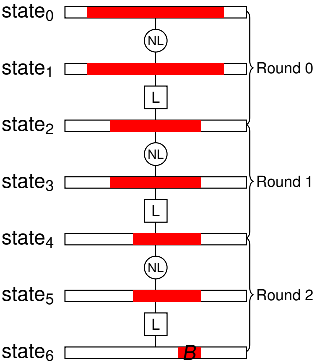


Backward determination

Variables Var(Y)



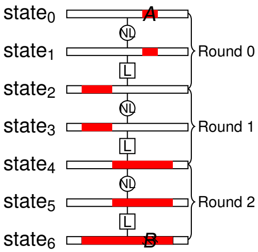
$$
\begin{aligned}
y_2 + y_3 &\leq 2y_0 \\
y_2 + y_3 &\geq y_0 \\
y_1 &= y_3
\end{aligned}
$$



Constraints for Var(Z)

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

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

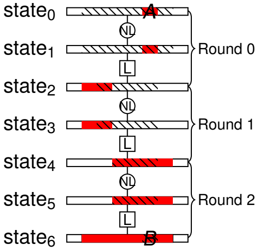


objective function: Minimize $\sum_{r=r_0+1}^{r_0+r_1-1} Z_{2r}$

Constraints for Var(Z)

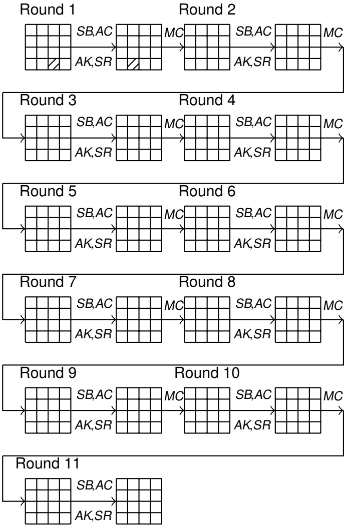
Variables `Var(Z)` describe the relation between `Var(X)` and `Var(Y)`:

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

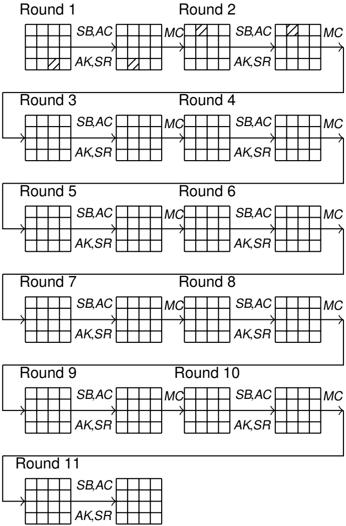


objective function: Minimize $\sum_{r=r_0+1}^{r_0+r_1-1} Z_{2r}$

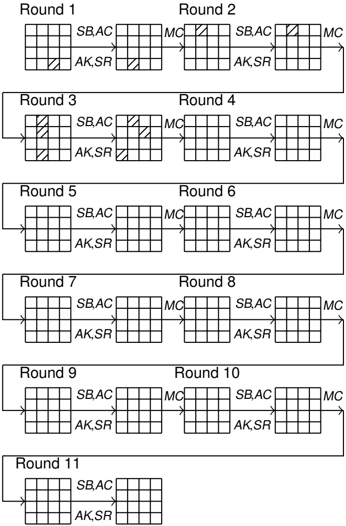
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



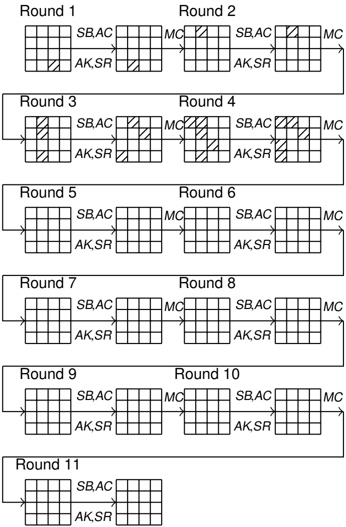
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



