Aalto University
School of Science
and Technology

Linear Cryptanalysis

Kaisa Nyberg

Department of Information and Computer Science
Aalto University School of Science
kaisa.nyberg@aalto.fi

June 6, 2013

Outline

- Matsui's Algorithms
- Trail Correlations
- Linear Hull

Section: Matsui's Algorithms

Symmetric-Key Encryption

$k \in \mathcal{K}$	the key
$x \in \mathcal{P}$	the plaintext
$y \in \mathcal{C}$	the ciphertext

Encryption method is a family $\{E_k\}$ of transformations $E_k : \mathcal{P} \to \mathcal{C}$, parametrised using the key k such that for each encryption transformation E_k there is a decryption transformation $D_k : \mathcal{C} \to \mathcal{P}$, such that $D_k(E_k(x))) = x$, for all $x \in \mathcal{P}$.

Block Cipher

The data to be encrypted is split into blocks x_i, $i = 1, \ldots, N$ of fixed length n. A typical value of n is 128. $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2^n$, $\mathcal{K} = \mathbb{Z}_2^\ell$.

For the purposes of linear cryptanalysis a block cipher is considered as a vectorial Boolean function

$$f : \mathbb{Z}_2^n \times \mathbb{Z}_2^\ell \to \mathbb{Z}_2^n \times \mathbb{Z}_2^n \times \mathbb{Z}_2^\ell, \;\; f(x, k) = (x, k, E_k(x))$$

Linear approximation with mask vector (u, v, w) of a block cipher is a relation

$$u \cdot x + v \cdot k + w \cdot E_k(x).$$

Correlation

- The correlation between two Boolean functions $f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2$ and $g : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2$ is defined as

  $$c(f,g) = 2^{-n}\left(\#\{x \in \mathbb{Z}_2^n \mid f(x) = g(x)\} - \#\{x \in \mathbb{Z}_2^n \mid f(x) \neq g(x)\}\right)$$

- Correlation $c(f,0)$ is called the correlation (sometimes aka bias) of f, and also denoted as $c_x(f(x))$.
- Correlation of f is the normalised bias of f:

  $$c_x(f(x)) = 2^{-n}\mathcal{E}(f) = 2^{-n}\sum_x (-1)^{f(x)}$$

  (see Anne's lecture).
- Linear cryptanalysis makes use of large correlations of Boolean functions in cipher constructions.

Algorithm 1

Matsui's Algorithm 1 is a statistical cryptanalysis method for finding one bit of the key with the following steps

1. Select the mask vector (u, v, w) for the linear approximation

$$u \cdot x + v \cdot k + w \cdot E_k(x)$$

   such that the correlation

$$c = c_x(u \cdot x + v \cdot k + w \cdot E_k(x))$$

   deviates from 0 as much as possible, for almost all keys k.

2. Sample plaintext-ciphertext pairs $x, E_k(x)$ for a fixed (unknown) key k and determine the empirical correlation $\hat{c}$ of the linear relation:

$$u \cdot x + w \cdot E_k(x)$$

3. If c and $\hat{c}$ are of the same sign, output $v \cdot k = 0$. Else output $v \cdot k = 1$.

Algorithm 2

Matsui's Algorithm 2 is a statistical cryptanalysis method for finding a part of the last round key for block ciphers where the encryption can be written in the form $E_{k',k_r}(x) = G_{k_r}(E'_{k'}(x))$ where k_r is relatively short.

1. Select the mask vector (u, v, w) for the linear approximation
$$u \cdot x + v \cdot k' + w \cdot E'_{k'}(x)$$
such that the correlation
$$c = c_x(u \cdot x + v \cdot k' + w \cdot E_{k'}(x))$$
deviates from 0 as much as possible, for almost all keys k'.
2. Sample plaintext-ciphertext pairs (x, E_{k',k_r}). For each last round key candidate $\tilde{k}_r$, compute pairs $(x, y = G^{-1}_{\tilde{k}_r}(E_{k'}(x))$ and determine the empirical correlation $\hat{c}(\tilde{k}_r)$ of the linear relation: $v \cdot x + w \cdot y$.
3. Output the value $\tilde{k}_r$, for which $|\hat{c}(\tilde{k}_r)|$ is the largest.
4. Additionally, one can determine the value $v \cdot k'$.

