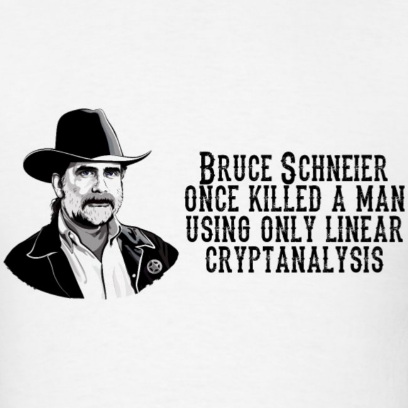


CSL 505
CRYPTOGRAPHY

Lecture 10
Linear Cryptanalysis

Instructor
Dr. Dhiman Saha

Image Source: Google

Linear Cryptanalysis

- Less effective than Differential Cryptanalysis
- But is a Known Plaintext Attack (Recall DC is CPA)
- Credited to Matsui for applications on DES
- Earlier references on FEAL-4
  - By Tardy-Corfdir and Gilbert

Linear Approximation — Basic Idea

Uses a linear relation between inputs and outputs of an encryption algorithm that holds with a certain probability

- This approximation can be used to assign probabilities to the possible keys and locate the most probable one.

- Less effective than Differential Cryptanalysis
- But is a Known Plaintext Attack (Recall DC is CPA)
- Credited to Matsui for applications on DES
- Earlier references on FEAL-4
  - By Tardy-Corfdir and Gilbert

Linear Approximation — **Basic Idea**

Uses a linear relation between inputs and outputs of an encryption algorithm that holds with a certain probability

- This approximation can be used to assign probabilities to the possible keys and locate the most probable one.

- Consider the encryption scheme

$$c = m \oplus k \qquad c, k, m \in \{0,1\}^b$$

- Bit expansion

$$\begin{bmatrix} c_0 & = & m_0 \oplus k_0 \\ c_1 & = & m_1 \oplus k_1 \\ & \vdots & \\ c_{b-1} & = & m_{b-1} \oplus k_{b-1} \end{bmatrix} \to \begin{bmatrix} k_0 & = & m_0 \oplus c_0 \\ k_1 & = & m_1 \oplus c_1 \\ & \vdots & \\ k_{b-1} & = & m_{b-1} \oplus c_{b-1} \end{bmatrix}$$

- Vulnerability if k reused What about KPA?

What did we do here?

Key expressed as a (linear) relation between plaintext and ciphertext

- Consider the following 4-bit cryptosystem

$$c_3 = m_3 \oplus m_1 \oplus m_0 \oplus k_3 \oplus k_1 \oplus k_0$$
$$c_2 = m_2 \oplus m_0 \oplus k_2 \oplus k_0$$
$$c_1 = m_3 \oplus m_2 \oplus k_3 \oplus k_2$$
$$c_0 = m_1 \oplus m_0 \oplus k_1 \oplus k_0$$

$$k_3 = m_3 \oplus c_0 \oplus c_3$$
$$k_2 = m_2 \oplus c_3 \oplus c_1 \oplus c_0$$
$$k_1 = m_1 \oplus c_3 \oplus c_2 \oplus c_1$$
$$k_0 = m_0 \oplus c_3 \oplus c_2 \oplus c_1 \oplus c_0$$

Reiterates the basic aim of LC

Constructing equations that express bits of the key in terms of bits of the message and ciphertext.

- Extracting specific bits using the mask vector

$$(1,0,0,0) \times \begin{pmatrix} m_3 \\ m_2 \\ m_1 \\ m_0 \end{pmatrix} = m_3 \qquad (1,0,1,0) \times \begin{pmatrix} m_3 \\ m_2 \\ m_1 \\ m_0 \end{pmatrix} = m_3 \oplus m_1$$

- Linear combination using the mask vector

$$(1,0,1,1) \times \begin{pmatrix} m_3 \\ m_2 \\ m_1 \\ m_0 \end{pmatrix} \oplus (1,0,1,1) \times \begin{pmatrix} k_3 \\ k_2 \\ k_1 \\ k_0 \end{pmatrix} = m_3 \oplus m_1 \oplus m_0 \oplus k_3 \oplus k_1 \oplus k_0$$