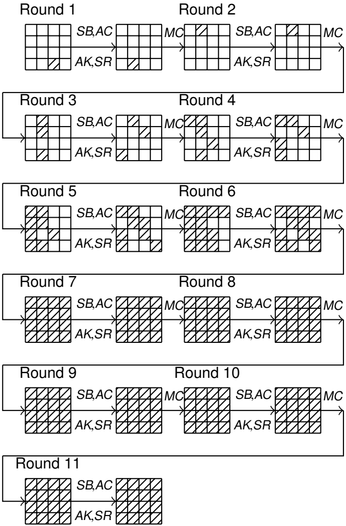
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



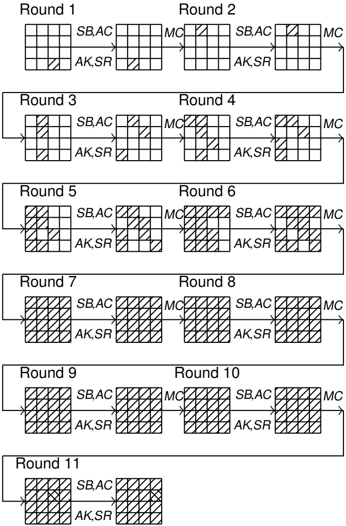
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



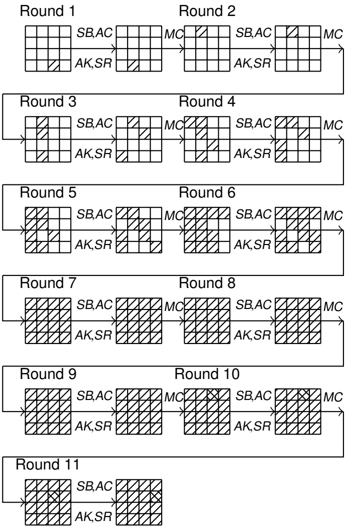
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



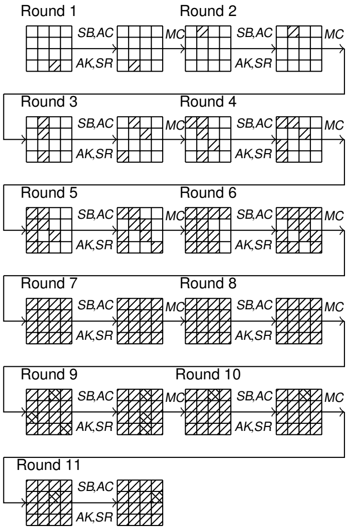
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



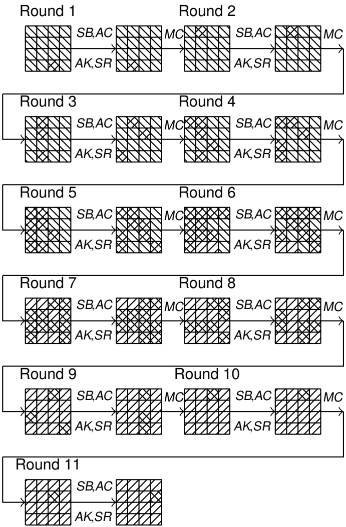
$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



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



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



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

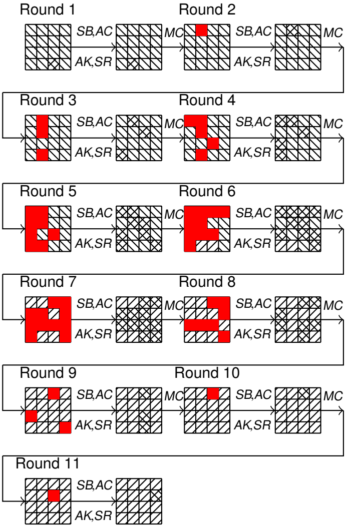


Table 2: An enumeration of all $\mathcal{DS}$-MITM distinguishers for 10.5-round SKINNY-128-384 with $40 \leq \text{Deg}(\mathcal{A}, \mathcal{B}) \leq 48$.

