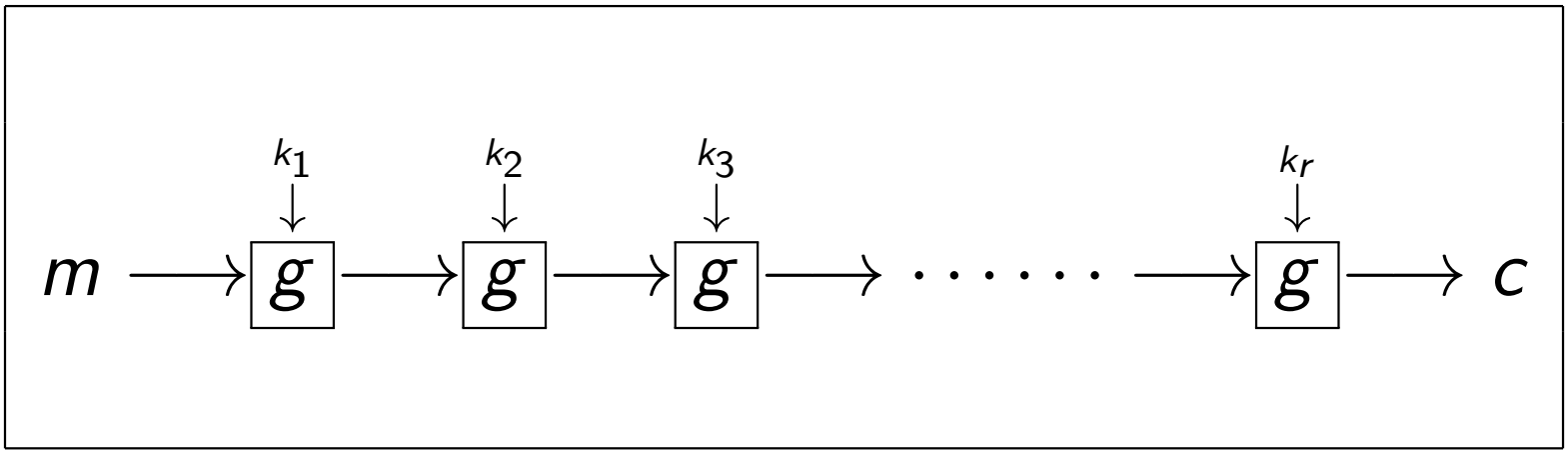
Differential and Linear Cryptanalysis

Lars R. Knudsen

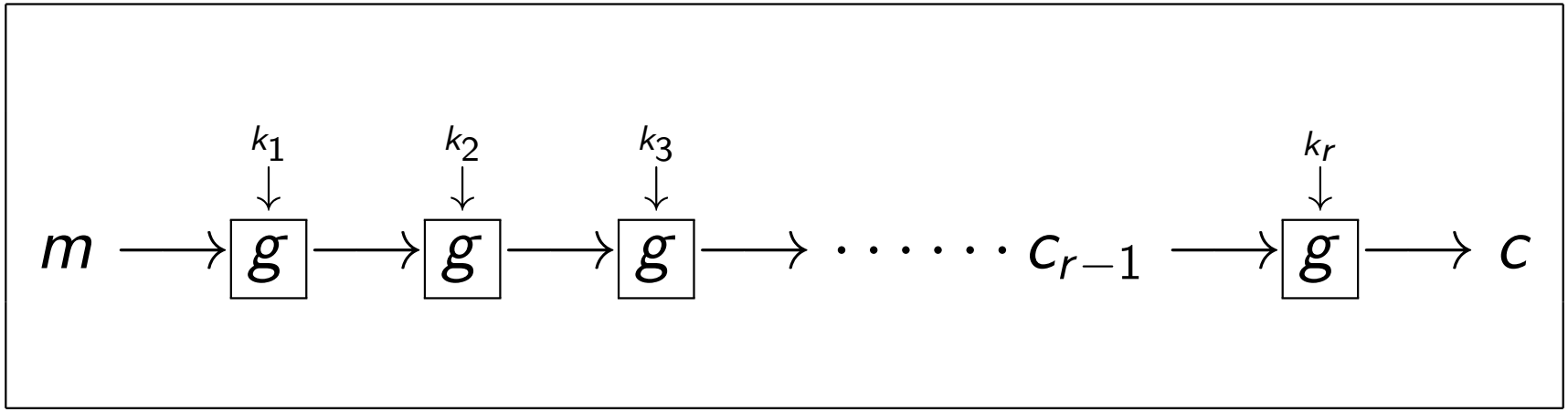
June 2014

Iterated block ciphers (DES, AES, ...)



- plaintext m, ciphertext c, key k
- key-schedule: user-selected key $k \rightarrow k_0, \ldots, k_r$
- round function, g, weak by itself
- idea: g^r, strong for "large" r

Generic attack: r-round iterated ciphers



1. assume "correlation" between m and c_{r-1}
2. given a number of pairs (m, c)
3. repeat for all pairs and all values i of k_r:
   1. let $c' = g^{-1}(c, i)$, compute $x = \mathrm{cor}(m, c')$
   2. if key gives $\mathrm{cor}(m, c_{r-1})$, increment counter
4. value of i which yields $\mathrm{cor}(m, c_{r-1})$ taken as value of k_r

Differential cryptanalysis - (Biham-Shamir 1991)

