CS 553

CRYPTOGRAPHY

Crypto Explainers

Linear Cryptanalysis

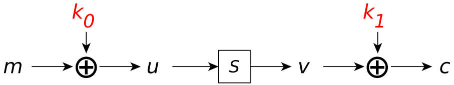
Sypher00A

Instructor

Dr. Dhiman Saha

Image Source: https://www.synthesia.io/

$\alpha = (1,0,0,1), \beta = (0,0,1,0)$ — Recall (Sypher00A)



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S[x]	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5
$\alpha \cdot x$	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
$\beta \cdot S[x]$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0

$p = ?$

$$\Pr\left[\alpha \cdot x = \beta \cdot S[x]\right] = \frac{2}{16}$$

or

$$\Pr\left[\alpha \cdot x \oplus 1 = \beta \cdot S[x]\right] = \frac{14}{16}$$

$\alpha = 9, \beta = 2,$ The Linear Approximation Table

- Linear Characteristic:

$$9 \xrightarrow{S} 2$$

- $LAT(9, 2) = -6$

	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	-2	.	2	.	-2	4	-2	2	4	2	.	-2	.	2	.
2	2	-2	.	-2	.	.	2	2	4	.	2	4	-2	-2	.
3	4	2	2	-2	2	.	.	.	.	2	-2	-2	-2	.	4
4	.	-2	2	2	-2	.	.	-4	.	2	2	2	2	.	4
5	-2	2	.	2	4	.	2	-2	4	.	-2	.	2	-2	.
6	-2	.	2	.	2	4	2	2	-4	2	.	2	.	-2	.
7	.	.	.	4	.	-4	.	.	.	.	4	.	4	.	.
8	.	-2	2	-4	.	2	2	-4	.	-2	-2	.	.	2	-2
9	-2	-6	.	.	2	-2	.	2	.	.	-2	-2	.	.	2
a	-2	.	-6	-2	.	2	.	-2	.	2	.	.	-2	.	2
b	.	.	.	2	-2	2	-2	.	.	-4	-4	2	-2	-2	2
c	.	.	.	-2	-2	-2	-2	.	.	4	-4	2	2	-2	-2
d	-2	.	2	2	.	-2	.	-2	.	2	.	.	-6	.	-2
e	2	-2	.	.	2	2	-4	-2	.	.	2	-2	.	-4	-2
f	-4	2	2	-4	.	-2	-2	.	.	-2	2	.	.	-2	2

- Implication

$$\Pr\left[9 \xrightarrow{S} 2\right] = \Pr\left[9 \cdot x = 2 \cdot S[x]\right]$$
$$= \left(\frac{-6}{16} + \frac{1}{2}\right) = \frac{1}{8}$$

- So, we take the complement event:

$$9 \cdot x \oplus 1 = 2 \cdot S[x]$$

- $\Pr\left[9 \cdot x \oplus 1 = 2 \cdot S[x]\right] = 1 - \frac{1}{8} = \frac{7}{8}$

- For Sypher00A, $\Longrightarrow$

$$\Pr\left[(9 \cdot m) \oplus (2 \cdot c) \oplus 1 = (9 \cdot k_0) \oplus (2 \cdot k_1)\right] = \frac{7}{8}$$

$\alpha = 9, \beta = 2,$ Summarizing LC of Sypher00A

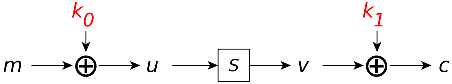
$$\begin{tikzcd}
 & k_0 \arrow[d] & & & & & k_1 \arrow[d] & \\
m \arrow[r] & \oplus \arrow[r] & u \arrow[r] & \boxed{S} \arrow[r] & v \arrow[rr] & & \oplus \arrow[r] & c
\end{tikzcd}$$

- $\Pr\left[9 \cdot u \oplus 1 = 2 \cdot v\right] = \frac{7}{8}$
- $\Pr\left[(9 \cdot m) \oplus (2 \cdot c) \oplus 1 = (9 \cdot k_0) \oplus (2 \cdot k_1)\right] = \frac{7}{8}$