Statistical Tests

- Linear cryptanalysis makes use of a statistical hypothesis test.
- Algorithm 1 makes a decision between

$$\begin{aligned} \mathrm{H}_0 &: \quad v \cdot k = 0 \\ \mathrm{H}_1 &: \quad v \cdot k = 1 \end{aligned}$$

- Algorithm 2 makes a decision between

$$\begin{aligned} \mathrm{H}_0 &: \quad \tilde{k}_r = k_r, \text{ that is, } G_{\tilde{k}_r}^{-1}(E_{k',k_r}(x)) = E'_{k'}(x), \text{ for all } x \\ \mathrm{H}_1 &: \quad \tilde{k}_r \text{ is not correct, that is, data pairs } (x, G_{\tilde{k}_r}^{-1}(E_{k',k_r}(x)) \\ &\quad\ \text{are not from the cipher} \end{aligned}$$

Probability of Success in Algorithm 1

Consider the case $c > 0$ and $v \cdot k = 0$. Other cases are similar.

Let N be the size of the sample and N_0 be the observed number of plaintexts x such that $u \cdot x + w \cdot E_K(x) = 0$.

N_0 is binomially distributed with expected value Np and variance $Np(1-p)$, where $p = \frac{c+1}{2}$. Then

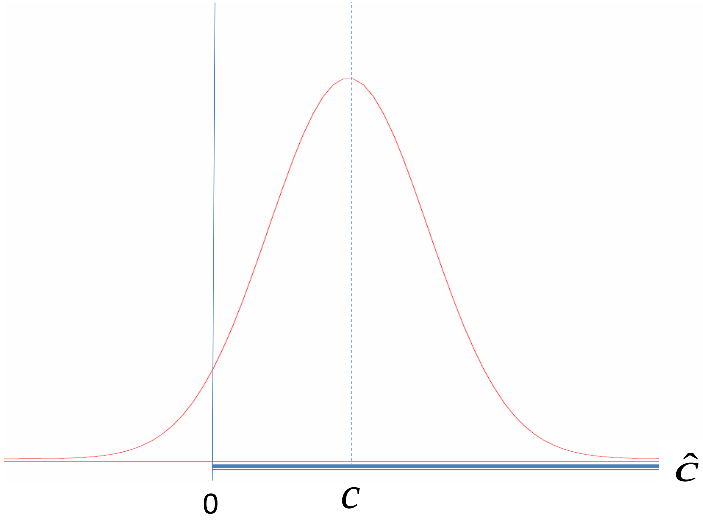
$$Z = \frac{N_0 - Np}{\sqrt{Np(1-p)}} \sim \mathcal{N}(0,1)$$

where $\mathcal{N}(0,1)$ is the standard normal distribution. Then the bit $v \cdot k$ is correctly determined if the observed correlation $\hat{c}$ is positive, which happens if and only if $N_0 > N/2$, or equivalently, $Z > -c\sqrt{N}$. Hence the probability of success can be estimated as

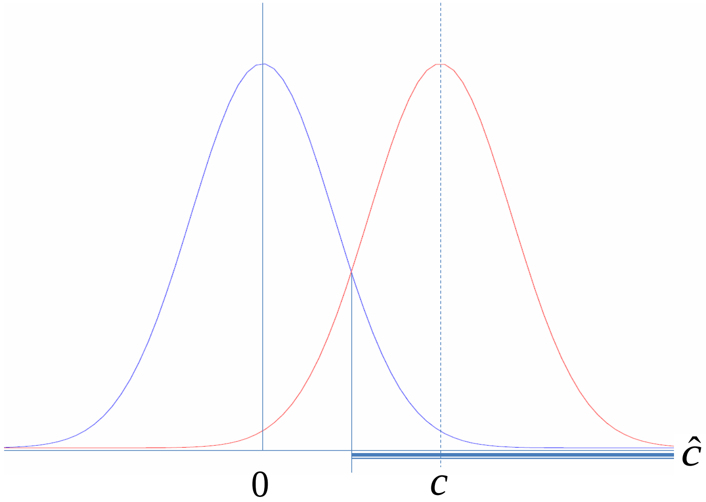
$$1 - \Phi(-c\sqrt{N})$$

where Φ is the cumulative density function of $\mathcal{N}(0,1)$. The probability is 0.921 for $N = 1/c^2$. This gives an estimate of the number N of plaintext-ciphertext pairs for successful cryptanalysis.