No.	$\mathcal{A}$	$\mathcal{B}$	$\text{Deg}(\mathcal{A}, \mathcal{B})$	No.	$\mathcal{A}$	$\mathcal{B}$	$\text{Deg}(\mathcal{A}, \mathcal{B})$	No.	$\mathcal{A}$	$\mathcal{B}$	$\text{Deg}(\mathcal{A}, \mathcal{B})$
1	[15]	[4]	40	21	[13]	[6, 4]	45	41	[13]	[5]	46
2	[12]	[5]	40	22	[14]	[7, 5]	45	42	[12]	[4]	46
3	[13]	[6]	40	23	[13]	[6, 4]	45	43	[14]	[6]	46
4	[14]	[7]	40	24	[15]	[4, 6]	45	44	[15]	[7]	46
5	[15]	[5]	42	25	[13]	[5]	45	51	[13]	[4, 6]	47
6	[12]	[6]	42	26	[15]	[6]	45	52	[12]	[7, 5]	47
7	[13]	[7]	42	27	[14]	[4]	45	53	[14]	[5, 7]	47
8	[14]	[4]	42	28	[13]	[4]	45	54	[15]	[6, 4]	47
9	[13]	[5]	43	29	[14]	[5]	45	49	[13]	[6]	47
10	[14]	[6]	43	30	[14]	[6]	45	50	[13]	[6]	47
11	[12]	[4]	43	31	[12]	[4]	45	51	[14]	[7]	47
12	[15]	[7]	43	32	[15]	[5]	45	52	[12]	[5]	47
13	[12]	[7]	44	33	[13]	[7]	45	53	[12]	[5]	47
14	[13]	[4]	44	34	[12]	[6]	45	54	[14]	[7]	47
15	[12]	[7]	44	35	[15]	[7]	45	55	[15]	[4]	47
16	[13]	[4]	44	36	[12]	[7]	45	56	[15]	[4]	47
17	[13]	[4]	44	37	[14]	[4, 6]	46	57	[15]	[7, 5]	48
18	[14]	[5]	44	38	[13]	[7, 5]	46	58	[14]	[6, 4]	48
19	[14]	[5]	44	39	[15]	[5, 7]	46	59	[12]	[4, 6]	48
20	[13]	[4]	44	40	[12]	[6, 4]	46	60	[13]	[5, 7]	48

Table 2: An enumeration of all $\mathcal{DS}$-MITM distinguishers for 10.5-round SKINNY-128-384 with $40 \le \mathsf{Deg}(\mathcal{A}, \mathcal{B}) \le 48$.