- chosen plaintext attack
- assume x is combined with key, k, via group operation $\otimes$
- define difference of x_1 and x_2 as

$$\Delta(x_1, x_2) = x_1 \otimes x_2^{-1}$$

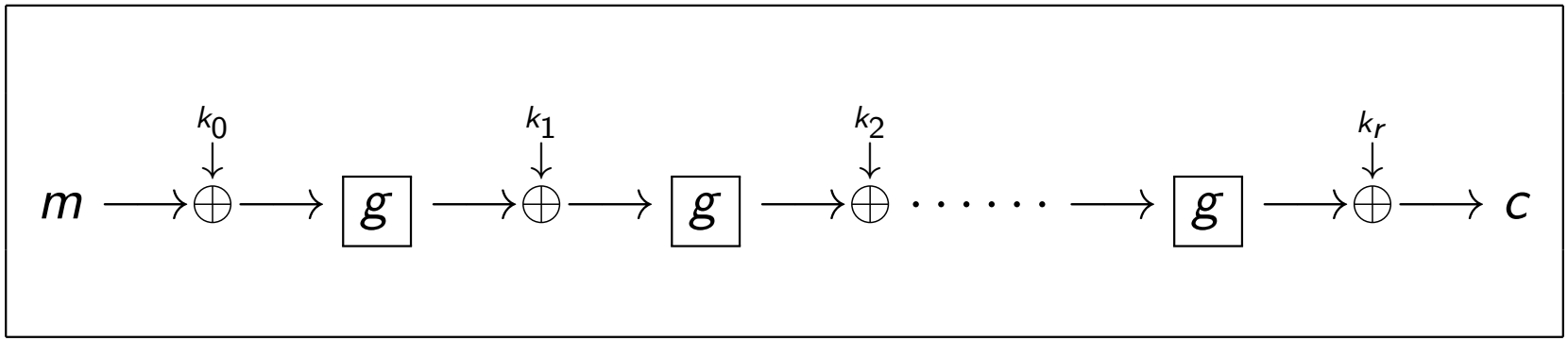
- difference same after combination of key

$$\Delta(x_1 \otimes k, x_2 \otimes k) = x_1 \otimes k \otimes k^{-1} \otimes x_2^{-1} = \Delta(x_1, x_2)$$

- definition of *difference* relative to cipher (often exor)

Differential cryptanalysis (2)

Consider r-round iterated ciphers of the form



Main criterion for success

distribution of differences through nonlinear components of g is non-uniform

Differential cryptanalysis - example (1)

- n-bit strings m, c, k

$$c = m \oplus k$$

- key used only once, system unconditionally secure under a ciphertext-only attack
- key used more than once, the system is insecure, since

$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'$$

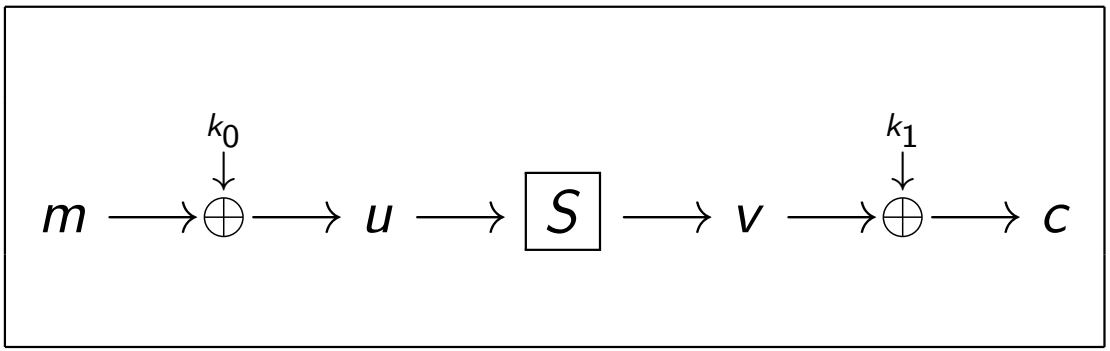
- note that key cancels out

Differential cryptanalysis - example (2)

- k_0, k_1 : n-bit keys, $S : \{0,1\}^n \to \{0,1\}^n$

$$c = S(m \oplus k_0) \oplus k_1$$

- assume attacker knows two pairs messages (m, c) and (m', c')



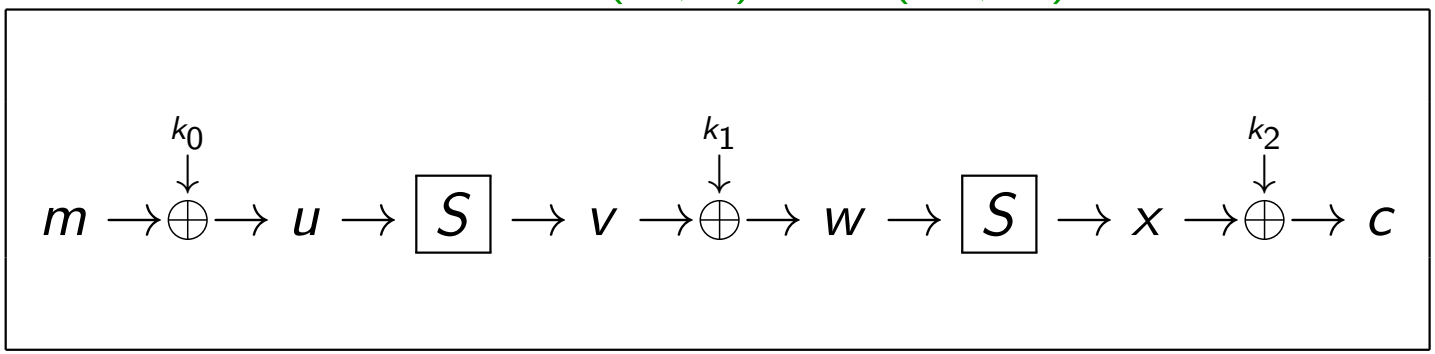
- from m, m', compute $u \oplus u' = m \oplus m'$
- key recovery: from c, c' and k_1, compute $u \oplus u'$

Differential cryptanalysis - example (3)

- k_0, k_1, k_2: n-bit keys, $S : \{0,1\}^n \to \{0,1\}^n$

$$c = S(S(m \oplus k_0) \oplus k_1) \oplus k_2$$

- assume attacker knows (m, c) and (m', c')



- from m, m', compute $u \oplus u' = m \oplus m'$
- from c, c' and k_2, compute $v \oplus v'$
- then what?