Success Area in Algorithm 1



Success Area in Algorithm 2



Section: Trail Correlations

Correlation for Iterated Block Cipher

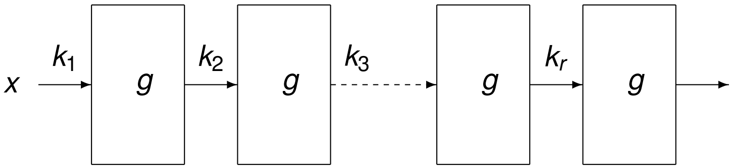
We focus on key alternating iterated block ciphers. Let $(k_1, k_2, \ldots, k_r)$ be the extended key with the round keys k_i derived from k and assume that E_k has the following structure

$$E_k(x) = g(\ldots g(g(g(x + k_1) + k_2) \ldots) + k_r).$$

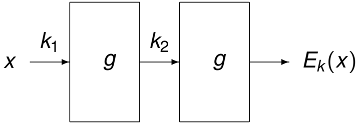
Then

$$c_x(u \cdot x + w \cdot E_k(x)) = \sum_{\tau_2, \ldots, \tau_r} \prod_{i=1}^{r} (-1)^{\tau_i \cdot k_i} c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z)),$$

where $\tau_1 = u$ and $\tau_{r+1} = w$. [JD94]



Proof in case $r = 2$



$$c_x(u \cdot x + w \cdot E_k(x)) = 2^{-n} \sum_x (-1)^{u \cdot x + w \cdot E_k(x)}$$

$$= 2^{-n} \sum_x (-1)^{u \cdot x + w \cdot g(g(x+k_1)+k_2)}$$

$$= 2^{-2n} \sum_\tau \sum_x (-1)^{u \cdot x + \tau \cdot g(x+k_1)} \sum_y (-1)^{\tau \cdot y + w \cdot g(y+k_2)}$$

$$= 2^{-2n} \sum_{z_1} (-1)^{u \cdot (z_1+k_1) + \tau \cdot g(z_1)} \sum_{z_2} (-1)^{\tau \cdot (z_2+k_2) + w \cdot g(z_2)}$$

$$= \sum_\tau (-1)^{u \cdot k_1 + \tau \cdot k_2} c_{z_1}(u \cdot z_1 + \tau \cdot g(z_1)) c_{z_2}(\tau \cdot z_2 + w \cdot g(z_2)).$$

Linear Trail with Fixed Key

We set $z_1 = x + k_1$ and $z_i = g(z_{i-1}) + k_i$, $i = 2, \ldots, r$, and $v_1 = u$, and $v_{r+1} = w$. Then

$$\bigoplus_{i=1}^{r} (v_i \cdot z_i + v_{i+1} \cdot g(z_i)) = u \cdot x + v_1 \cdot k_1 + \ldots + v_r \cdot k_r + w \cdot E_k(x).$$

The sequence $v = (v_1, \ldots, v_r, v_{r+1})$, where $v_1 = u$ and $v_{r+1} = w$ is called a linear trail from u to w over E_k.
We set $v \cdot k = v_1 \cdot k_1 + \ldots + v_r \cdot k_r$. Then the linear trail $v = (v_1, \ldots, v_r, v_{r+1})$ gives the linear approximation

$$u \cdot x + v \cdot k + w \cdot E_k(x)$$

over the key-alternating block cipher E_k.

To run Matsui's Algorithms 1 and 2 we need an estimate of its correlation that holds for almost all keys.

