# Enumerating Nondegenerate Permutations

Luke O'Connor
Department of Computer Science
University of Waterloo, Ontario, Canada, N2L 3G1
email: ljpoconn@watmath.uwaterloo.ca

**Abstract**

Every cryptosystem with an $n$-bit block length may be modeled as a system of $n$-bit boolean equations. The cipher is said to be nondegenerate if the equation $f_i$ that describes the output $c_i$ is nondegenerate, for $1 \leq i \leq n$. Let $\mathcal{N}^{n,n}$ be the set of nondegenerate permutations. We will derive an exact expression for $|\mathcal{N}^{n,n}|$, and show that

$$\frac{|\mathcal{N}^{n,n}|}{2^n!} = 1 + o\left(\frac{\sqrt{2^n}}{2^{2^{n-1}+n}}\right).$$

## 1 Introduction

One of the basic design criteria for a block encryption function is to ensure that each ciphertext bit depends nonlinearly on each message bit, for each fixed key. For example, this property is essential if the encryption function is to be used as the basis for an authentication algorithm [7], or if we are to avoid meet-in-the-middle attacks based on bit independence [3]. More generally, total nonlinear dependence between the message and ciphertext is a necessary condition for small changes in the message to produce large unpredictable changes in the ciphertext. This phenomenon, known as the avalanche effect [6], reduces the information that a cryptanalyst can gain by considering the encryption of similar messages. For a discussion of other design criteria for block ciphers see [1] [6] [14] [18].

A boolean equation $f$ is nondegenerate if its output depends on all the input bits to the equation. As each ciphertext bit can be described by a boolean equation in the message and the key, we are then interested in encryption functions for which the output, or the ciphertext, is described by a system of nondegenerate equations. Ciphers with this property will be called *nondegenerate ciphers.*

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 368-377, 1991.

Kam and Davida [11] were the first to show that large nondegenerate product ciphers, the so-called SP-networks, can be constructed from small nondegenerate substitutions, or $S$-boxes. The Kam and Davida algorithm selects special transpositions at each round of the product cipher, which cause the influence of a variable to propagate throughout the intermediate ciphertext in a regular and controlled manner, such that the final round the propagation is complete (for a reason possibly similar to this, Kam and Davida called such functions *complete* rather than nondegenerate). Subsequently, Ayoub has shown that a similarly constructed product cipher, employing only *random* transpositions, would almost certainly guarantee the nondegeneracy property of the product cipher [2]. Ayoub derives a combinatorial expression for the probability that a product cipher is nondegenerate, and then demonstrates empirically that a randomly constructed product cipher attains the nondegeneracy property after a small number of rounds.

From the work of Ayoub we may hypothesize that *most product ciphers are nondegenerate.* We further observe that product ciphers give rise to a very general class encryption functions, and in fact it has been shown that for a given block size $n$, these ciphers can generate the alternating group of the set $\{0, 1, \cdots 2^n - 1\}$ [4][5][12]. Thus we may further hypothesize that for a given $n$, most *$n$-bit permutations* are nondegenerate.

Our main result is to show that almost all systems of boolean equations which describe a permutation will be nondegenerate. Consider the problem of determining the number of $n$-bit to $m$-bit boolean functions that are nondegenerate. The case where $m = 1$ has been solved by Harrison [9], and also by Hu [10]. If we let $\mathcal{N}^n$ denote the set of $n$-bit nondegenerate functions, then the number of $n$-bit to $m$-bit degenerate functions is simply $(|\mathcal{N}^n|)^m$. However, as noted by Mitchell [14], the difficulty of this problem seems to increase if we further require that the functions be nonsingular ($n = m$ and the functions are invertible).

Let $\mathcal{N}^{n,n}$ denote the set of nondegenerate $n$-bit nonsingular functions, or nondegenerate $n$-bit permutations. In this paper we will prove that

$$\frac{|\mathcal{N}^{n,n}|}{2^n!} = 1 + O\left(\frac{n^2}{2^{2^{n-1}}}\right), \tag{1}$$

and it clearly follows that $|\mathcal{N}^{n,n}| \sim 2^n!$. The immediate implication is that as $n$ increases, the probability of randomly selecting a nondegenerate $n$-bit permutation tends to unity.

