




CS 553

CRYPTOGRAPHY

Lecture 10

More on Linear Cryptanalysis

Instructor
Dr. Dhiman Saha

- ▶ The idea of linear masks
- ▶ The notion of approximation
- ▶ Expressing key bits in terms of plaintext and ciphertexts
- ▶ Approximating the non-linear component 
- ▶ Extending the approximation to other associate parts of a simple cryptosystem
- ▶ Using the linear approximation to mount a KPA
- ▶ Recovering a single bit of key material

Sypher00B

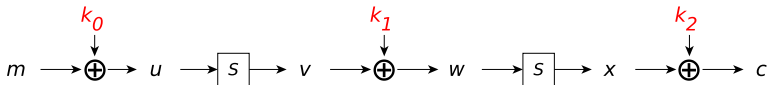
Moving on to a more complex but still toy cryptosystem:

- Sypher00B encrypts 4 bits with **three** 4 bit keys

S-box

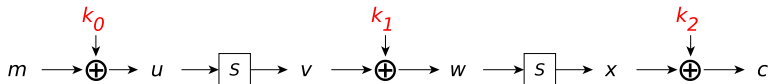
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5


Encryption



- Again, same as Sypher002 with a different SBox

- KPA assumption: attacker knows message m and ciphertext c



- WLOG the following holds for any mask α, β, γ . Why? 

$$(\alpha \cdot m) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \quad (1)$$

$$(\beta \cdot v) = (\beta \cdot k_1) \oplus (\beta \cdot w) \quad (2)$$

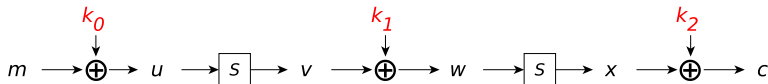
$$(\gamma \cdot x) = (\gamma \cdot k_2) \oplus (\gamma \cdot c) \quad (3)$$

- We assume: we can find α, β, γ such that 

$$\alpha \cdot u = \beta \cdot S[u] = \beta \cdot v \quad \text{Holds with prob. } p_1 \neq \frac{1}{2}$$

$$\beta \cdot w = \gamma \cdot S[w] = \gamma \cdot x \quad \text{Holds with prob. } p_2 \neq \frac{1}{2}$$

- KPA assumption: attacker knows message m and ciphertext c



- WLOG the following holds for any mask α, β, γ . Why?

$$(\alpha \cdot m) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \quad (1)$$

$$(\beta \cdot v) = (\beta \cdot k_1) \oplus (\beta \cdot w) \quad (2)$$

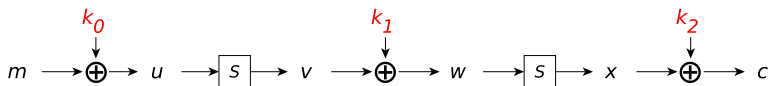
$$(\gamma \cdot x) = (\gamma \cdot k_2) \oplus (\gamma \cdot c) \quad (3)$$


- We assume: we can find α, β, γ such that

$$\alpha \cdot u = \beta \cdot S[u] = \beta \cdot v \quad \text{Holds with prob. } p_1 \neq \frac{1}{2}$$

$$\beta \cdot w = \gamma \cdot S[w] = \gamma \cdot x \quad \text{Holds with prob. } p_2 \neq \frac{1}{2}$$

- KPA assumption: attacker knows message m and ciphertext c



- WLOG the following holds for any mask α, β, γ . Why? 

$$(\alpha \cdot m) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \quad (1)$$

$$(\beta \cdot v) = (\beta \cdot k_1) \oplus (\beta \cdot w) \quad (2)$$

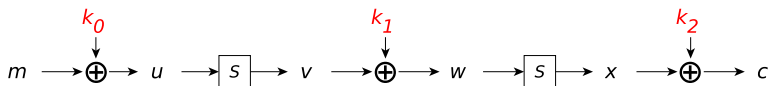
$$(\gamma \cdot x) = (\gamma \cdot k_2) \oplus (\gamma \cdot c) \quad (3)$$


- We assume: we can find α, β, γ such that 

$$\alpha \cdot u = \beta \cdot S[u] = \beta \cdot v \quad \text{Holds with prob. } p_1 \neq \frac{1}{2}$$

$$\beta \cdot w = \gamma \cdot S[w] = \gamma \cdot x \quad \text{Holds with prob. } p_2 \neq \frac{1}{2}$$

