Substitution-permutation ciphers

Linear cryptanalysis

Block ciphers

- Modern product ciphers incorporate a sequence of permutation and substitution operations.

Modern product ciphers incorporate a sequence of permutation and substitution operations.
Substitution-permutation networks

- The game is to do this over and over again, substitution for confusion and permutation for defusion.
- A typical iterated cipher requires a round function and key schedule.

Key schedules and round functions

- Round keys, $K^1, ..., K^{Nr}$, are constructed from a random binary key, $K$, using some fixed, public algorithm.
- A round function, $g$, takes inputs $K^r$ and a current state $w^{r-1}$ and produces the next state, $w^r$.

\[
\begin{align*}
  w^0 & \equiv x \\
  w^1 & \equiv g(w^0, K^1) \\
  w^2 & \equiv g(w^1, K^2) \\
  \vdots \\
  w^{Nr-1} & \equiv g(w^{Nr-2}, K^{Nr-1}) \\
  w^N & \equiv g(w^{Nr-1}, K^{Nr}) \\
  y & \equiv w^N
\end{align*}
\]

*The plaintext is the initial state, $w^0$. 
Substitution and permutation

- Plaintext and ciphertext are broken into binary sequences of length $lm$, the block length.
- A permutation $\pi : \{0, 1\}^l \rightarrow \{0, 1\}^l$, called an S-box, substitutes each set of $l$ bits for another.
- A permutation $\pi : \{1, \ldots, lm\} \rightarrow \{1, \ldots, lm\}$ mixes everything up.

In the example shown, . . .

- . . . the S-boxes are given by the substitutions:

  \[
  \begin{array}{cccccccccccc}
  x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
  r_{\text{S}}(x) & D & 1 & F & E & B & A & C & F & E & D & 1 & F & E & B & A & C \\
  \end{array}
  \]

- . . . while the permutation is:

  \[
  \begin{array}{cccccccccccccccccccc}
  x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
  r_{\text{P}}(x) & 1 & 5 & 6 & 10 & 14 & 2 & 7 & 11 & 15 & 4 & 8 & 12 & 16 & 13 & 9 \\
  \end{array}
  \]

Linear cryptanalysis 12-5
We still need a key schedule

- Given a 32-bit key $K = (k_1, ..., k_{32})$, define $K'$, for $1 \leq r \leq 5$, to consist of 16 consecutive bits of $K$, beginning with $k_{4r-3}$.
- For $K$ given by
  
  $\begin{align*}
    K_1 &= 0011 \ 1010 \ 1001 \ 0100 \ 1101 \ 0110 \ 0011 \ 1111 \\
    K_2 &= 1010 \ 1001 \ 0100 \ 1101 \\
    K_3 &= 1001 \ 0100 \ 1101 \ 0110 \\
    K_4 &= 0100 \ 1101 \ 0110 \ 0011 \\
    K_5 &= 1101 \ 0110 \ 0011 \ 1111
  \end{align*}$

For $x = 0010 \ 0110 \ 1011 \ 0111$

$\begin{align*}
  x^0 &= 0010 \ 0110 \ 1011 \ 0111 \\
  x^1 &= 0011 \ 1010 \ 1001 \ 0100 \\
  x^2 &= 0001 \ 1100 \ 0010 \ 0011 \\
  x^3 &= 0100 \ 0110 \ 1101 \ 0001 \\
  x^4 &= 0010 \ 1110 \ 0000 \ 0111 \\
  x^5 &= 1010 \ 1001 \ 0100 \ 1101 \\
  x^6 &= 0011 \ 1000 \ 0010 \ 0110 \\
  x^7 &= 0100 \ 0001 \ 1011 \ 1000 \\
  x^8 &= 0011 \ 0000 \ 1101 \ 0110 \\
  x^9 &= 0001 \ 0100 \ 1101 \ 0101 \\
  x^{10} &= 1000 \ 0111 \ 0100 \ 1100 \\
  x^{11} &= 1010 \ 1001 \ 0100 \ 1101 \\
  x^{12} &= 0010 \ 1010 \ 1101 \ 1001 \\
  x^{13} &= 1101 \ 0110 \ 0011 \ 1111 \\
  x^{14} &= 1011 \ 1100 \ 1101 \ 0010
\end{align*}$
Linear cryptanalysis