This paper is organized as follows. Section 2 contains the definitions and notations that will be used throughout the paper. In §3 we consider asymptotic estimates for the number of degenerate $n$-bit functions. In §4 we prove our main theorem by deriving an expression for $|\mathcal{N}^{n,n}|$ using the inclusion-exclusion principle.

## 2 Definitions and Notations

The following definitions will be used throughout the paper when describing boolean functions and permutations.

**Definition 2.1** Let $f$ be an $n$-bit function where $f : \{0,1\}^n \rightarrow \{0,1\}$. For $0 \leq i \leq 2^n-1$, let $b(i)$ denote that element of $\{0,1\}^n$ whose decimal representation is $i$. The *vector representation* $V_f$ *of a function* $f$ is defined as $V_f = v_0, v_1, \cdots v_{2^n-1} \in \{0,1\}^{2^n}$ where $v_i = f(b(i))$, $0 \leq i \leq 2^n - 1$. The *distance between two n-bit functions* $f$ and $g$ is defined as $d(f,g) = w(V_f \oplus V_g)$ where $w(\cdot)$ is the hamming weight function. □

Let the symmetric group on $2^n$ elements be denoted as $S_{2^n}$.

**Definition 2.2** For $P \in S_{2^n}$, define $V_P^i = v_0, v_1, \cdots v_{2^n-1} \in \{0,1\}^{2^n}$ as $v_j = y_i$, where $P(j) = Y = y_1, y_2, \cdots y_m \in \{0,1\}^m$, $0 \leq j \leq 2^n - 1$, $1 \leq i \leq m$. The $n$-tuple of boolean functions $F = [f_1, f_2, \cdots f_m]$ is said to *realize the permutation* $P$ if $w(V_P^i \oplus V_{f_i}) = 0$, $1 \leq i \leq m$. □

**Definition 2.3** Let $F = [f_1, f_2 \cdots f_k]$ be a $k$-tuple of $n$-bit functions. Let $\mathcal{E}(F)$ be defined as the set

$$\mathcal{E}(F) = \{\ F' \mid F' = [f_1, \cdots f_k, f'_{k+1}, \cdots f'_n] \in S_{2^n}\}. \tag{2}$$

Then $\mathcal{E}(F)$ will be called the *extension set of* $F$. If $|\mathcal{E}(F)| > 0$ then we will say that $F$ is *extendible*. □

The following theorem was used implicitly by Gordon and Retkin [8].

**Theorem 2.1** For $k$, $0 \leq k \leq n-1$, and an arbitrary $k$-tuple $F$ of $n$-bit functions, if $F$ is extendible then $|\mathcal{E}(F)| = (2^{n-k}!)^{2^k}$.

*proof.* Proof by induction on $k$ [16]. □

## 3 Nondegenerate Functions

An $n$-bit function $f$ is *vacuous* in variable $x_i$ if for all of $x_1, x_2, \cdots x_n \in \{0,1\}^n$,

$$f(x_1, \cdots x_i, \cdots, x_n) = f(x_1, \cdots, \overline{x_i}, \cdots x_n). \tag{3}$$

If $f$ is vacuous in any variable then $f$ is *degenerate*, otherwise $f$ is *nondegenerate*. Let $\mathcal{N}_k^n$ be the set of $n$-bit nondegenerate functions of weight $k$, and let $\mathcal{N}^n = \bigcup \mathcal{N}_k^n$. For degenerate functions, we may similarly define the sets $\mathcal{D}^n$ and $\mathcal{D}_k^n$. It follows that $|\mathcal{D}_k^n| = \binom{2^n}{k} - |\mathcal{N}_k^n|$.

The number of nondegenerate functions has been determined by Harrison using inversion formulae [9, p169], and it follows that $|\mathcal{N}^n| \sim 2^{2^n}$. Thus most $n$-bit functions are nondegenerate.

**Theorem 3.1 (Harrison)** The number of degenerate $n$-bit functions of weight $k$ is

$$|\mathcal{D}_k^n| = \sum_{1 \le j \le \nu_2(k)} (-1)^{j-1} \binom{n}{j} \binom{2^{n-j}}{k \cdot 2^{-j}}. \tag{4}$$

□

For $1 \le j \le n-1$, let $A_k^n(j) = \binom{2^{n-j}}{k2^{-j}}$, which are the coefficients of the sum in eq. (??). In general, $A_k^n(1)$ dominates the sum, and we will prove this for the case where $k = 2^{n-1}$, as we will require an asymptotic estimate of $|\mathcal{D}_{2^{n-1}}^n|$ in a later section.