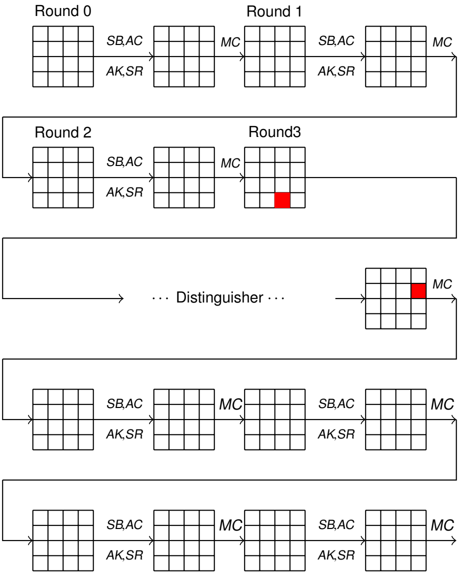
No.	$\mathcal{A}$	$\mathcal{B}$	$\mathsf{Deg}(\mathcal{A},\mathcal{B})$	No.	$\mathcal{A}$	$\mathcal{B}$	$\mathsf{Deg}(\mathcal{A},\mathcal{B})$	No.	$\mathcal{A}$	$\mathcal{B}$	$\mathsf{Deg}(\mathcal{A},\mathcal{B})$
1	[15]	[4]	40	21	[13]	[6, 4]	45	41	[13]	[5]	46
2	[12]	[5]	40	22	[14]	[7, 5]	45	42	[12]	[4]	46
3	[13]	[6]	40	23	[13]	[6, 4]	45	43	[14]	[6]	46
4	[14]	[7]	40	24	[15]	[4, 6]	45	44	[15]	[7]	46
5	[15]	[5]	42	25	[13]	[5]	45	51	[13]	[4, 6]	47
6	[12]	[6]	42	26	[15]	[6]	45	52	[12]	[7, 5]	47
7	[13]	[7]	42	27	[14]	[4]	45	53	[14]	[5, 7]	47
8	[14]	[4]	42	28	[13]	[4]	45	54	[15]	[6, 4]	47
9	[13]	[5]	43	29	[14]	[5]	45	49	[13]	[6]	47
10	[14]	[6]	43	30	[14]	[6]	45	50	[13]	[6]	47
11	[12]	[4]	43	31	[12]	[4]	45	51	[14]	[7]	47
12	[15]	[7]	43	32	[15]	[5]	45	52	[12]	[5]	47
13	[12]	[7]	44	33	[13]	[7]	45	53	[12]	[5]	47
14	[13]	[4]	44	34	[12]	[6]	45	54	[14]	[7]	47
15	[12]	[7]	44	35	[15]	[7]	45	55	[15]	[4]	47
16	[13]	[4]	44	36	[12]	[7]	45	56	[15]	[4]	47
17	[13]	[4]	44	37	[14]	[4, 6]	46	57	[15]	[7, 5]	48
18	[14]	[5]	44	38	[13]	[7, 5]	46	58	[14]	[6, 4]	48
19	[14]	[5]	44	39	[15]	[5, 7]	46	59	[12]	[4, 6]	48
20	[13]	[4]	44	40	[12]	[6, 4]	46	60	[13]	[5, 7]	48

New 0-1 variables 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

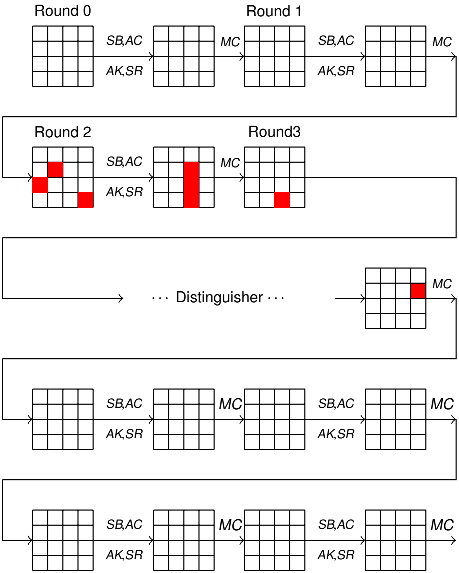


New 0-1 variables Var(M) and Var(W)