- KPA assumption: attacker knows message m and ciphertext c



- WLOG the following holds for any mask α, β, γ . Why? 

$$(\alpha \cdot m) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \quad (1)$$

$$(\beta \cdot v) = (\beta \cdot k_1) \oplus (\beta \cdot w) \quad (2)$$

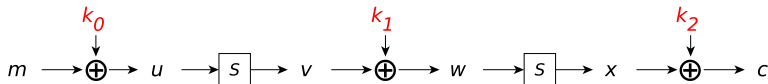
$$(\gamma \cdot x) = (\gamma \cdot k_2) \oplus (\gamma \cdot c) \quad (3)$$


- We assume: we can find α, β, γ such that 

$$\alpha \cdot u = \beta \cdot S[u] = \beta \cdot v \quad \text{Holds with prob. } p_1 \neq \frac{1}{2}$$

$$\beta \cdot w = \gamma \cdot S[w] = \gamma \cdot x \quad \text{Holds with prob. } p_2 \neq \frac{1}{2}$$

- KPA assumption: attacker knows message m and ciphertext c




- **W**LOG the following holds for any mask α, β, γ . Why? 

$$(\alpha \cdot m) = (\alpha \cdot k_0) \oplus (\alpha \cdot u) \quad (1)$$

$$(\beta \cdot v) = (\beta \cdot k_1) \oplus (\beta \cdot w) \quad (2)$$

$$(\gamma \cdot x) = (\gamma \cdot k_2) \oplus (\gamma \cdot c) \quad (3)$$

- We assume: we can find α, β, γ such that 

$$\alpha \cdot u = \beta \cdot S[u] = \beta \cdot v$$

Holds with prob. $p_1 \neq \frac{1}{2}$

$$\beta \cdot w = \gamma \cdot S[w] = \gamma \cdot x$$

Holds with prob. $p_2 \neq \frac{1}{2}$

- Using Eqn. (1) – (3)

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) = (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) \oplus (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Rearranging 

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) \oplus (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Note RHS is a constant, for LHS, we know:

$$\left. \begin{array}{ll} (\alpha \cdot u) = (\beta \cdot v) & \text{with prob. } p_1 \\ (\beta \cdot w) = (\gamma \cdot x) & \text{with prob. } p_2 \end{array} \right\} \text{taken over all } u \text{ and } w$$

- Possibility to remove intermediate variables:

$$\alpha \cdot u \quad \beta \cdot v \quad \beta \cdot w \quad \gamma \cdot x$$

What is the probability that the approximation holds when all the internal variables have canceled out?

- Using Eqn. (1) – (3)

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) = (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) \oplus (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Rearranging 

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) \oplus (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Note RHS is a constant, for LHS, we know:

$$\left. \begin{array}{ll} (\alpha \cdot u) = (\beta \cdot v) & \text{with prob. } p_1 \\ (\beta \cdot w) = (\gamma \cdot x) & \text{with prob. } p_2 \end{array} \right\} \text{taken over all } u \text{ and } w$$

- Possibility to remove intermediate variables:

$$\alpha \cdot u \quad \beta \cdot v \quad \beta \cdot w \quad \gamma \cdot x$$

What is the probability that the approximation holds when all the internal variables have canceled out?

- Using Eqn. (1) – (3)

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) = (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) \oplus (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Rearranging 

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) \oplus (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Note RHS is a constant, for LHS, we know:

$$\left. \begin{array}{ll} (\alpha \cdot u) = (\beta \cdot v) & \text{with prob. } p_1 \\ (\beta \cdot w) = (\gamma \cdot x) & \text{with prob. } p_2 \end{array} \right\} \text{taken over all } u \text{ and } w$$

- Possibility to remove intermediate variables:

$$\alpha \cdot u \quad \beta \cdot v \quad \beta \cdot w \quad \gamma \cdot x$$

What is the probability that the approximation holds when all the internal variables have canceled out?