- The object of linear cryptanalysis is to find a probabilistic linear relationship between subsets of plaintext and ciphertext bits*.
- The attacker computes XOR of relevant bits in relationship using various keys in order to find a key that yields a nonrandom distribution.

*Thus, this is known-plaintext attack.

Before the details, we need . . .

- Suppose, $X_1, X_2, \ldots$ are independent random variables taking values from the set $\{0, 1\}$ such that:
  \[
  \Pr[X_i = 0] = p_i \quad \text{and} \quad \Pr[X_i = 1] = 1 - p_i
  \]
- The independence of $X_i$ and $X_j$ implies that:
  \[
  \begin{align*}
  &\Pr[X_i = 0, X_j = 0] = p_i p_j \\
  &\Pr[X_i = 0, X_j = 1] = p_i (1 - p_j) \\
  &\Pr[X_i = 1, X_j = 0] = (1 - p_i) p_j \\
  &\Pr[X_i = 1, X_j = 1] = (1 - p_i)(1 - p_j)
  \end{align*}
  \]
- We compute $\Pr[X_i \oplus X_j = 0]$ and $\Pr[X_i \oplus X_j = 1]$. 

A random variable’s bias

- The bias of a random variable $X_i$ is
  $\mathbb{E} = p \cdot \frac{1}{2}$

- Observe that
  $\mathbb{E} \cdot \frac{1}{2} \cdot \mathbb{E} \cdot \frac{1}{2}$
  $\Pr[X_i = 0] = \frac{1}{2} + \mathbb{E}$
  $\Pr[X_i = 1] = \frac{1}{2} - \mathbb{E}$

The piling-up lemma*

Lemma. Let $\mathbb{E}_{i_1, i_2, \ldots, i_k}$ denote the bias of the random variable $X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_k}$. Then

$$\mathbb{E}_{i_1, i_2, \ldots, i_k} = 2^{\sum_{j=1}^{k} \mathbb{E}_{i_j}}$$

Corollary. Let $\mathbb{E}_{i_1, i_2, \ldots, i_k}$ denote the bias of the random variable $X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_k}$. Suppose that $\mathbb{E}_{i_j} = 0$ for some $j$, then $\mathbb{E}_{i_1, i_2, \ldots, i_k} = 0$.

*Proof by induction on $k$. 

Linear cryptanalysis 12-11

Linear cryptanalysis 12-12
Linear approximations of S-boxes

- Consider an S-box \( \mathcal{S} : \{0, 1\}^m \rightarrow \{0, 1\}^n \).
- Assume input chosen uniformly at random from \( \{0, 1\}^m \).
- Similarly, each output co-ordinate \( y_j \) defines a random variable \( Y_j \) taking values 0 and 1.

*Thus, each input co-ordinate \( x_i \) defines a random variable \( X_i \) taking on values 0 and 1 and these \( X_i \) are independent with zero biases.*

In our example, . . .

- . . . the permutation \( \mathcal{S} : \{0, 1\}^4 \rightarrow \{0, 1\}^4 \), is given by

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

- The random variable \( X_1 \oplus X_4 \oplus Y_2 \) is unbiased.

<table>
<thead>
<tr>
<th>X_1</th>
<th>X_2</th>
<th>X_3</th>
<th>X_4</th>
<th>Y_1</th>
<th>Y_2</th>
<th>Y_3</th>
<th>Y_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Linear cryptanalysis 12-13
Linear approximation table $N_L(a, b)$

<table>
<thead>
<tr>
<th>a</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

*Bias of the binary 8-tuple: $\mathbb{E}(a, b) = Pr(a,b) - 1/2 = N_L(a, b) - 1/2$.