Trail Correlation for Fixed Key

Using

$$c_x(u \cdot x + w \cdot E_k(x)) = \sum_{\tau_2,\ldots,\tau_r} \prod_{i=1}^{r} (-1)^{\tau_i \cdot k_i} c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z)),$$

where $\tau_1 = u$ and $\tau_{r+1} = w$, we obtain

$$\begin{aligned} c_x(u \cdot x + v \cdot k + w \cdot E_k(x)) &= (-1)^{v \cdot k} c_x(u \cdot x + w \cdot E_k(x)) \\ &= (-1)^{v \cdot k} \sum_{\tau_2,\ldots,\tau_r} \prod_{i=1}^{r} (-1)^{\tau_i \cdot k_i} c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z)) \\ &= \prod_{i=1}^{r} c_z(v_i \cdot z + v_{i+1} \cdot g(z)) + \sum_{\tau \neq v} \prod_{i=1}^{r} (-1)^{\tau_i \cdot k_i} c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z)). \end{aligned}$$

Taking the average over k_i will make the second term vanish.

Average Trail Correlation

Assumption. Round keys $k_1, \ldots, k_r$ take on all possible values.

Theorem. Average correlation of a (non-zero) linear approximation trail $v - 1, v_2, \ldots, v_r, v_{r+1}$ from u to w taken over round keys $k_1, k_2, \ldots, k_r$ is

$$\begin{aligned}\tilde{c}(u, v, w) &= \mathrm{Avg}_k c_x(u \cdot x + v \cdot k + w \cdot E_k(x)) \\ &= \prod_{i=1}^{r} c_z(v_i \cdot z + v_{i+1} \cdot g(z))\end{aligned}$$

- Matsui used in the first practical linear cryptanalysis of DES:

$$\prod_{i=1}^{r} c_z(v_i \cdot z + v_{i+1} \cdot g(z)) \approx (-1)^{v \cdot k} c_x(u \cdot x + w \cdot E_k(x))$$

- Is this a good estimate for any fixed key?

Case of Single Dominant Trail

Matsui used

$$c_x(u \cdot x + w \cdot E_k(x)) \approx (-1)^{v_1 \cdot k_1 + \ldots + v_r \cdot k_r} \prod_{i=1}^{r} c_z(v_i \cdot z + v_{i+1} \cdot g(z)),$$

while in reality

$$c_x(u \cdot x + w \cdot E_k(x)) = \sum_{\tau_2, \ldots, \tau_r} (-1)^{\tau_1 \cdot k_1 + \ldots + \tau_r \cdot k_r} \prod_{i=1}^{r} c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z)).$$

The estimate works, if the selected trail $v_1, \ldots, v_{r+1}$ from u to w has an exceptionally large average trail correlation

$$\prod_{i=1}^{r} c_z(v_i \cdot z + v_{i+1} \cdot g(z))$$

and for $\tau \neq v$

$$c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z)) \approx 0.$$

Example

$E_k(x) = g(g(x) + k)$ where g is the AES 8×8 S-box and k is eight bits. The maximum $|c(u \cdot x + v \cdot g(x))|$ is 2^{-3}.Then all 8-bit u and w have trails with equally good trail correlations, and there exist several values v such that

$$|\tilde{c}(u, v, w)|$$

taken over E_k achieves its maximum possible value 2^{-6}.

On the other hand, for a given (u, w) the true values $|c_x(u \cdot x + w \cdot E_k(x))|$ vary a lot with the key k.

Consider $(u, w) = (\mathtt{EA}, \mathtt{EA})$. Then we have $|c_x(u \cdot x + w \cdot E_k(x))| = 0$, for 21 keys k.

For the remaining 235 keys we have $|c_x(u \cdot x + w \cdot E_k(x))| \geq 2^{-6}$.

There are no single dominant trails.

Linear Trails for SPN: S-box Layer

$$\begin{aligned} x &= (x_1, x_2, \ldots, x_t) \\ g(x) &= (S_1(x_1), S_2(x_2), \ldots, S_t(x_t)) \end{aligned}$$

$$\begin{aligned} u &= (u_1, u_2, \ldots, u_t) \\ v &= (v_1, v_2, \ldots, v_t) \end{aligned}$$

$$c_x(u \cdot x + v \cdot g(x)) = \prod_{j=1}^{t} c_{x_j}(u_j \cdot x_j + v_j \cdot g(x_j))$$

To maximize the correlation one usually takes almost all u_j and v_j equal to zero, since for those j one has $c_{x_j}(u_j \cdot x_j + v_j \cdot g(x_j)) = 1$.