- Using Eqn. (1) – (3)

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) = (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) \oplus (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Rearranging 

$$(\alpha \cdot m) \oplus (\beta \cdot v) \oplus (\gamma \cdot x) \oplus (\alpha \cdot u) \oplus (\beta \cdot w) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- Note RHS is a constant, for LHS, we know:

$$\left. \begin{array}{ll} (\alpha \cdot u) = (\beta \cdot v) & \text{with prob. } p_1 \\ (\beta \cdot w) = (\gamma \cdot x) & \text{with prob. } p_2 \end{array} \right\} \text{taken over all } u \text{ and } w$$

- Possibility to remove intermediate variables:

$$\alpha \cdot u \quad \beta \cdot v \quad \beta \cdot w \quad \gamma \cdot x$$

What is the probability that the approximation holds when all the internal variables have canceled out?

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$\begin{aligned}(\alpha \cdot u) &= (\beta \cdot v) \\ (\beta \cdot w) &= (\gamma \cdot x)\end{aligned}$$

Case 2

$$\begin{aligned}(\alpha \cdot u) &= (\beta \cdot v) \oplus 1 \\ (\beta \cdot w) &= (\gamma \cdot x) \oplus 1\end{aligned}$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$\begin{aligned}(\alpha \cdot u) &= (\beta \cdot v) \\ (\beta \cdot w) &= (\gamma \cdot x) \oplus 1\end{aligned}$$

Case 4

$$\begin{aligned}(\alpha \cdot u) &= (\beta \cdot v) \oplus 1 \\ (\beta \cdot w) &= (\gamma \cdot x)\end{aligned}$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Case 2

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Case 4

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Case 2

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Case 4

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Case 2

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Case 4

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Case 2

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Case 4

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Case 2

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Case 4

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Events $(\alpha \cdot u) = (\beta \cdot v)$ and $(\beta \cdot w) = (\gamma \cdot x)$ are independent

The Possibilities

Case 1

$$(\alpha \cdot u) = (\beta \cdot v)$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Case 2

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$

Case 3

$$(\alpha \cdot u) = (\beta \cdot v)$$


$$(\beta \cdot w) = (\gamma \cdot x) \oplus 1$$

Case 4

$$(\alpha \cdot u) = (\beta \cdot v) \oplus 1$$

$$(\beta \cdot w) = (\gamma \cdot x)$$

Implication: $(\alpha \cdot m) \oplus (\gamma \cdot c) \oplus 1 = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$


- ▶ Favorable events: 
 $\begin{cases} \text{Case 1} \rightarrow \text{Prob.} = p_1 \times p_2 \\ \text{Case 2} \rightarrow \text{Prob.} = (1 - p_1) \times (1 - p_2) \end{cases}$
- ▶ Probability of linear approximation: $p_1 p_2 + (1 - p_1)(1 - p_2)$
- ▶ If $p_1 = \frac{1}{2} + \epsilon_1$ and $p_2 = \frac{1}{2} + \epsilon_2$, then

$$\begin{aligned} & p_1 p_2 + (1 - p_1)(1 - p_2) \\ &= 1 - p_1 - p_2 + 2p_1 p_2 \\ &= 1 - \frac{1}{2} - \epsilon_1 - \frac{1}{2} - \epsilon_2 + 2 \left(\frac{1}{4} + \frac{\epsilon_1}{2} + \frac{\epsilon_2}{2} + \epsilon_1 \epsilon_2 \right) \\ &= \frac{1}{2} + 2\epsilon_1 \epsilon_2 \end{aligned}$$

Intuition

What would the general case look like?




- ▶ Favorable events: 
 - Case 1 \rightarrow Prob. $= p_1 \times p_2$
 - Case 2 \rightarrow Prob. $= (1 - p_1) \times (1 - p_2)$
- ▶ Probability of linear approximation: $p_1 p_2 + (1 - p_1)(1 - p_2)$
- ▶ If $p_1 = \frac{1}{2} + \epsilon_1$ and $p_2 = \frac{1}{2} + \epsilon_2$, then

$$\begin{aligned} & p_1 p_2 + (1 - p_1)(1 - p_2) \\ &= 1 - p_1 - p_2 + 2p_1 p_2 \\ &= 1 - \frac{1}{2} - \epsilon_1 - \frac{1}{2} - \epsilon_2 + 2 \left(\frac{1}{4} + \frac{\epsilon_1}{2} + \frac{\epsilon_2}{2} + \epsilon_1 \epsilon_2 \right) \\ &= \frac{1}{2} + 2\epsilon_1 \epsilon_2 \end{aligned}$$

Intuition

What would the general case look like?