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

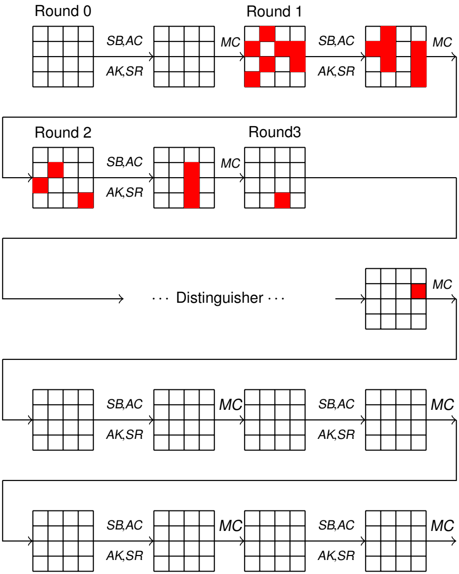


New 0-1 variables `Var(M)` and `Var(W)`

`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

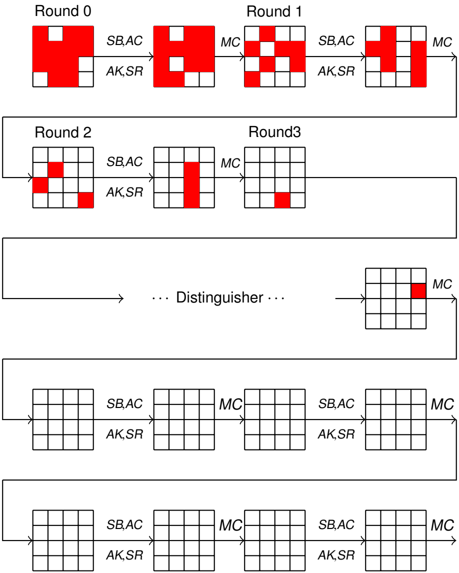


New 0-1 variables Var(M) and Var(W)

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

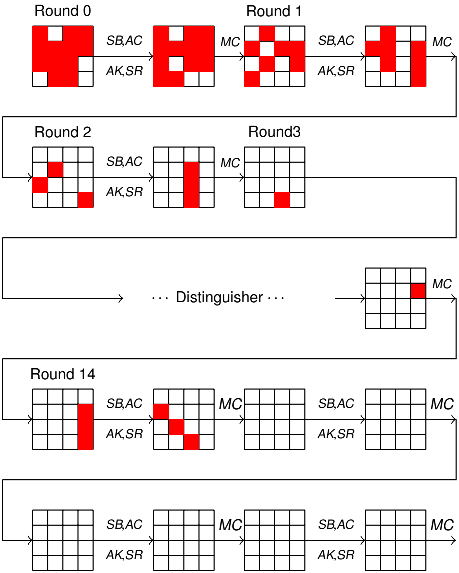


New 0-1 variables Var(M) and Var(W)

`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

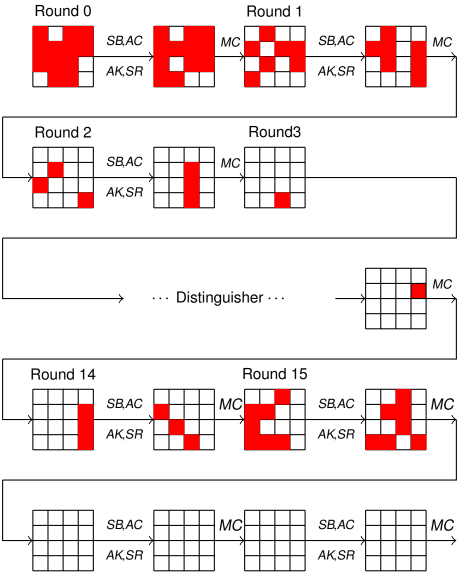


New 0-1 variables Var(M) and Var(W)

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

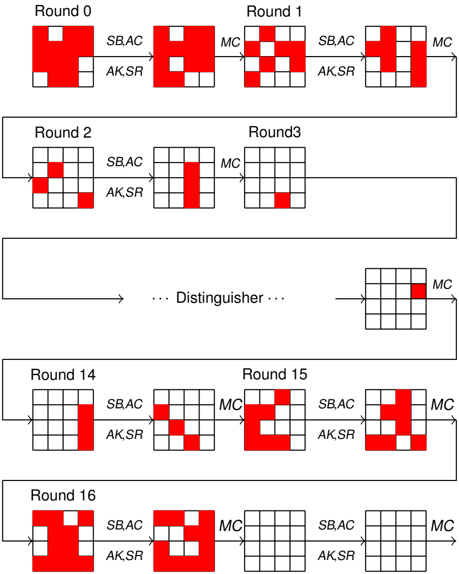


New 0-1 variables Var(M) and Var(W)