Linear Mask

Recall the scalar product of vectors in linear algebra

The idea of masking

- Extracting specific bits using the mask vector

$$(1,0,0,0) \times \begin{pmatrix} m_3 \\ m_2 \\ m_1 \\ m_0 \end{pmatrix} = m_3 \qquad (1,0,1,0) \times \begin{pmatrix} m_3 \\ m_2 \\ m_1 \\ m_0 \end{pmatrix} = m_3 \oplus m_1$$

- Linear combination using the mask vector

$$(1,0,1,1)\times \begin{pmatrix} m_3 \\ m_2 \\ m_1 \\ m_0 \end{pmatrix} \oplus (1,0,1,1)\times \begin{pmatrix} k_3 \\ k_2 \\ k_1 \\ k_0 \end{pmatrix} = m_3 \oplus m_1 \oplus m_0 \oplus k_3 \oplus k_1 \oplus k_0$$

Linear Mask

Recall the scalar product of vectors in linear algebra

- Recall our 4-bit cryptosystem

$$\begin{aligned} c_3 &= m_3 \oplus m_1 \oplus m_0 \oplus k_3 \oplus k_1 \oplus k_0, \\ c_2 &= m_2 \oplus m_0 \oplus k_2 \oplus k_0, \\ c_1 &= m_3 \oplus m_2 \oplus k_3 \oplus k_2, \text{ and} \\ c_0 &= m_1 \oplus m_0 \oplus k_1 \oplus k_0. \end{aligned}$$

- Consider the first equation

$$c_3 = m_3 \oplus m_1 \oplus m_0 \oplus k_3 \oplus k_1 \oplus k_0$$

- With masks α, β this can be written as:

$$\alpha \cdot c = \beta \cdot m \oplus \beta \cdot k, \text{where } \alpha = \{1, 0, 0, 0\},\ \beta = \{1, 0, 1, 1\}$$

First Target — Sypher00A

- Sypher00A encrypts 4 bits with two 4 bit keys

S-box

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

Encryption

$$m \xrightarrow{\oplus k_0} u \longrightarrow \boxed{S} \longrightarrow v \xrightarrow{\oplus k_1} c$$

- Same as Sypher001 in DC but different Sbox

The Non-linear Component

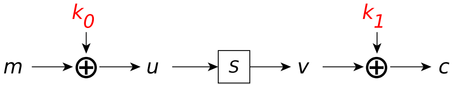
- Linear approximation of $S[\cdot]$

To find some (α, β) such that

$$\Pr\Big[\alpha \cdot x = \beta \cdot S[x]\Big] \neq \frac{1}{2}$$

- Implication:
  - `XOR` of certain bits of the input to S equals
  - `XOR` of certain bits in the output of S
  - With a probability "**different** from the random case"

Linear Approximation Sypher00A



- Note:

$$\alpha \cdot m = \alpha \cdot k_0 \oplus \alpha \cdot u \qquad \rightarrow \text{Holds with prob. } 1 \qquad (1)$$

$$\alpha \cdot u = \beta \cdot v \qquad \rightarrow \text{Holds with prob. } p \qquad (2)$$

$$\beta \cdot v = \beta \cdot k_1 \oplus \beta \cdot c \qquad \rightarrow \text{Holds with prob. } 1 \qquad (3)$$

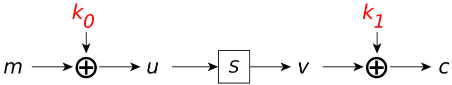
- Adding Eqn. $(1 - 3)$:

$$(\alpha \cdot m) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) \oplus (\beta \cdot k_1) \oplus (\beta \cdot c)$$