Procedure

- Initialize counters T_0 and T_1 to 0
- Request the encryptions of N known plaintexts.
- For each plaintext-ciphertext pair, we compute the **left-hand side** of the equation: $(9 \cdot m) \oplus (2 \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(9 \cdot k_0) \oplus (2 \cdot k_1)$
- T_0++ if LHS evaluates to 0; T_1++ if LHS evaluates to 1

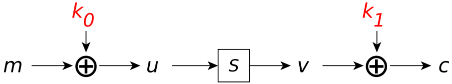
Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



- Message Count #1 $m = 0, c = 6$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 0) \oplus (2 \cdot 6) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$

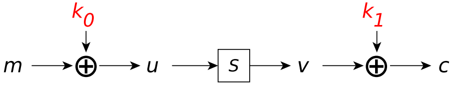


- Message Count #2 $m = 1, c = 0$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 1) \oplus (2 \cdot 0) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0 2

T_1 0

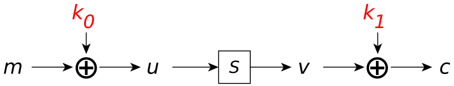


- Message Count #3 $m = 2, c = 1$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 2) \oplus (2 \cdot 1) \oplus 1 \\ &= 1 \implies \boxed{T_1{+}{+}} \end{aligned}$$

T_0 2

T_1 1

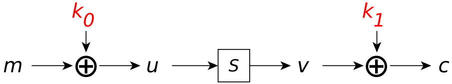


- Message Count #4 $m = 3, c = 5$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 3) \oplus (2 \cdot 5) \oplus 1 \\ &= 0 \implies \boxed{T_0{+}{+}} \end{aligned}$$

T_0	T_1
3	1

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



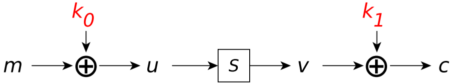
- Message Count #5 $m = 4, c = 7$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 4) \oplus (2 \cdot 7) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0 4

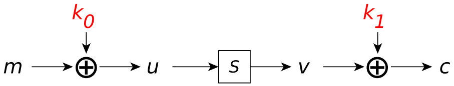
T_1 1

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



- Message Count #6 $m = 5, c = 4$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 5) \oplus (2 \cdot 4) \oplus 1 \\ &= 0 \implies \boxed{T_0{+}{+}} \end{aligned}$$

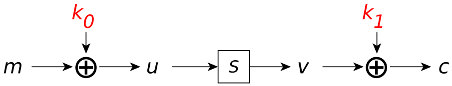


- Message Count #7 $m = 6, c = 14$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 6) \oplus (2 \cdot 14) \oplus 1 \\ &= 0 \implies \boxed{T_0{+}{+}} \end{aligned}$$

T_0: 6

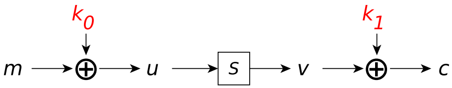
T_1: 1



- Message Count #8 $m = 7, c = 13$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 7) \oplus (2 \cdot 13) \oplus 1 \\ &= 0 \implies \boxed{T_0{+}{+}} \end{aligned}$$

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



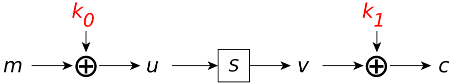
- Message Count #9 $\qquad m = 8, c = 9$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 8) \oplus (2 \cdot 9) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0 : 8

T_1 : 1

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$

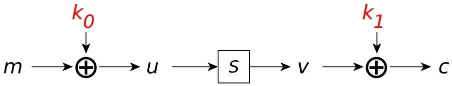


- Message Count #10 $m = 9, c = 2$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 9) \oplus (2 \cdot 2) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0	T_1
9	1

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



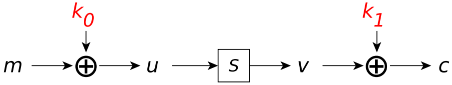
- Message Count #11 $m = 10, c = 12$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 10) \oplus (2 \cdot 12) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0 10