**Theorem 3.2**

$$|\mathcal{D}_{2^{n-1}}^n| = A_{2^{n-1}}^n(1)\Big(1 + o\Big(\frac{1}{2^{2^{n-2}}}\Big)\Big). \tag{5}$$

*proof.* Using bounds for the factorial function [15, p183], we have that for $2 \le j \le n-1$,

$$\begin{aligned}
\frac{A^n(j)}{A_{2^{n-1}}^n(1)} &= \frac{(2^{n-2}!)^2 \cdot 2^{n-j}!}{2^{n-1}! \cdot (2^{n-j-1})^2}, & (6)\\
&< \frac{2^{2^{n-j}}}{2^{2^{n-1}}} \cdot \sqrt{\pi \cdot 2^{j-1}} \cdot \frac{exp\Big[\frac{2}{12 \cdot 2^{n-2}} + \frac{1}{12 \cdot 2^{n-j}}\Big]}{exp\Big[\frac{2}{12 \cdot 2^{n-j-1}+1/4} + \frac{1}{12 \cdot 2^{n-1}+1/4}\Big]}, & (7)\\
&= o\Big(\frac{1}{2^{2^{n-2}}}\Big). & (8)
\end{aligned}$$

The theorem follows from

$$\begin{aligned}
|\mathcal{D}_{2^{n-1}}^n| &= \sum_{j=1}^{n-1} (-1)^{j-1} \binom{n}{j} A_{2^{n-1}}^n(j), & (9)\\
&= A_{2^{n-1}}^n(1) \cdot \Big[ \sum_{j=1}^{n-1} (-1)^{j-1} \binom{n}{j} \frac{A_{2^{n-1}}^n(j)}{A_{2^{n-1}}^n(1)} \Big], & (10)\\
&= A_{2^{n-1}}^n(1) \cdot \Big[ 1 + o\Big(\frac{1}{2^{2^{n-2}}}\Big) \cdot \sum_{j=2}^{n-1} (-1)^j \binom{n}{j} \Big], & (11)\\
&= A_{2^{n-1}}^n(1) \cdot \Big[ 1 + o\Big(\frac{1}{2^{2^{n-2}}}\Big) \Big]. & (12)
\end{aligned}$$

□

# 4 Nondegenerate Permutations

In this section we will determine the number of $n$-bit permutations that are nondegenerate.

**Definition 4.1** Let $\mathcal{N}^{n,n}$ be the set of permutations $P \in S_{2^n}$, such that if $P$ is realized by $F = [f_1, f_2, \cdots f_n]$ then $f_i \in \mathcal{N}^n_{2^n-1}$, $1 \leq i \leq n$. □

Our technique is to enumerate all sets $F = [f_1, f_2, \cdots f_k]$ where $f_i \in \mathcal{D}^n_{2^n-1}$, and then compute the extension set of $F$. This method allows us to compute the necessary coefficients in the inclusion-exclusion expansion for $|\mathcal{N}^{n,n}|$.

**Definition 4.2** For $k$, $1 \leq k \leq n$, let $C^n(k)$ denote the number of tuples $F = [f_1, f_2, \cdots f_k]$ such that

1. $\mathcal{E}(F) \neq \emptyset$ ;
2. $f_i \in \mathcal{D}^n_{2^n-1}$, $1 \leq i \leq k$. □

**Definition 4.3** For $k$, $1 \leq k \leq n$, let $C^n_k$ be the set of all $n$-bit permutations $P$ such that if $P$ is realized by $F = [f_1, f_2, \cdots f_n]$ then $f_i \in \mathcal{D}^n_{2^n-1}$, $1 \leq i \leq k$. □

Thus $C^n(k)$ is the number of degenerate $k$-tuples that realize the first $k$ bits of some permutation, and $C^n_k$ is the set of all $k$-tuples of degenerate functions that can be extended to permutations. The next theorem shows that the $|C^n_i|$ can be expressed in terms of the $C^n(i)$, which leads to an expression for $|\mathcal{N}^{n,n}|$.