Simplifying **Holds with prob. p**

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

Linear Approximation — Sypher00A



- Note:

$$\alpha \cdot m = \alpha \cdot k_0 \oplus \alpha \cdot u \quad \rightarrow \text{Holds with prob. } 1 \qquad (1)$$

$$\alpha \cdot u = \beta \cdot v \quad \rightarrow \text{Holds with prob. } p \qquad (2)$$

$$\beta \cdot v = \beta \cdot k_1 \oplus \beta \cdot c \quad \rightarrow \text{Holds with prob. } 1 \qquad (3)$$

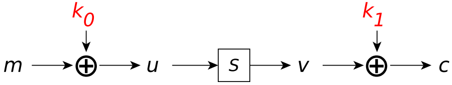
- Adding Eqn. $(1 - 3)$:

$$(\alpha\cdot m)\oplus(\alpha\cdot u)\oplus(\beta\cdot v) = (\alpha\cdot k_0)\oplus(\alpha\cdot u)\oplus(\beta\cdot v)\oplus(\beta\cdot k_1)\oplus(\beta\cdot c)$$

Simplifying — Holds with prob. p

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

Linear Approximation Sypher00A



- Note:

$$\alpha \cdot m = \alpha \cdot k_0 \oplus \alpha \cdot u \qquad \rightarrow \text{Holds with prob. } 1 \qquad (1)$$

$$\alpha \cdot u = \beta \cdot v \qquad \rightarrow \text{Holds with prob. } p \qquad (2)$$

$$\beta \cdot v = \beta \cdot k_1 \oplus \beta \cdot c \qquad \rightarrow \text{Holds with prob. } 1 \qquad (3)$$

- Adding Eqn. $(1-3)$:

$$(\alpha \cdot m) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) \oplus (\beta \cdot k_1) \oplus (\beta \cdot c)$$

Simplifying Holds with prob. p

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

Linear Approximation — Sypher00A

$$m \longrightarrow \overset{k_0 \atop \downarrow}{\oplus} \longrightarrow u \longrightarrow \boxed{S} \longrightarrow v \longrightarrow \overset{k_1 \atop \downarrow}{\oplus} \longrightarrow c$$

- Note:

$$\alpha \cdot m = \alpha \cdot k_0 \oplus \alpha \cdot u \qquad \rightarrow \text{Holds with prob. } 1 \qquad (1)$$

$$\alpha \cdot u = \beta \cdot v \qquad \rightarrow \text{Holds with prob. } p \qquad (2)$$

$$\beta \cdot v = \beta \cdot k_1 \oplus \beta \cdot c \qquad \rightarrow \text{Holds with prob. } 1 \qquad (3)$$

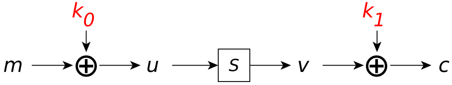
- Adding Eqn. $(1-3)$:

$$(\alpha \cdot m) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) \oplus (\beta \cdot k_1) \oplus (\beta \cdot c)$$

Simplifying — Holds with prob. p

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

Linear Approximation — Sypher00A



- Note:

$$\alpha \cdot m = \alpha \cdot k_0 \oplus \alpha \cdot u \qquad \rightarrow \text{Holds with prob. } 1 \qquad (1)$$

$$\alpha \cdot u = \beta \cdot v \qquad \rightarrow \text{Holds with prob. } p \qquad (2)$$

$$\beta \cdot v = \beta \cdot k_1 \oplus \beta \cdot c \qquad \rightarrow \text{Holds with prob. } 1 \qquad (3)$$

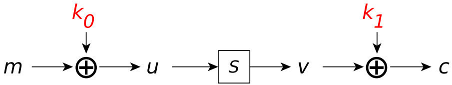
- Adding Eqn. $(1-3)$:

$$(\alpha\cdot m)\oplus(\alpha\cdot u)\oplus(\beta\cdot v) = (\alpha\cdot k_0)\oplus(\alpha\cdot u)\oplus(\beta\cdot v)\oplus(\beta\cdot k_1)\oplus(\beta\cdot c)$$