Differential cryptanalysis - example (4)

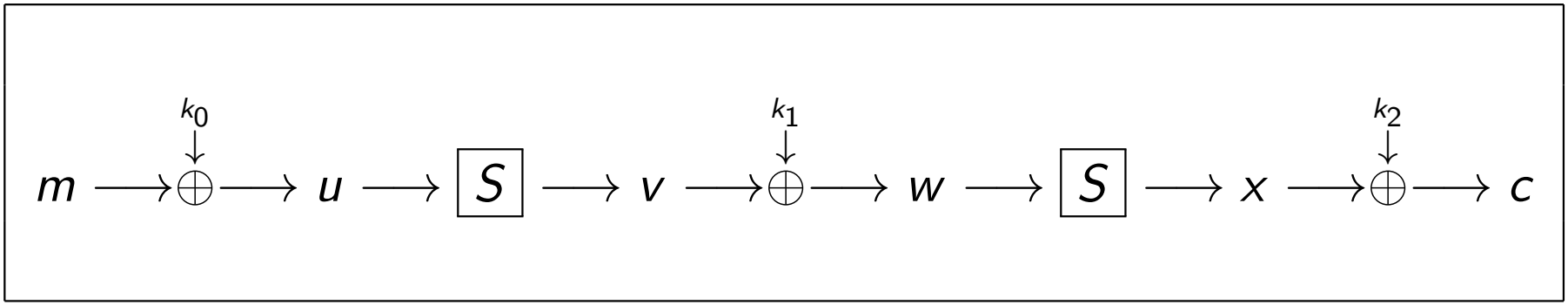
- Assume for concreteness that $n = 4$ and that S is

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

- consider two inputs to S, m and $\overline{m}$, where $\overline{m}$ is the bitwise complemented value of m.

m	m'	$S(m)$		$S(m')$		$S(m) \oplus S(m')$
0	f	6	$\oplus$	b	$=$	d
1	e	4	$\oplus$	9	$=$	d
2	d	c	$\oplus$	a	$=$	6
3	c	5	$\oplus$	8	$=$	d
4	b	0	$\oplus$	d	$=$	d
5	a	7	$\oplus$	3	$=$	4
6	9	2	$\oplus$	f	$=$	d
7	8	e	$\oplus$	1	$=$	f
8	7	1	$\oplus$	e	$=$	f
9	6	f	$\oplus$	2	$=$	d
a	5	3	$\oplus$	7	$=$	4
b	4	d	$\oplus$	0	$=$	d
c	3	8	$\oplus$	5	$=$	d
d	2	a	$\oplus$	c	$=$	6
e	1	9	$\oplus$	4	$=$	d
f	0	b	$\oplus$	6	$=$	d

Differential cryptanalysis - example (5)

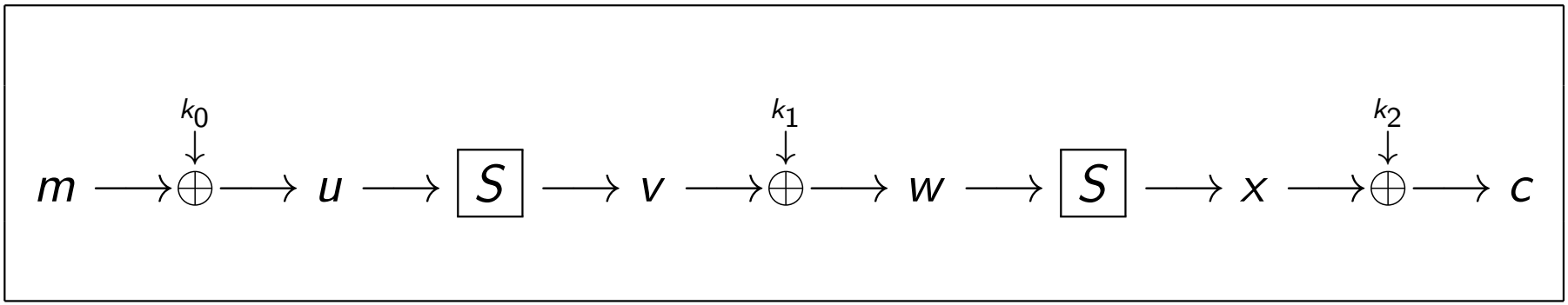


- choose random m, get (m, c), (m', c'), where $m \oplus m' = f_x$.
- then $u \oplus u' = f_x$ $\qquad$ $v \oplus v' = \delta$
- for correct value of k_2: In 10 of 16 cases, one gets $\delta = d_x$

Assumption

for an incorrect value of k_2, δ is random

Differential cryptanalysis - example (6)



1. choose random m, compute $m' = m \oplus f_x$, obtain (m, c) and (m', c')
2. for $i = 0, \ldots, 15$: (guess $k_2 = i$)
   1. compute $\delta = S^{-1}(c \oplus i) \oplus S^{-1}(c' \oplus i)$
   2. if $\delta = d_x$ increment counter for i
3. go to 1, until one counter holds significant value