Linear Trails for SPN: Linear Layer

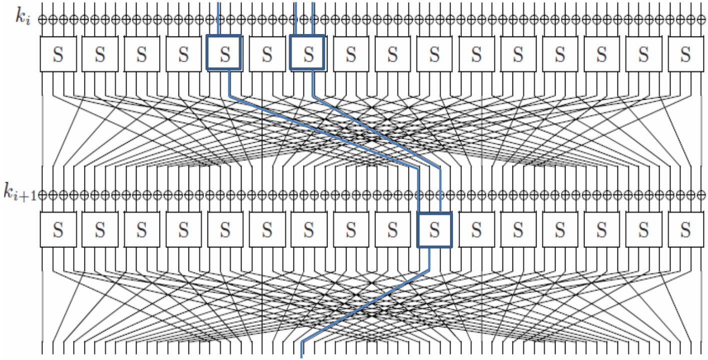
$$g(x) = Mx$$

$$\begin{aligned} c_x(u \cdot x + v \cdot Mx)) &= c_x(u \cdot x + M^t v \cdot x)) \\ &= \begin{cases} 1 & \text{if } u = M^t v \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

This uniquely determines the masks over the linear layer.

For text-book examples of how to construct linear trails over SPNs, see Stinson or Knudsen-Robshaw.

SPN Trails



Section: Linear Hull

Estimating Data Complexity

Data complexity is proportional to c^{-2}, where

- in Algorithm 1

$$c = c_x(u \cdot x + v \cdot k + w \cdot E_k(x))$$

- in Algorithm 2

$$c = c_x(u \cdot x + w \cdot E'_{k'}(x))$$

For Algorithm 1 we use $\tilde{c}$ as an estimate of c, and the value $\tilde{c}^{-2}$ is a commonly used estimate for data complexity for Algorithm 1 in the case of a single dominant trail.

Algorithm 2 needs that $c_x(u \cdot x + w \cdot E'_{k'}(x))$ is large. Several trails may contribute to such a large correlation value. Algorithm 2 works if for a substantial proportion of keys $|c_x(u \cdot x + w \cdot E'_{k'}(x))|$ is large, or what is equivalent,

$$c_x(u \cdot x + w \cdot E'_{k'}(x))^2 = c_x(u \cdot x + v \cdot k' + w \cdot E'_{k'}(x))^2$$

is large.

The Fundamental Theorem

By Jensen's inequality

$$\mathrm{Avg}_k c_x(u \cdot x + v \cdot k + w \cdot E_k(x))^2 \geq \tilde{c}(u, v, w)^2,$$

for all v, and in general the strict inequality holds. More accurately, the following theorem holds

The Linear Hull Theorem [KN94, KN01] If the round keys of a block cipher E_k take on all values, then

$$\mathrm{Avg}_k c_x(u \cdot x + w \cdot E_k(x))^2 = \sum_{\tau} \tilde{c}(u, \tau, w)^2.$$

We denote

$$\mathrm{pot}(u, w) = \mathrm{Avg}_k (c_x(u \cdot x + w \cdot E_k(x)))^2$$

and call it the potential of (u, w).

Example Cont'd

Consider the previous example. We saw that in terms of single trails, all (u, w) are about equally good, but there are no dominant trails.

Also in terms of linear hulls, all (u, w) are about equally good:

$$\mathrm{pot}(\mathtt{33}, \mathtt{D5}) = 2^{-10.40} \leq \mathrm{pot}(u, w) \leq 2^{-9.65} = \mathrm{pot}(\mathtt{EA}, \mathtt{EA})$$

$|c(u \cdot x + w \cdot E_k(x))|^2 \geq \mathrm{pot}(\mathtt{EA}, \mathtt{EA})$, for 76 keys k.

The weakest of (u, w) is $(\mathtt{33}, \mathtt{D5})$. For this mask pair $|c_x(u \cdot x + w \cdot E_k(x))| = 0$, for 33 keys k.

For the remaining 223 keys we have $|c_x(u \cdot x + w \cdot E_k(x))| \geq 2^{-6}$.

$|c(u \cdot x + w \cdot E_k(x))|^2 \geq \mathrm{pot}(\mathtt{33}, \mathtt{D5})$, for 80 keys k.