Simplifying — Holds with prob. p

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

Linear Approximation Sypher00A



- Note:

$$\begin{aligned}
\alpha \cdot m &= \alpha \cdot k_0 \oplus \alpha \cdot u && \rightarrow \text{Holds with prob. } 1 \quad (1)\\
\alpha \cdot u &= \beta \cdot v && \rightarrow \text{Holds with prob. } p \quad (2)\\
\beta \cdot v &= \beta \cdot k_1 \oplus \beta \cdot c && \rightarrow \text{Holds with prob. } 1 \quad (3)
\end{aligned}$$

- Adding Eqn. $(1-3)$:

$$(\alpha \cdot m) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \oplus (\beta \cdot v) \oplus (\beta \cdot k_1) \oplus (\beta \cdot c)$$

Simplifying **Holds with prob. p**

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

$p = 1$ Vs $p = 0$

Holds with prob. p

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

- $p = 0$ or $p = 1$, equally useful for attacker
- if $p = 1$, attacker recovers a key-bit using multiple (m, c)
  - Recall this a KPA
- if $p = 0$, attacker uses the same strategy with

$$(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

$p = 1$ Vs $p = 0$

Holds with prob. p

$$(\alpha \cdot m) \oplus (\beta \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

- $p = 0$ or $p = 1$, equally useful for attacker
- if $p = 1$, attacker recovers a key-bit using multiple (m, c)
  - Recall this a KPA
- if $p = 0$, attacker uses the same strategy with

$$(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$$

- Worst-case scenario for attacker: $p = \frac{1}{2}$
- Attacker gets no extra info about key-bit
- 0/1 is equally probable
- Ideal from designer's perspective

Non-zero Bias — Aim of LC

Choose masks α and β so that equations in linear approximation hold with probability

$$p = \frac{1}{2} + \epsilon$$

where ϵ, which is known as the bias is non-zero ("non-negligible")

- Target: $0 < |\epsilon| \leq \frac{1}{2}$
- Larger $|\epsilon| \implies$ better attack

- Worst-case scenario for attacker: $p = \frac{1}{2}$
- Attacker gets no extra info about key-bit
- 0/1 is equally probable
- Ideal from designer's perspective

Non-zero Bias — **Aim of LC**

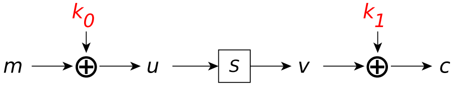
Choose masks α and β so that equations in linear approximation hold with probability

$$p = \frac{1}{2} + \epsilon$$

where ϵ, which is known as the bias is non-zero ("non-negligible")

- Target: $0 < |\epsilon| \leq \frac{1}{2}$
- Larger $|\epsilon| \implies$ better attack

$\alpha = (1,0,0,1), \beta = (0,0,1,0)$ Example (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

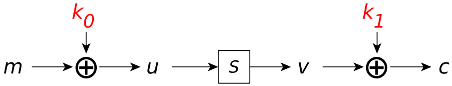
$p = ?$

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

or

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

LC of Sypher00A

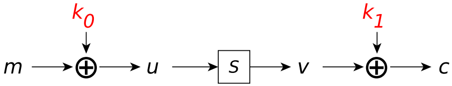


- In terms of Sypher00A $\longrightarrow \Pr\left[\alpha \cdot u \oplus 1 = \beta \cdot v\right] = \frac{14}{16}$
- i.e., $\Pr\left[(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)\right] = \frac{14}{16}$

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: $(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
- $T_0{+}{+}$ if LHS evaluates to 0; $T_1{+}{+}$ if LHS evaluates to 1

LC of Sypher00A

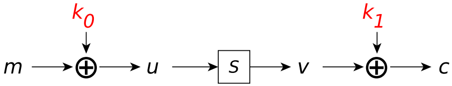


- In terms of Sypher00A $\longrightarrow \Pr\left[\alpha \cdot u \oplus 1 = \beta \cdot v\right] = \frac{14}{16}$
- i.e., $\Pr\left[(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)\right] = \frac{14}{16}$

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: $(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
- $T_0{+}{+}$ if LHS evaluates to 0; $T_1{+}{+}$ if LHS evaluates to 1