A linear attack on an SPN

- We find a linear approximation of $S$-boxes incorporating four active $S$-boxes:
  - $S^1_2: T_1 = U_1^6 \oplus U_1^7 \oplus V_1^3 \oplus V_1^4$ has bias 1/4
  - $S^2_2: T_2 = U_1^6 \oplus V_2^3 \oplus V_8^3$ has bias -1/4
  - $S^3_2: T_3 = U_6^6 \oplus V_6^6 \oplus V_8^3$ has bias -1/4
  - $S^2_3: T_3 = U_1^6 \oplus V_1^3 \oplus V_1^3 \oplus V_8^3$ has bias -1/4

- Assuming independences of $T_i$, piling up lemma implies $T_1 \oplus T_2 \oplus T_3 \oplus T_4$ has bias -1/32.
Canceling “intermediate” variables

- The XOR of the $T_i$ can be expressed in terms of plaintext bits, bits of $u_4$, and key bits.
  - $T_1 = U_1^1 \oplus U_1^5 \oplus V_6^1 \oplus V_8^1$
  - $= X_5 \oplus K_5^1 \oplus X_7 \oplus K_7^1 \oplus X_8 \oplus K_8^1 \oplus V_6^1$
  - $T_2 = U_6^2 \oplus V_6^2 \oplus V_8^2$
  - $= V_6^1 \oplus K_6^2 \oplus V_6^2 \oplus V_8^2$
  - $T_3 = U_6^3 \oplus V_6^3 \oplus V_8^3$
  - $= V_6^2 \oplus K_6^3 \oplus V_6^3 \oplus V_8^3$
  - $T_4 = U_{14}^1 \oplus V_{14}^1 \oplus V_{16}^1$
  - $= V_8^2 \oplus K_{14}^1 \oplus V_{14}^1 \oplus V_{16}^1$

Plaintext, bits of $u^4$ and keybits

- $T_1 \oplus T_2 \oplus T_3 \oplus T_4 = X_5 \oplus X_7 \oplus X_8 \oplus V_6^3 \oplus V_8^3 \oplus V_{14}^3 \oplus V_{16}^3$
  - $\oplus K_5^1 \oplus K_7^1 \oplus K_8^1 \oplus K_6^2 \oplus K_8^2 \oplus K_{14}^3$

- Next, replace the $V_i^3$ by expressions involving $U_i^4$.
  - $V_6^3 = U_6^4 \oplus K_6^4$
  - $V_8^3 = U_{14}^4 \oplus K_{14}^4$
  - $V_{14}^3 = U_8^4 \oplus K_8^4$
  - $V_{16}^3 = U_{16}^4 \oplus K_{16}^4$
Selecting the biased random variable

- The result

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4 \oplus K_5^1 \oplus K_7^1 \oplus K_8^1 \oplus K_6^3 \oplus K_8^3 \oplus K_{14}^4 \oplus K_{16}^4$$

- If the keybits are fixed, then the random variable

$$K_5^1 \oplus K_7^1 \oplus K_8^1 \oplus K_6^3 \oplus K_8^3 \oplus K_{14}^4 \oplus K_{16}^4$$

has fixed value 0 or 1 and

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4$$

has bias equal to $\pm 1/32$, where the sign depends on the values of the unknown key bits.

Candidate subkeys

- Recall our random variable

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4$$

- There are $2^8 = 256$ possibilities for the keys that are XORed with the $2^{nd}$ and $4^{th}$ S-boxes in the final row.

- For each plaintext, ciphertext pair a partial decryption is possible, and the value of the random variable is computed.
**Success**

- It is suggested that a linear attack based on a linear approximation having bias equal to $\varepsilon$ will be successful if the number of plaintext-ciphertext pairs is approximately $c\varepsilon^2$, for a small constant $c$. 