T_1 1

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$

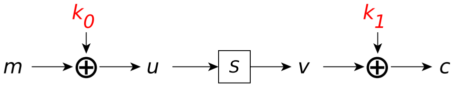


- Message Count #12 $m = 11, c = 3$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 11) \oplus (2 \cdot 3) \oplus 1 \\ &= 0 \implies \boxed{T_0{+}{+}} \end{aligned}$$

T_0	T_1
10	1

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



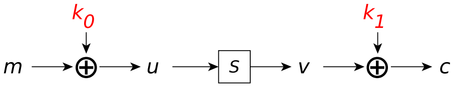
- Message Count #13 $m = 12, c = 10$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 12) \oplus (2 \cdot 10) \oplus 1 \\
&= 1 \implies \boxed{T_1{+}{+}}
\end{aligned}
$$

T_0 T_1

11 2

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$

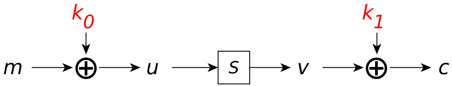


- Message Count #14 $m = 13, c = 11$

$$\begin{aligned} LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\ &= (9 \cdot 13) \oplus (2 \cdot 11) \oplus 1 \\ &= 0 \implies \boxed{T_0{+}{+}} \end{aligned}$$

T_0	T_1
12	2

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$

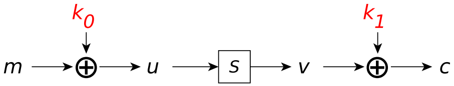


- Message Count #15 $m = 14, c = 8$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 14) \oplus (2 \cdot 8) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0	T_1
13	2

Simulating LC - Sypher00A $\alpha = 9, \beta = 2$



- Message Count #16 $m = 15, c = 15$

$$
\begin{aligned}
LHS &= (\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 \\
&= (9 \cdot 15) \oplus (2 \cdot 15) \oplus 1 \\
&= 0 \implies \boxed{T_0{+}{+}}
\end{aligned}
$$

T_0: 14

T_1: 2

Interpretation — Values in $T_0 = 14$ and $T_1 = 2$

- $RHS = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \stackrel{?}{=} 0/1$
- Key-bit estimation correct with prob. $\frac{14}{16}$
- What to expect at T_0 / T_1 after N KP encryptions

If $(\alpha \cdot k_0) \oplus (\beta \cdot k_1) = 1$	
$T_0 \leftarrow \frac{2N}{16}$	$T_1 \leftarrow \frac{14N}{16}$

If $(\alpha \cdot k_0) \oplus (\beta \cdot k_1) = 0$	
$T_0 \leftarrow \frac{14N}{16}$	$T_1 \leftarrow \frac{2N}{16}$

Here, $N = 16$

T_0	T_1
14	2

- Verifying any one counter say, T_0
  - Reveals one bit $\rightarrow (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
  - Attack Outcome $\rightarrow (9 \cdot k_0) \oplus (2 \cdot k_1) = 0$

m	c	$(9 \cdot m) \oplus (2 \cdot c) \oplus 1$	T_0	T_1	Remarks
0	6	0	1	0	T_0++
1	0	0	2	0	T_0++
2	1	1	2	1	T_1++
3	5	0	3	1	T_0++
4	7	0	4	1	T_0++
5	4	0	5	1	T_0++
6	14	0	6	1	T_0++
7	13	0	7	1	T_0++
8	9	0	8	1	T_0++
9	2	0	9	1	T_0++
10	12	0	10	1	T_0++
11	3	0	10	1	T_0++
12	10	1	11	2	T_1++
13	11	0	12	2	T_0++
14	8	0	13	2	T_0++
15	15	0	14	2	T_0++

- Every group needs to generate the Hawk-Eye Table from last slide using their own oracles for (m, c) pairs and submit in the **notebook**.
- You are free to choose any of the masks you used for the In-Class assignment.