- Favorable events: 

$$\begin{cases} \text{Case 1} \rightarrow \text{Prob.} = p_1 \times p_2 \\ \text{Case 2} \rightarrow \text{Prob.} = (1 - p_1) \times (1 - p_2) \end{cases}$$

- Probability of linear approximation: $p_1 p_2 + (1 - p_1)(1 - p_2)$

- If $p_1 = \frac{1}{2} + \epsilon_1$ and $p_2 = \frac{1}{2} + \epsilon_2$, then


$$\begin{aligned} & p_1 p_2 + (1 - p_1)(1 - p_2) \\ &= 1 - p_1 - p_2 + 2p_1 p_2 \\ &= 1 - \frac{1}{2} - \epsilon_1 - \frac{1}{2} - \epsilon_2 + 2 \left(\frac{1}{4} + \frac{\epsilon_1}{2} + \frac{\epsilon_2}{2} + \epsilon_1 \epsilon_2 \right) \\ &= \frac{1}{2} + 2\epsilon_1 \epsilon_2 \end{aligned}$$

Intuition

What would the general case look like? 

- ▶ Extending this to m independent events with probabilities $p_i, i = 1, \dots, m$, we have:


$$\frac{1}{2} + 2^{m-1} \prod_{i=1}^m \left(p_i - \frac{1}{2} \right) \triangle$$

- ▶ How would you define the event in the general case?
 - ▶ What is actually piling-up? 
 - ▶ What happens when constituent events are true?

The piling-up lemma allows us to compute the **bias** of a set of combined linear approximations provided that the constituent linear approximations are **independent**.

- ▶ Extending this to m independent events with probabilities $p_i, i = 1, \dots, m$, we have:

$$\frac{1}{2} + 2^{m-1} \prod_{i=1}^m \left(p_i - \frac{1}{2} \right) \triangle$$

- ▶ How would you define the event in the general case?
 - ▶ What is actually piling-up? 
 - ▶ What happens when constituent events are true?

The piling-up lemma allows us to compute the **bias** of a set of combined linear approximations provided that the constituent linear approximations are **independent**.

- ▶ Task is to find masks α, β, γ for satisfying

$$(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- ▶ How?

The Linear Approximation Table

This table lists the probabilities that the **sum** of certain input bits of a equals the sum of certain output bits of $S[a]$.

- ▶ Each entry gives us the linear characteristic for a pair of input-output masks

$$\alpha \xrightarrow{S} \beta$$

- ▶ And also the associated **bias**

- ▶ Task is to find masks α, β, γ for satisfying

$$(\alpha \cdot m) \oplus (\gamma \cdot c) = (\alpha \cdot k_0) \oplus (\beta \cdot k_1) \oplus (\gamma \cdot k_2)$$

- ▶ How?

The Linear Approximation Table

This table lists the probabilities that the **sum** of certain input bits of a equals the sum of certain output bits of $S[a]$.

- ▶ Each entry gives us the linear characteristic for a pair of input-output masks

$$\alpha \xrightarrow{S} \beta$$

- ▶ And also the associated **bias**

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

Highest Bias for $\alpha = \beta = \gamma = d$

- ▶ The chosen characteristic: $d \xrightarrow{S} d \xrightarrow{S} d$
- ▶ For Sypher00B this implies:

$$(d \cdot m) \oplus (d \cdot c) = (d \cdot k_0) \oplus (d \cdot k_1) \oplus (d \cdot k_2)$$

- ▶ Associated prob.

$$\begin{aligned} \Pr(d \xrightarrow{S} d \xrightarrow{S} d) &= \frac{1}{8} \times \frac{1}{8} + \frac{7}{8} \times \frac{7}{8} \\ &= \frac{25}{32} \\ &= \frac{1}{2} + \frac{9}{32} \end{aligned}$$

- ▶ Attacker collects N KPs to calculate $(d \cdot m) \oplus (d \cdot c)$
- ▶ Based on counter values determine if $(k_0 \oplus k_1 \oplus k_2) \cdot d \stackrel{?}{=} 0/1$

- ▶ The chosen characteristic: $d \xrightarrow{S} d \xrightarrow{S} d$
- ▶ For Sypher00B this implies:


$$(d \cdot m) \oplus (d \cdot c) = (d \cdot k_0) \oplus (d \cdot k_1) \oplus (d \cdot k_2)$$