Main idea in differential attacks

For r-round iterated ciphers

- find suitable differences in plaintexts such that differences in ciphertexts after $r-1$ rounds can be determined with good probability.
- for all values of last-round key k_r, compute difference after $r-1$ rounds of encryption from the ciphertexts

Example. CipherFour: block size 16, r rounds

Round keys independent, uniformly random. One round:

1. exclusive-or round key to text
2. split text, evaluate each nibble via S-box

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

   and concatenate results into 16-bit string $y = y_0, \ldots, y_{15}$

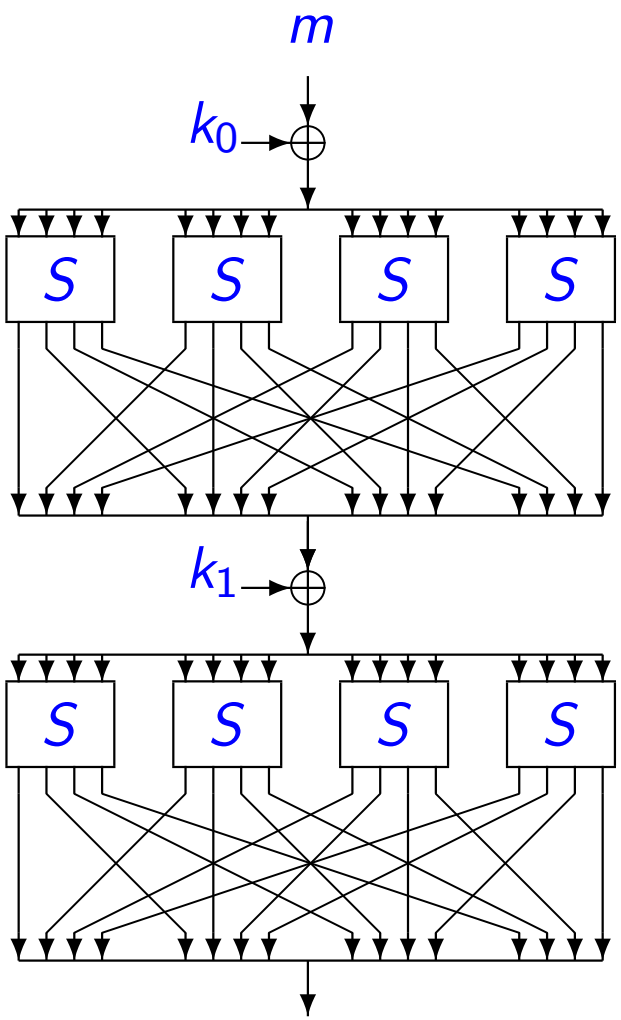
3. permute bits in y according to:

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

   so, $P(y) = y_0, y_4, \ldots, y_{11}, y_{15}$.

Exclusive-or round key to output of last round

Product cipher example - 16-bit messages



Differential characteristics

- denote by

$$(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \xrightarrow{S} (\beta_0, \beta_1, \beta_2, \beta_3)$$

that two 4-word inputs to S-boxes of differences $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ lead to outputs from S-boxes of differences $(\beta_0, \beta_1, \beta_2, \beta_3)$ with some probability p

- similar notation for P, $(\beta_0, \beta_1, \beta_2, \beta_3) \xrightarrow{P} (\gamma_0, \gamma_1, \gamma_2, \gamma_3)$
- then

$$(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \xrightarrow{1r} (\gamma_0, \gamma_1, \gamma_2, \gamma_3)$$

is called a *one-round characteristic* of probability p for CipherFour.

Differential characteristics - probabilities

- assume $\Pr(\alpha_i \xrightarrow{S_i} \beta_i) = p_i$ for $i = 0, ..., 3$ where probability is computed over all inputs to S_i
- then $\Pr((\alpha_0, \alpha_1, \alpha_2, \alpha_3) \xrightarrow{S} (\beta_0, \beta_1, \beta_2, \beta_3)) = p_0 p_1 p_2 p_3$
- assume further that $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \xrightarrow{1r} (\gamma_0, \gamma_1, \gamma_2, \gamma_3)$ is of probability p and that $(\gamma_0, \gamma_1, \gamma_2, \gamma_3) \xrightarrow{1r} (\phi_0, \phi_1, \phi_2, \phi_3)$ is of probability q
- then under suitable assumptions (u.s.a.) $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \xrightarrow{2r} (\phi_0, \phi_1, \phi_2, \phi_3)$ is of probability pq

Example - differential attack

Differential distribution table for S:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

CipherFour - some possible characteristics

$$(0,0,0,f_x) \xrightarrow{S} (0,0,0,d_x)$$

has a probability of $\frac{10}{16}$. Consequently (since P is linear)

$$(0,0,0,f_x) \xrightarrow{1r} (1,1,0,1)$$

is one-round characteristic of probability $\frac{10}{16}$.

$$(1,1,0,1) \xrightarrow{S} (2,2,0,2)$$

has a probability of $(\frac{6}{16})^3$. Consequently (u.s.a.)

$$(0,0,0,f_x) \xrightarrow{2r} (0,0,d_x,0)$$

is a two-round characteristic of probability $\frac{10}{16}(\frac{6}{16})^3 \simeq 0.033$.

CipherFour - iterative characteristics

$(0,0,2,0) \xrightarrow{S} (0,0,2,0)$ has a probability of $\frac{6}{16}$ and therefore
$(0,0,2,0) \xrightarrow{1r} (0,0,2,0)$ is 1-round characteristic of probability $\frac{6}{16}$

It can be concatenated with itself, e.g.,
$(0,0,2,0) \xrightarrow{2r} (0,0,2,0)$ has probability $(\frac{6}{16})^2 \simeq 0.14$

And $(0,0,2,0) \xrightarrow{4r} (0,0,2,0)$ is a 4-round characteristic of probability $(\frac{6}{16})^4$

These are called "iterative" characteristics

CipherFour - differential attack

Consider CipherFour with 5 rounds and the 4-round characteristic

$$(0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0)$$

with a (conjectured) probability of $(\frac{6}{16})^4 \simeq 1/51$

Idea of attack:

- choose pairs of messages with desired difference
- for all values of four (target) bits of k_5
  - from ciphertexts compute backwards one round etc.