Linear Hull Effect in Algorithm 2

Corollary Consider Algorithm 2, and let ρ be the (significant) fraction of keys k' such that

$$\begin{aligned} \mathrm{pot}(u, w) &= \mathrm{Avg}_{\kappa}(c_x(u \cdot x + w \cdot E'_{\kappa}(x)))^2 \\ &\leq c_x(u \cdot x + w \cdot E'_{k'}(x))^2 \end{aligned}$$

Assume that the round keys of E' take on all values. Then for the fraction of ρ of the keys k' the data complexity for the successful recovery of the last round key k_r is upperbounded by $\mathrm{pot}(u, w)^{-1}$

To prove resistance against linear cryptanalysis the upperbound for data complexity given by $\mathrm{pot}(u, w)$ is relevant.

Computing an Estimate of $\mathrm{pot}(u, w)$

$$
\begin{aligned}
\mathrm{pot}(u, w) &= \mathrm{Avg}_k c_x(u \cdot x + w \cdot E_k(x))^2 = \sum_{\tau_2, \ldots, \tau_r} \prod_{i=1}^{r} c_z(\tau_i \cdot z + \tau_{i+1} \cdot g(z))^2 \\
&= \sum_{\tau_r} c_z(\tau_r \cdot z + w \cdot g(z))^2 \sum_{\tau_{r-1}} c_z(\tau_{r-1} \cdot z + \tau_r \cdot g(z))^2 \\
&\quad \cdots\cdots \quad \sum_{\tau_3} c_z(\tau_3 \cdot z + \tau_4 \cdot g(z))^2 \\
&\quad \sum_{\tau_2} c_z(\tau_2 \cdot z + \tau_3 \cdot g(z))^2 c_z(u \cdot z + \tau_2 \cdot g(z))^2
\end{aligned}
$$

- This expression gives an iterative algorithm: start from the bottom line to compute for each τ_3 the value on the last line.
- Can be made feasible by restricting to τ with low Hamming weight and keeping only the largest values from each iteration.
- Restrictions on τ will lead to a lower bound of $\mathrm{pot}(u, w)$, which is still much larger than any $\tilde{c}(u, v, w)^2$.

Linear Hull Effect in Algorithm 1

Assume a (hypothetical) situation where we have two linear trails (u, v, w) and (u, τ, w) such that $|\tilde{c}(u, v, w)| = |\tilde{c}(u, \tau, w)|$, and that $\tilde{c} = 0$ for all other trails, see also [AES book]. Then

$$c_x(u \cdot x + w \cdot E_k(x)) = (-1)^{v \cdot k}\tilde{c}(u, v, w) + (-1)^{\tau \cdot k}\tilde{c}(u, \tau, w).$$

We denote by c the common value $|\tilde{c}(u, v, w)| = |\tilde{c}(u, \tau, w)|$. It follows that for half of the keys k it holds

$$|c_x(u \cdot x + w \cdot E_k(x))| \quad = \quad 2c,$$

and by observing $c_x(u \cdot x + w \cdot E_k(x))$ from the data we obtain two bits $v \cdot k$ and $\tau \cdot k$ of the key k with high confidence using about c^{-2} data pairs (x, y).

If k is in the other half, then $c_x(u \cdot x + w \cdot E_k(x)) = 0$. Then we get one bit $(v + \tau) \cdot k$ of information of the key by observing the data and using about the same number of pairs as above.

On the average, we get 3/2 bits of information of the key.

Cited Papers and Books

[KN94] K. Nyberg: Linear approximation of block ciphers. In Advances in Cryptology - EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science. Springer-Verlag, 1995.

[JD94] J. Daemen: Correlation Matrices. In Fast Software Encryption, FSE 2, volume 1008 of Lecture Notes in Computer Science. Springer-Verlag, 1995.

[KN01] K. Nyberg: Correlation theorems in cryptanalysis. Discrete Applied Mathematics, 111:177-188, 2001.

[AES book] J. Daemen and V. Rijmen: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag, 2002.

[Stinson] D. R. Stinson: Cryptography: Theory and Practice, 3rd ed.. CRC Press, 2005.

[Knudsen-Robshaw] L. R. Knudsen and M. Robshaw: The Block Cipher Companion. Springer, 2011.