**Theorem 4.1** For $n > 1$,

$$|\mathcal{N}^{n,n}| = 2^n! + \sum_{i=1}^{n} (-1)^i \binom{n}{i} C^n(i) \cdot (2^{n-i}!)^{2^i}. \tag{13}$$

*proof.* We have that

$$|\mathcal{N}^{n,n}| = 2^n! - \left| \bigcup_{1 \leq i \leq n} C^n_i \right|. \tag{14}$$

Let $C^n_{i_1,i_2,\cdots i_k} = \bigcap_{i \in \{i_1,i_2,\cdots i_k\}} C^n_i$ where $i_1, i_2, \cdots i_k \in \{1, 2, \cdots, n\}$. By symmetry we have that $|C^n_{1,2,\cdots,k}| = |C^n_{i_1,i_2,\cdots,i_k}|$. Then from Theorem 2.1 we have that

$$|C^n_{1,2,\cdots,k}| = C^n(k) \cdot (2^{n-k}!)^{2^k}. \tag{15}$$

The theorem now follows using the inclusion-exclusion principle. □

It remains to calculate the coefficients $C^n(i)$. These coefficients can be calculated exactly [16], but the resulting expression is cumbersome. As we will show, the first term dominates the sum in eq. (14), and we will concentrate on estimating this term.

**Theorem 4.2** For $n > 1$, $1 \leq k \leq n$,

$$C^n(k) \leq |\mathcal{D}^n_{2^{n-1}}| \cdot \prod_{i=1}^{k-1} \left( |\mathcal{D}^{n-i}_{2^{n-i-1}}|^{2^i} + \sum_{j=1}^{i} (-1)^{j-1} \binom{i}{j} \binom{2^{i-j}}{2^{i-j-1}}^{2^{i-j}} \right). \tag{16}$$

*proof.* By induction on $k$.
*Basis.* Let $k = 1$. Then $C^n(1)$ is the number of balanced $n$-bit degenerate functions which is exactly $|\mathcal{D}^n_{2^{n-1}}|$, and thus the theorem is true when $k = 1$.
*Induction Hypothesis.* Assume that the theorem is true for $k$, $1 < k < n$.
*Inductive Step.* Let $F_k = [f_1, f_2, \cdots f_k]$ such that $f_i \in \mathcal{D}^n_{2^{n-1}}$, and $F$ is extendible. We wish to determine the number of number of $n$-bit degenerate functions $f$ such that $F_{k+1} = [f_1, f_2, \cdots f_k, f]$ is extendible.

Let $f$ depend on the variables $x_1, x_2, \cdots x_n$, and partition $V_f$ into $2^k$ blocks of size $2^{n-k}$. Denote these blocks as $V_{g_1}, V_{g_2}, \cdots V_{g_{2^{n-k}}}$, and let $G = \{g_1, g_2, \cdots g_{2^k}\}$.

We may consider each function $g_i$ as depending on a subset of the variables $x_1, x_2, \cdots x_n$, and w.l.o.g., let these variables be $x_1, x_2, \cdots x_{n-k}$. Now $f$ is degenerate in the variable $x_j \in \{x_1, x_2, \cdots x_{n-k}\}$ if and only if $g_i$ is degenerate in $x_j$, $\forall g_i \in G$. Then it follows that the number of functions $f$ that are degenerate in some variable from the set $\{x_1, x_2, \cdots x_{n-k}\}$ is less than $|\mathcal{D}^{n-k}_{2^{n-k-1}}|^{2^k}$.

The function $f$ will be degenerate in a variable from the set $\{x_{n-k+1}, x_{n-k+2}, \cdots x_n\}$ if $g_{i \oplus 2^j} = g_i$, for some $j$, $1 \leq j \leq k$. The number of $2^k$-tuples $G$ for which $g_{i \oplus 2^j} = g_i$ is given by

$$\sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j} \binom{2^{n-k}}{2^{n-k-1}}^{2^{k-j}}, \tag{17}$$

where we have used the inclusion-exclusion principle.