If successful, this (sub)attack finds four bits of k_5

CipherFour - differential attack

Consider final round for a pair of texts. One has
$(0,0,2,0) \xrightarrow{S} (0,0,h,0)$, where $h \in \{1,2,9,a_x\}$

Since P linear, last round must have one of following forms:
$(0,0,2,0) \xrightarrow{1r} (0,0,0,2)$ $\quad$ $(0,0,2,0) \xrightarrow{1r} (0,0,2,0)$
$(0,0,2,0) \xrightarrow{1r} (2,0,0,2)$ $\quad$ $(0,0,2,0) \xrightarrow{1r} (2,0,2,0)$

Filtering

Use only pairs for which difference in ciphertexts is of one of above four

In our case, most pairs which survive filtering will have difference $(0,0,2,0)$ after four rounds

CipherFour - differential attack

$$S/N = \frac{\text{prob. correct key is counted}}{\text{prob. any wrong key is counted}}$$

- a "right" pair of texts "follow" characteristic in each round
- let p be prob. of characteristic
- assume all surviving pairs after filtering are right pairs
- prob. correct key is counted $= p$
- prob. random (wrong) key is counted $= p/15$
- signal-to-noise ratio:

$$S/N = \frac{p}{p/15} = 15$$

CipherFour - differential attack

- how many pairs of plaintexts, M, are needed?
- depends on (at least) p, S/N and on number of target bits
- in our case, $Mp = 3$ suffices.
- with $Mp = 3 \Rightarrow M = 3 \cdot 51 = 153$ pairs of plaintexts

CipherFour - differentials

Consider CipherFour with 5 rounds and the 4-round characteristic

$$(0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0)$$

with a (conjectured) probability of $(\frac{6}{16})^4 \simeq 1/51$

In attack only first and last occurrence of $(0,0,2,0)$ is used. In our example, what was used is, in fact

$$(0,0,2,0) \xrightarrow{1r} (*,*,*,*) \xrightarrow{1r} (*,*,*,*) \xrightarrow{1r} (*,*,*,*) \xrightarrow{1r} (0,0,2,0),$$

where asterisks represent "any value". Such a structure is called a *differential*

CipherFour - differentials

$$(0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0),$$
$$(0,0,2,0) \xrightarrow{1r} (0,0,0,2) \xrightarrow{1r} (0,0,0,1) \xrightarrow{1r} (0,0,1,0) \xrightarrow{1r} (0,0,2,0),$$
$$(0,0,2,0) \xrightarrow{1r} (0,0,0,2) \xrightarrow{1r} (0,0,1,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,2,0),$$
$$(0,0,2,0) \xrightarrow{1r} (0,0,2,0) \xrightarrow{1r} (0,0,0,2) \xrightarrow{1r} (0,0,1,0) \xrightarrow{1r} (0,0,2,0),$$

- are four 4-round characteristics: $(0,0,2,0) \rightarrow (0,0,2,0)$
- all four characteristics have a (conjectured) probability of $1/51$
- one should think $\Pr((0,0,2,0) \xrightarrow{4r} (0,0,2,0)) \geq 4/51$
- with $Mp = 3 \Rightarrow M = 3 * 4/51 \approx 40$ pairs of plaintexts

Differential cryptanalysis in general

Definition

An s-round *characteristic* is a series of differences defined as an $(s+1)$-tuple

$$\Omega : \{\alpha_0, \alpha_1, \ldots, \alpha_s\},$$

where $\Delta m = \alpha_0$, $\Delta c_i = \alpha_i$ for $1 \leq i \leq s$

Probability

$\Pr(\Omega) = \Pr(\Delta c_s = \alpha_s, ..., \Delta c_1 = \alpha_1 | \Delta m = \alpha_0)$.
Probability is taken over all possible plaintexts and keys

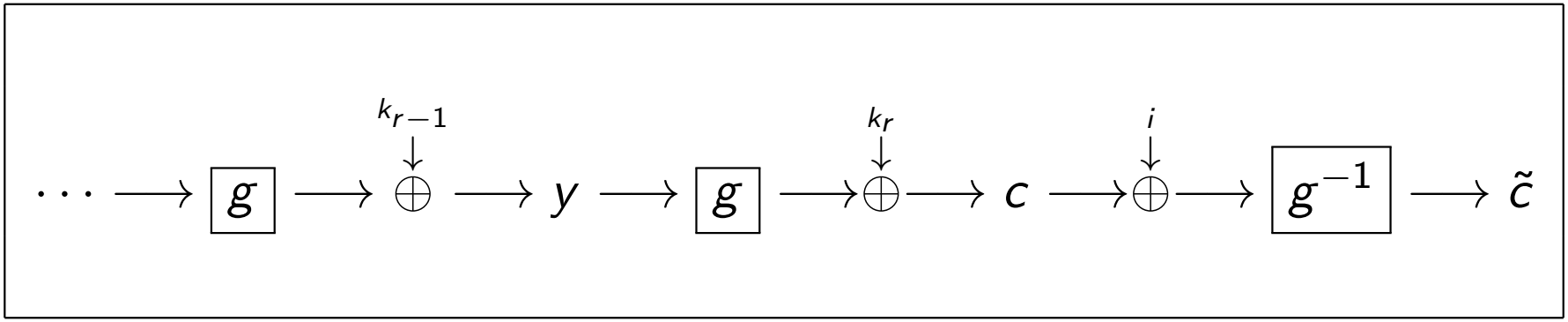
Differential cryptanalysis in general

Find $(r-1)$-round characteristic determining Δc_{r-1} with prob. p
Repeat

1. choose pairs of plaintexts with difference Δm
2. get the pairs of ciphertexts c and c^*
3. for all possible values of k_r do:
   - decrypt ciphertexts one round using guess $k_r = i$,
   - if expected difference Δc_{r-1} is obtained, counter for i incremented