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

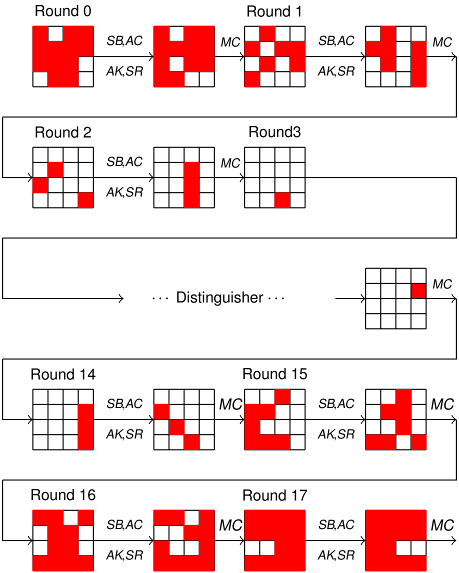


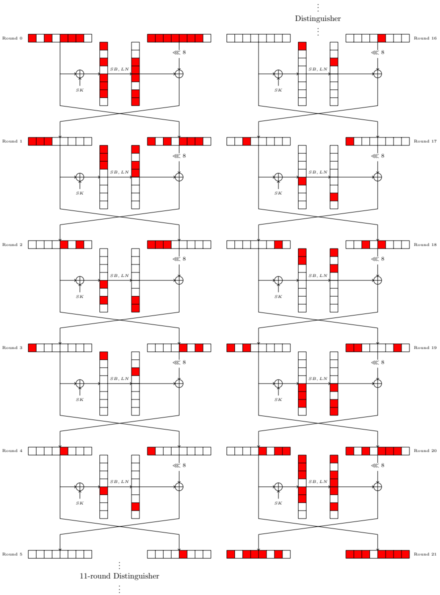
New 0-1 variables Var(M) and Var(W)