- ▶ Associated prob.

$$\begin{aligned} \Pr \left(d \xrightarrow{S} d \xrightarrow{S} d \right) &= \frac{1}{8} \times \frac{1}{8} + \frac{7}{8} \times \frac{7}{8} \\ &= \frac{25}{32} \\ &= \frac{1}{2} + \frac{9}{32} \end{aligned}$$

- ▶ Attacker collects N KPs to calculate $(d \cdot m) \oplus (d \cdot c)$
- ▶ Based on counter values determine if $(k_0 \oplus k_1 \oplus k_2) \cdot d \stackrel{?}{=} 0/1$


Is recovering single key-bit material enough?

- ▶ Can we do more? How?
- ▶ How about more linear approximations? 
- ▶ Fine, but may not be always available

Better if we can use one but recover more than one

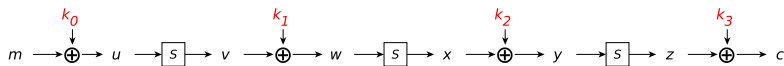
- ▶ How to deduce more key bits?
- ▶ Sypher00C leads the way

Is recovering single key-bit material enough?

- ▶ Can we do more? How?
- ▶ How about more linear approximations? 
- ▶ Fine, but may not be always available

Better if we can use one but recover more than one

- ▶ How to deduce more key bits?
- ▶ Sypher00C leads the way



- ▶ Sypher00B \leftarrow Sypher00B with extra round
- ▶ Use characteristic from Sypher00B for first two rounds

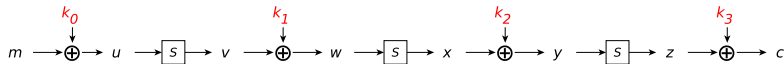
$$(d \cdot m) \oplus (d \cdot y) = (d \cdot k_0) \oplus (d \cdot k_1) \oplus (d \cdot k_2)$$

- ▶ Holds with prob. $\frac{1}{2} + \frac{9}{32}$
- ▶ How to handle last round?

Intuition

Guess k_3 and invert last round

- ▶ Repeat the attack used for Sypher00B for every guess of k_3



- ▶ Sypher00B \leftarrow Sypher00B with extra round
- ▶ Use characteristic from Sypher00B for first two rounds

$$(d \cdot m) \oplus (d \cdot y) = (d \cdot k_0) \oplus (d \cdot k_1) \oplus (d \cdot k_2)$$

- ▶ Holds with prob. $\frac{1}{2} + \frac{9}{32}$
- ▶ How to handle last round?

Intuition

Guess k_3 and invert last round

- ▶ Repeat the attack used for Sypher00B for every guess of k_3

- For a given ciphertext c , attacker computes

$$y' = S^{-1}[c \oplus i]$$

for every guess $k_3 = i$

- Uses the corresponding message m to compute

$$(d \cdot m) \oplus (d \cdot y')$$

- For each guess i , he maintains two counters T_0^i and T_1^i

$$T_0^i \text{++ if } (d \cdot m) \oplus (d \cdot y') = 0$$

$$T_1^i \text{++ if } (d \cdot m) \oplus (d \cdot y') = 1$$

- For a given ciphertext c , attacker computes

$$y' = S^{-1}[c \oplus i]$$

for every guess $k_3 = i$

- Uses the corresponding message m to compute

$$(d \cdot m) \oplus (d \cdot y')$$

- For each guess i , he maintains two counters T_0^i and T_1^i

$$T_0^i \text{++ if } (d \cdot m) \oplus (d \cdot y') = 0$$

$$T_1^i \text{++ if } (d \cdot m) \oplus (d \cdot y') = 1$$

How to distinguish?

- ▶ For the correct guess, $k_3 = \nu$ (say), expected value of

$$\begin{cases} T_0^\nu \leftarrow \frac{N}{2} + \frac{9N}{32} \\ T_1^\nu \leftarrow \frac{N}{2} - \frac{9N}{32} \end{cases}$$

- ▶ For incorrect guess, things should behave randomly
 - ▶ Expected value in both counters close to $\frac{N}{2}$

How to distinguish?