until one counter has value significantly different from other counters

Key recovery part



$$k_r = i \quad \Rightarrow \quad \tilde{c} = y$$
$$k_r \neq i \quad \Rightarrow \quad \tilde{c} = ?$$

Hypothesis of random-key randomization (standard): $\tilde{c}$ is random

Filtering

Definition (Right pair)

A right pair is a pair of plaintexts with intermediate ciphertexts following the characteristic

Definition (Wrong pair)

A wrong pair is a pair which is not a right pair

- right pairs always suggest the correct value of the key
- strategy: minimise the number of wrong pairs
- often possible from ciphertexts alone to determine that a pair is wrong; in that case the pair is *filtered out* (not used) in the analysis

Signal to noise ratio

$$S/N = \frac{\text{prob. correct key is counted}}{\text{prob. a random key is counted}}$$

k	number of key bits to find
p	probability of characteristic
m	number of pairs required
β	ratio of used pairs to all pairs
α	# keys suggested by each used pair

$$S/N = \frac{m \cdot p}{\frac{m \cdot \beta \cdot \alpha}{2^k - 1}} = \frac{p \cdot (2^k - 1)}{\alpha \cdot \beta}$$

If $S/N \neq 1$ repeat attack until correct key "sticks out"

Complexity

- chosen plaintexts needed roughly $c \times 1/p_\Omega$, where
  p_Ω probability of characteristic Ω used,
  $c \geq 1$ a function of S/N (usually small)
- increase S/N ratio: filter out wrong pairs
- success of differential attacks depends on
  - probability of characteristic
  - number of counters required
  - S/N ratio
  - filtering
  - time to run the attack

Differentials

In attacks based on basic differential cryptanalysis intermediate differences (usually) not used

- characteristic $\Phi = (\Delta m, \Delta c_1, \ldots \Delta c_{r-2}, \Delta c_{r-1})$
- differential $\Omega = (\Delta m, \Delta c_{r-1})$
- $\Pr(\Omega) \geq \Pr(\Phi)$

Differentials and probabilities

- probability of differentials taken over all plaintexts and keys
- in an attack, one key is used. Probability?

Definition (Hypothesis of stochastic equivalence)

For virtually all high probability s-round differentials (α, β)

$$\Pr_M(\Delta c_s = \beta \mid \Delta m = \alpha,\ K = k) \approx$$
$$\Pr_{M,K}(\Delta c_s = \beta \mid \Delta m = \alpha)$$

holds for substantial fraction of key values k

Linear cryptanalysis

Linear cryptanalysis (Matsui 1993)

- Known plaintext attack
- Uses linear relations between bits of m, $c = e_k(m)$ and k
- Suppose with probability $p \neq \frac{1}{2}$

$$(m \cdot \alpha) \oplus (c \cdot \beta) = 0 \quad (*)$$

- Collect N pairs of plaintext/ciphertext (using same key!)
- T : number of times left side of (*) is 0
- If $p > 1/2$, $E(T) > N/2$
- If m and c independent, $T \simeq N/2$.

Linear attack: Complexity

- **T** binomial random variable which is 0 with $p > 1/2$

$$\begin{aligned}\Pr(T > N/2) = 1 - \Pr(T \leq N/2) &\simeq 1 - \Phi(\frac{N/2 + 1/2 - Np}{\sqrt{p(1-p)} \times \sqrt{N}}) \\ &\simeq 1 - \Phi(-2\sqrt{N}|p - 1/2|) \\ &= \Phi(2\sqrt{N}|p - 1/2|)\end{aligned}$$

  where Φ is the normal distribution function

- With $N = |p - 1/2|^{-2}$ probability is about 97.72%
- $|p - 1/2|$ called the *bias*

Joining linear approximations

Random, independent boolean variables X, Y, and Z

If $\alpha \cdot X = \beta \cdot Y$ with probability p_1

and $\beta \cdot Y = \gamma \cdot Z$ with probability p_2

then $\alpha \cdot X = \gamma \cdot Z$ with probability $\frac{1}{2} + 2(p_1 - 1/2)(p_2 - 1/2)$

Piling Up-Lemma

Let Z_i, $1 \leq i \leq n$, be independent random boolean variables, which are 0 with probability p_i. Then

$$\Pr(Z_1 \oplus Z_2 \oplus .... \oplus Z_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} (p_i - 1/2)$$

Joining linear approximations

Piling Up-Lemma

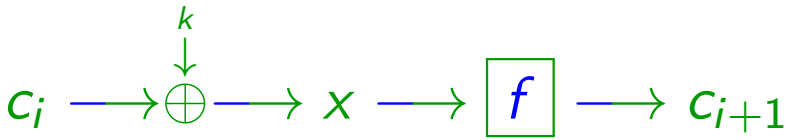
Let Z_i, $1 \leq i \leq n$, be independent random boolean variables, which are 0 with probability p_i. Then

$$\Pr(Z_1 \oplus Z_2 \oplus .... \oplus Z_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} (p_i - 1/2)$$

or similarly

$$2\Pr(Z_1 \oplus Z_2 \oplus .... \oplus Z_n = 0) - 1 = \prod_{i=1}^{n} (2p_i - 1)$$