LC of Sypher00A

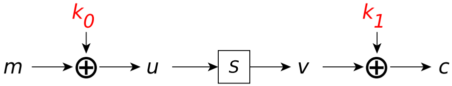


- In terms of Sypher00A $\longrightarrow \Pr\Big[\alpha \cdot u \oplus 1 = \beta \cdot v\Big] = \frac{14}{16}$
- i.e., $\Pr\Big[(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)\Big] = \frac{14}{16}$

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: $(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
- $T_0{++}$ if LHS evaluates to 0; $T_1{++}$ if LHS evaluates to 1

LC of Sypher00A

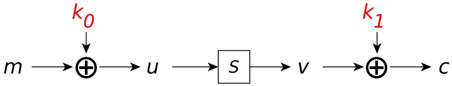


- In terms of Sypher00A $\longrightarrow \Pr\Big[\alpha \cdot u \oplus 1 = \beta \cdot v\Big] = \frac{14}{16}$
- i.e., $\Pr\Big[(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)\Big] = \frac{14}{16}$

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: $(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
- $T_0{+}{+}$ if LHS evaluates to 0; $T_1{+}{+}$ if LHS evaluates to 1

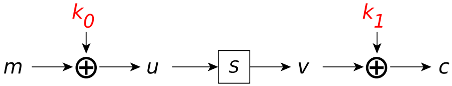
LC of Sypher00A



- In terms of Sypher00A $\longrightarrow \Pr\Big[\alpha \cdot u \oplus 1 = \beta \cdot v\Big] = \frac{14}{16}$
- i.e., $\Pr\Big[(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)\Big] = \frac{14}{16}$

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: $(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
- $T_0{++}$ if LHS evaluates to 0; $T_1{++}$ if LHS evaluates to 1



- In terms of Sypher00A $\longrightarrow \Pr\Big[\alpha \cdot u \oplus 1 = \beta \cdot v\Big] = \frac{14}{16}$
- i.e., $\Pr\Big[(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1)\Big] = \frac{14}{16}$

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: $(\alpha \cdot m) \oplus (\beta \cdot c) \oplus 1$,
  - Which is either 0 or 1.
- Gives an estimate for the value of $(\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
- $T_0{+}{+}$ if LHS evaluates to 0; $T_1{+}{+}$ if LHS evaluates to 1

- $(\alpha \cdot k_0) \oplus (\beta \cdot k_1) \stackrel{?}{=} 0/1$
- 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 $(\alpha \cdot k_0) \oplus (\beta \cdot k_1) = 0$

$T_0 \leftarrow \frac{14N}{16}$ $T_1 \leftarrow \frac{2N}{16}$

- Verifying any one counter say, T_0 for $\frac{2N}{16}$ or $\frac{14N}{16}$
  - Reveals one bit $\rightarrow (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
  - Increase $N \rightarrow$ better success prob.

- $(\alpha \cdot k_0) \oplus (\beta \cdot k_1) \stackrel{?}{=} 0/1$
- 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 $(\alpha \cdot k_0) \oplus (\beta \cdot k_1) = 0$

$T_0 \leftarrow \frac{14N}{16}$ $T_1 \leftarrow \frac{2N}{16}$

- Verifying any one counter say, T_0 for $\frac{2N}{16}$ or $\frac{14N}{16}$
  - Reveals one bit $\rightarrow (\alpha \cdot k_0) \oplus (\beta \cdot k_1)$
  - Increase $N \rightarrow$ better success prob.

In General

- $s \rightarrow$ value of RHS of target equation involving secret key
- Counters $\rightarrow T_s, T_{s \oplus 1}$
- Expected values after using N texts

$$T_s \leftarrow pN \qquad T_{s \oplus 1} \leftarrow (1 - p)N$$

- For $p \neq \frac{1}{2}$ and enough N
  - Possible to determine s
  - Correspondingly recover 1 bit of key info.

The Linear Approximation Table

	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

How to interpret it[1] ?

[1] Will be discussed in details in next class