- ▶ For the correct guess, $k_3 = \nu$ (say), expected value of

$$\begin{cases} T_0^\nu \leftarrow \frac{N}{2} + \frac{9N}{32} \\ T_1^\nu \leftarrow \frac{N}{2} - \frac{9N}{32} \end{cases}$$

- ▶ For incorrect guess, things should behave randomly
 - ▶ Expected value in both counters close to $\frac{N}{2}$

- ▶ Looking at (T_0^i, T_1^i) with **highest imbalance**, k_3 is recovered
- ▶ What else?
- ▶ Looking at actual values of T_0^i and T_1^i in the highest imbalanced counter value of $(k_0 \oplus k_1 \oplus k_2) \cdot d$ is recovered
- ▶ For Sypher00C, largest counter indicates value of $(k_0 \oplus k_1 \oplus k_2) \cdot d$


How many counters? 

- ▶ Last round inversion works for Sypher00C

Point to Ponder

Can the same be done for the first round?

- ▶ Looking at (T_0^i, T_1^i) with **highest imbalance**, k_3 is recovered
- ▶ What else?
- ▶ Looking at actual values of T_0^i and T_1^i in the highest imbalanced counter value of $(k_0 \oplus k_1 \oplus k_2) \cdot d$ is recovered
- ▶ For Sypher00C, largest counter indicates value of $(k_0 \oplus k_1 \oplus k_2) \cdot d$

How many counters? 

- ▶ Last round inversion works for Sypher00C

Point to Ponder


Can the same be done for the first round?

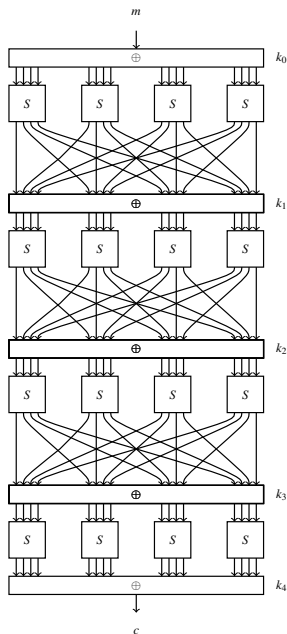
What is estimate for number of KPs required: N ?

- For Single-bit recovery a good estimate is

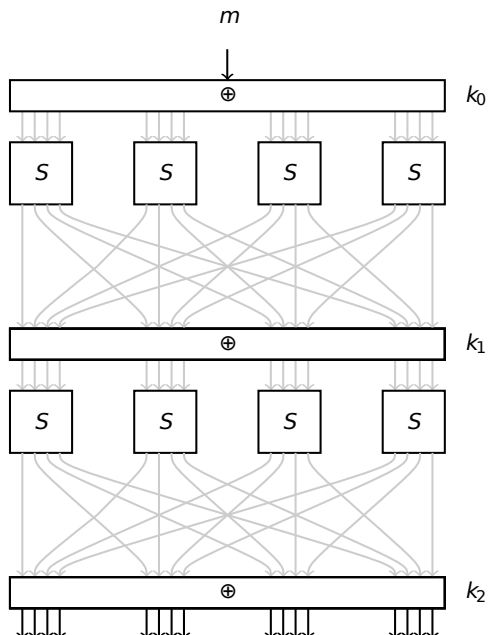
$$N = c \left| p - \frac{1}{2} \right|^{-2} \quad \text{or} \quad N = c |\epsilon|^{-2}$$

where $\epsilon \rightarrow$ bias

- Constant $c \geq 2$ varies with block cipher and attack
- c for single-bit recovery will definitely be less than that for multiple-bit recovery 
- Think about #counters to choose from

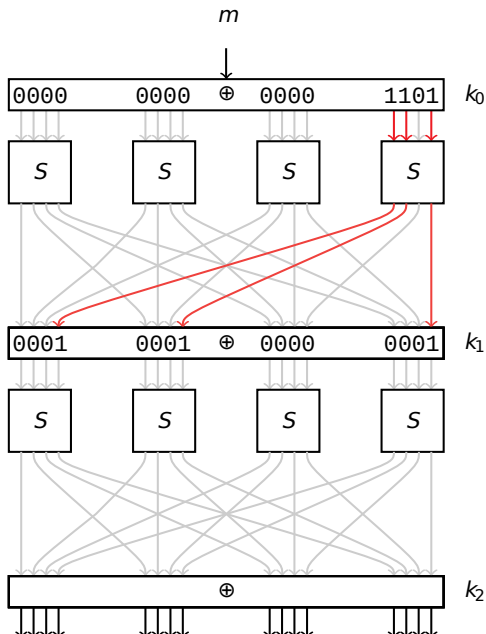


- ▶ Sbox same as Sypher00A-C
- ▶ Permutation same as Sypher004 in DC lecture
- ▶ Number of rounds is 4