Linear cryptanalysis - iterated ciphers

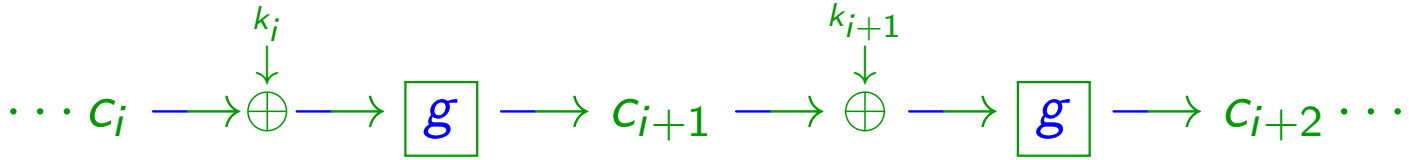


- $(\alpha \cdot c_i) \oplus (\alpha \cdot x) = (\alpha \cdot k)$
- $(\alpha \cdot x) = (\beta \cdot c_{i+1})$ with $p_i \neq 1/2$
- $(\alpha \cdot c_i) \oplus (\beta \cdot c_{i+1}) = 0$ with bias $|p_i - 1/2|$ (whatever value of $(\alpha \cdot k)$)
- linear characteristic (δ_i, δ_{i+1}) with bias $|p_i - 1/2|$ means that

$$(\delta_i \cdot c_i) \oplus (\delta_{i+1} \cdot c_{i+1}) = 0$$

with bias $|p_i - 1/2|$

Linear characteristics - iterated ciphers

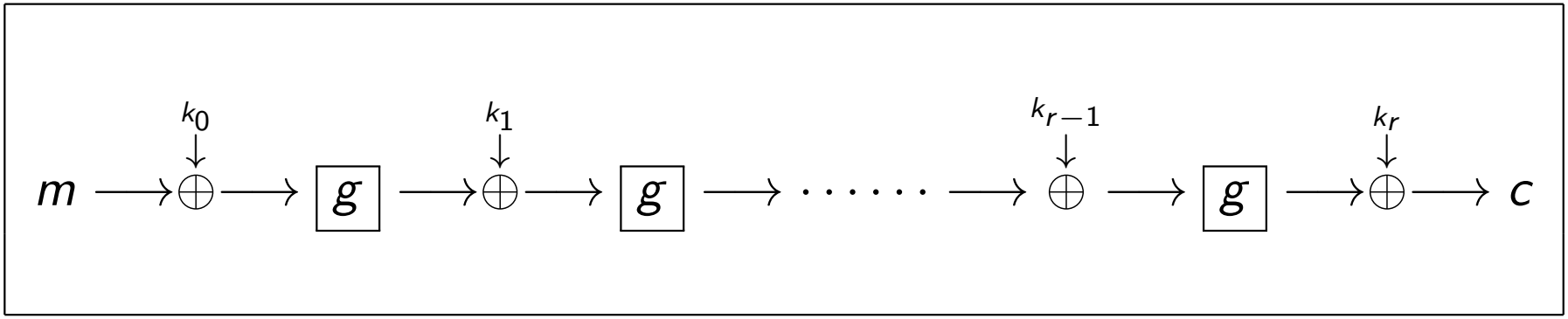


- assume that

$$(\delta_0 \cdot c_0) \oplus (\delta_1 \cdot c_1) = 0 \text{ with bias } |p_1 - 1/2|$$
$$(\delta_1 \cdot c_1) \oplus (\delta_2 \cdot c_2) = 0 \text{ with bias } |p_2 - 1/2|$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$(\delta_{s-1} \cdot c_{s-1}) \oplus (\delta_s \cdot c_s) = 0 \text{ with bias } |p_s - 1/2|$$

- then (u.s.a.) $(\delta_0, \delta_1, \ldots, \delta_s)$ is called an s-round linear characteristic with bias $2^{s-1} \prod_{i=1}^{s} |p_i - 1/2|$ (piling up biases)

Linear attack - r-round iterated cipher

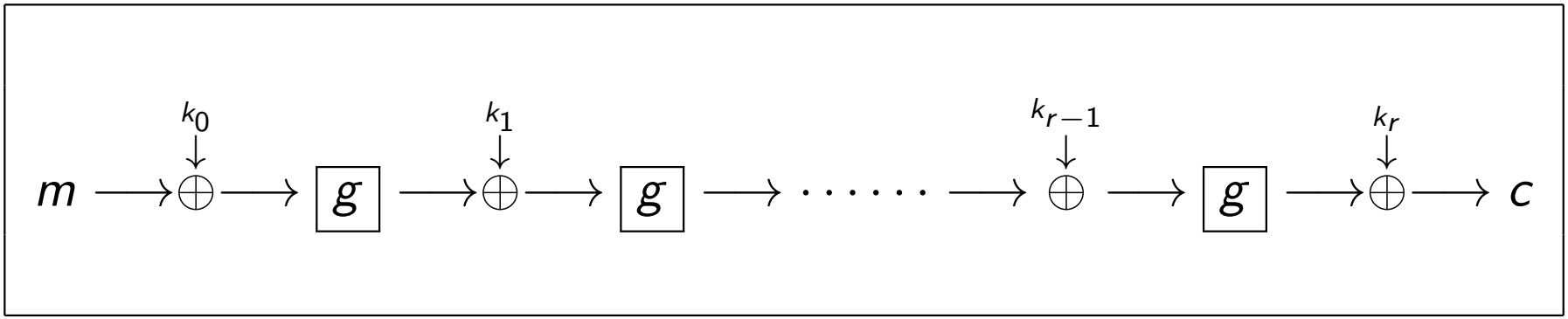


- consider r-round characteristic $(\delta_0, \ldots, \delta_{r-1})$ with bias b
  $(m \cdot \delta_0) \oplus (c_{r-1} \cdot \delta_{r-1}) = 0$
- consider for some value of i:
  $(m \cdot \delta_0) \oplus (g^{-1}(c, i) \cdot \delta_{r-1}) = 0 \quad (*)$
- with $i = k_r$, (*) is characteristic for $r - 1$ rounds