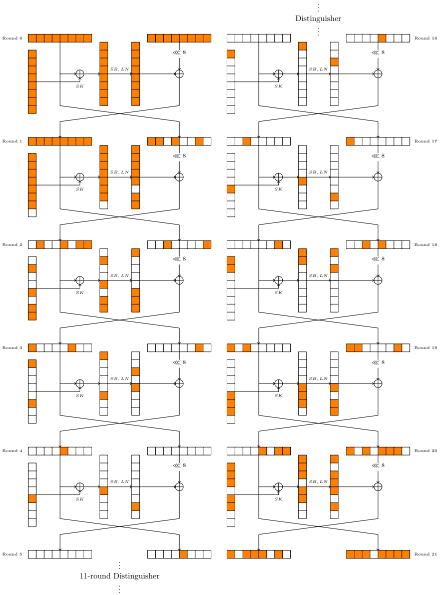
Var(M): Backward differential

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

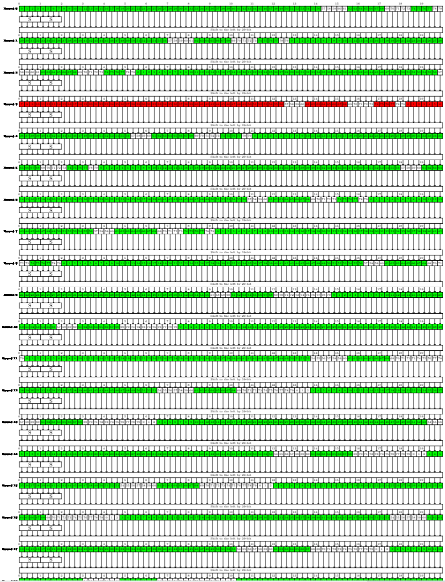
Var(W): Forward determination



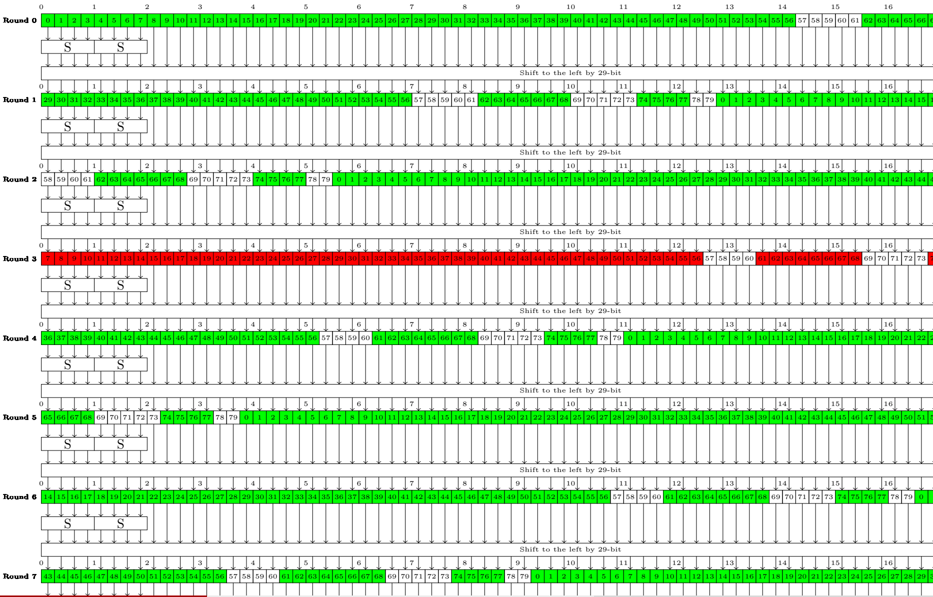

Distinguisher
Round 0
Round 1
Round 2
Round 3
Round 4
Round 5
Round 16
Round 17
Round 18
Round 19
Round 20
Round 21
SB, LN
SK
⋘ 8
11-round Distinguisher


Distinguisher
Round 0
Round 1
Round 2
Round 3
Round 4
Round 5
Round 16
Round 17
Round 18
Round 19
Round 20
Round 21
SB, LN
SK
⋘ 8
11-round Distinguisher

Key bridging technique



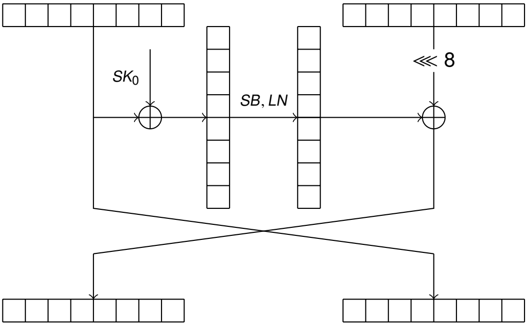
Key bridging technique



Outline

LBlock

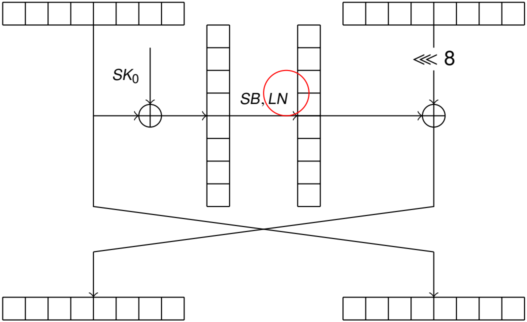
- LBlock



- $8! = 40320$ variants ciphers against MITM and ID

LBlock

- LBlock



- $8! = 40320$ variants ciphers against MITM and ID

Results of LBlock

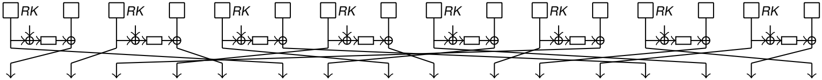
All exist 14-round ID distinguisher

32 permutations are good:

- no 15-round ID distinguisher
- strong against the MITM Distinguisher

TWINE

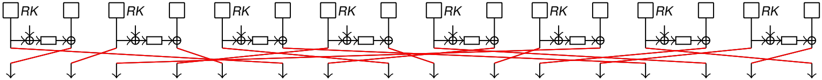
TWINE Cipher:



Enumeration: $22 \cdot 8!$

TWINE

TWINE Cipher:



Enumeration: $22 \cdot 8!$

Results of TWINE

- 144 permutations: no 15-round ID Distinguisher.
- 84 permutations are good in the view of MITM.
- 12 permutations are best: no 11-round MITM distinguisher

Outline

Conclusion

Conclusion

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

Future Work

- Differential enumaraion
- Key Bridging

Thanks for your attention.