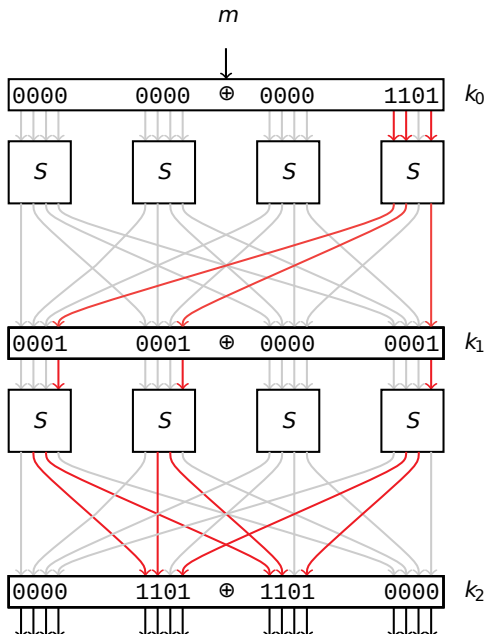
$$(0, 0, 0, d) \xrightarrow{\mathcal{R}} (1, 1, 0, 1)$$

$$p_1 = \frac{1}{2} - \frac{6}{16}$$

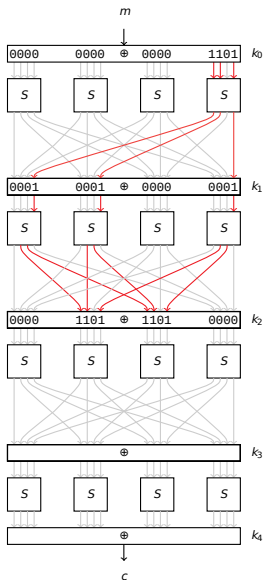


$$(1, 1, 0, 1) \xrightarrow{\mathcal{R}} (0, d, d, 0)$$

$$p_2 = \frac{1}{2} + 2^2 \left(\frac{4}{16} \right)^3 = \frac{1}{2} + \frac{1}{16}$$



2-Round Linear Characteristic



► $(0, 0, 0, d) \xrightarrow{\mathcal{R}} (1, 1, 0, 1) \xrightarrow{\mathcal{R}} (0, d, d, 0)$

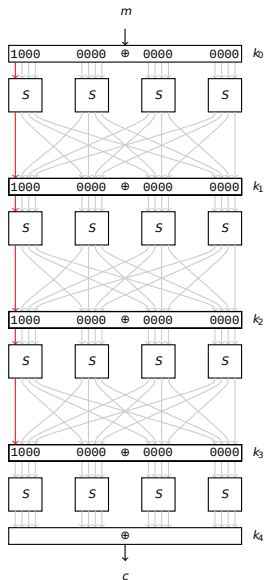
$$p_1 = \frac{1}{2} - \frac{6}{16} = \frac{1}{8}$$

$$p_2 = \frac{1}{2} + 2^2 \left(\frac{4}{16} \right)^3 = \frac{1}{2} + \frac{1}{16} = \frac{9}{16}$$

► Prob. of 2-round characteristic:

$$\frac{1}{8} \times \frac{9}{16} + \frac{7}{8} \times \frac{7}{16} = \frac{29}{64} = \frac{1}{2} - \frac{3}{64}$$

► And so on.



- Prob. of one round characteristic:

$$(8, 0, 0, 0) \xrightarrow{\mathcal{R}} (8, 0, 0, 0) : \frac{1}{2} - \frac{4}{16}$$

Iterative Characteristic

Input mask = Output mask

- Using piling-up lemma we have
prob. for $(8, 0, 0, 0) \xrightarrow{3\mathcal{R}} (8, 0, 0, 0)$

$$\frac{1}{2} + 2^2 \left(\frac{1}{4} \right)^3 = \frac{9}{16} = \frac{1}{2} + \frac{1}{16}$$

- Key recovery as illustrated before