Assumption

For $i \neq k_r$, (*) is random approximation with bias $\simeq 0$

Linear attack (2)



- assume k_r has κ bits
- for $i = 0, \ldots, 2^\kappa - 1$ compute bias of

$$(m \cdot \delta_0) \oplus (g^{-1}(c, i) \cdot \delta_{r-1}) = 0$$

  using N known plaintexts

- guess $k_r = i$, for value of i which produces bias closest to expected
- complexity $N \simeq c \cdot |p - 1/2|^{-2}$, c small constant

Probability of linear characteristics

For attack (k is secret key)

$$\Pr_M((c_{r-1} \cdot \delta_{r-1}) \oplus (m \cdot \delta_0) = 0 \mid k \text{ is key})$$

But k unknown? Average over all keys:

$$\Pr_{M,K}((c_{r-1} \cdot \delta_{r-1}) \oplus (m \cdot \delta_0) = 0)$$

can be hard to calculate

Probability of linear characteristics

Assume that

$$|\Pr_K((c_i \cdot \delta_i) = (c_{i-1} \cdot \delta_{i-1}) \mid c_{i-1} = \gamma) - 1/2|$$

is independent of γ

and

assume that round keys are independent, then bias of

$$|\Pr_{M,K}((c_{r-1} \cdot \delta_{r-1}) \oplus (m \cdot \delta_0) = 0) - 1/2|$$

can be calculated from one-round biases and the Piling-up Lemma

Example: CipherFour: block size 16, r rounds

Round keys independent, uniformly random. One round:

1. exclusive-or round key to text
2. split text, evaluate each nibble via S-box

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

   and concatenate results into 16-bit string $y = y_0, \ldots, y_{15}$

3. permute bits in y according to:

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

   So, $P(y) = y_0, y_4, \ldots, y_{11}, y_{15}$.

Exclusive-or round key to output of last round

Example cipher - linear attack

Linear approximation table for S (entries are $(p - 1/2) \cdot 16$)

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

CipherFour - linear characteristic

- entry (c_x, c_x), value '-6': bias $\frac{6}{16}$, probability $-\frac{6}{16} + \frac{1}{2} = \frac{2}{16}$
- thus $(0\,0\,0\,c_x) \xrightarrow{S} (0\,0\,0\,c_x)$ has bias $\frac{6}{16}$
- since P is linear, $(0\,0\,0\,c_x) \xrightarrow{1r} (1\,1\,0\,0_x)$ is one-round characteristic of bias $\frac{3}{8}$
- also, $(1\,1\,0\,0_x) \xrightarrow{S} (4\,4\,0\,0_x)$, has bias $2(\frac{4}{16})(\frac{4}{16}) = \frac{1}{8}$
- so (u.s.a.) $(0\,0\,0\,c_x) \xrightarrow{2r} (0\,0\,c\,0_x)$ is two-round characteristic of bias $2(\frac{3}{8})(\frac{1}{8}) = \frac{3}{32}$

CipherFour - linear iterative characteristic

Better approach for CipherFour:

$$(8000_x) \xrightarrow{S} (8000_x)$$

has bias $\frac{4}{16}$ and therefore

$$(8000_x) \xrightarrow{1r} (8000_x)$$

is a one-round characteristic of bias $\frac{1}{4}$

Use it to build t-round characteristics

$$(8000_x) \xrightarrow{t\,r} (8000_x)$$

of bias $2^{t-1}(1/4)^t = 2^{-1-t}$

CipherFour - a linear attack

- consider CipherFour with 5 rounds and the four-round characteristic

  $$(8000_x) \xrightarrow{1r} (8000_x) \xrightarrow{1r} (8000_x) \xrightarrow{1r} (8000_x) \xrightarrow{1r} (8000_x)$$

  which (u.s.a.) has bias of $2^{-1-4} = \frac{1}{32}$ according to Piling-up Lemma

- for all values of four bits in last-round key, (partically) decrypt ciphertexts one round, compute bias
- value of key which produces bias of $\frac{1}{32}$ is taken as value of secret key
- $N = c \cdot |p - 1/2|^{-2} = c \cdot 2^{10}$ known plaintexts required to find four bits of last-round key

Linear attack on DES

- iterative 4-round characteristic
- build 14-round characteristic with bias 1.2×2^{-21}
- guess on six round key bits in both first and last rounds
- potential to find 12 key bits
- swap role of plaintext and ciphertext, repeat attack
- in total, potential to find 24 bits of key information
- find remaining 32 bits by an exhaustive search

Linear attack on DES

- estimate - with 2^{45} known plaintexts a DES key can be recovered with 98.8% success rate
- Matsui-test:
  - January, 1994
  - key found in 50 days on 12 HP9735 workstations (120 Mips)
  - 2^{43} known plaintexts
- ciphertext only attack possible, assuming English plaintexts encoded in ASCII

Rounding off

- intro to block ciphers
- differential cryptanalysis
  - characteristics
  - differentials
- linear cryptanalysis
  - linear hulls equivalent to differential
- two most general attacks on block ciphers
- good knowledge of how to protect against these attacks, see AES