It follows $C^n(k+1)/C^n(k)$ gives the number of ways a degenerate function can be added to $F$ such that the resulting $(k+1)$-tuple is still extendible. Then using the induction hypothesis, we have that

$$C^n(k+1)/C^n(k) < |\mathcal{D}^{n-k}_{2^{n-k-1}}|^{2^k} + \sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j} \binom{2^{n-k}}{2^{n-k-1}}^{2^{k-j}}, \tag{18}$$

$$C^n(k+1) < |\mathcal{D}^n_{2^{n-1}}| \cdot \prod_{i=1}^{k} \left( |\mathcal{D}^{n-i}_{2^{n-i-1}}|^{2^i} + \sum_{j=1}^{i} (-1)^{j-1} \binom{i}{j} \binom{2^{n-k}}{2^{n-k-1}}^{2^{i-j}} \right). \tag{19}$$

Thus the induction hypothesis is true for $k+1$. □

**Corollary 4.1** For $k$, $1 < k \leq n$,

$$C^n(k) < n^{2^k-2} \cdot (2^{n-1}!) \cdot \binom{2^{n-1}}{2^{n-2}} \cdot (2^{n-k}!)^{2^{k-1}}. \tag{20}$$

*proof.* Using the estimates of $|\mathcal{D}_k^n|$ from Theorem 3.2, and the fact that the sum in eq. (17) is dominated by its first term, it follows that

$$C^n(k) \;<\; n\binom{2^{n-1}}{2^{n-2}} \cdot \prod_{i=1}^{k-1}(n-i)^{2^i} \cdot \left(\binom{2^{n-i-1}}{2^{n-i-2}}^{2^i} + i \cdot \binom{2^{n-i}}{2^{n-i-1}}^{2^{i-1}}\right) \tag{21}$$

Using Stirling's approximation it can be shown that $\binom{2^{n-i}}{2^{n-i-1}} > \binom{2^{n-i-1}}{2^{n-i-2}}^2$, and with the observation that $(n-i)^{2^i} + i < n^{2^i}$ for $n \geq 2, i \geq 1$, the estimate of $C^n(k)$ in eq. (21) can be simplified to

$$C^n(k) \;<\; n\binom{2^{n-1}}{2^{n-2}} \cdot \prod_{i=1}^{k-1} n^{2^i} \cdot \binom{2^{n-i}}{2^{n-i-1}}^{2^{i-1}}, \tag{22}$$

$$\;<\; n^{2^k-2} \cdot \binom{2^{n-1}}{2^{n-2}} \cdot (2^{n-1}!) \cdot \frac{2^{n-1}!}{(2^{n-k}!)^{2^{k-1}}}, \tag{23}$$

since

$$\prod_{i=1}^{k-1} n^{2^i} \cdot \binom{2^{n-i}}{2^{n-i-1}}^{2^{i-1}} \;=\; n^{2^k-2} \cdot \frac{2^{n-1}!}{(2^{n-k}!)^{2^{k-1}}}. \tag{24}$$

□

Using theses estimates of the $C^n(k)$ we can in turn estimate $|C_{1,\cdots k}|$, and thus give a lower bound on $|\mathcal{N}^{n,n}|$.

**Theorem 4.3**

$$|\mathcal{N}^{n,n}| \;=\; 2^n! - |C_1^n| \cdot (1 + o(1)). \tag{25}$$

*proof.* Using bounds for the factorial function [15], we have that for $2 \leq k \leq n$,

$$\frac{|C^n_{1,\cdots,k}|}{|C^n_1|} \;<\; \frac{n^{2^k-1} \cdot \binom{2^{n-1}}{2^{n-2}} (2^{n-k}!)^{2^{k-1}}}{(2^{n-1}!) \cdot (1 + o(1)) \cdot n \cdot \binom{2^{n-1}}{2^{n-2}}}, \tag{26}$$

$$\;=\; \frac{n^{2^k-2} \cdot (2^{n-k}!)^{2^{k-1}}}{(2^{n-1}!) \cdot (1 + o(1))}, \tag{27}$$

$$\;<\; \frac{(2^{\log n + n - k})^{2^k}}{\sqrt{2^n \pi} \cdot (2^{k-1})^{2^{n-1}}}, \tag{28}$$

$$\;<\; \frac{(2^{\log n - n + 2})^{2^{n-1}}}{(1 + o(1))}, \tag{29}$$

$$\;=\; o\Big((2^{\log n - n + 2})^{2^{n-1}}\Big). \tag{30}$$

Then from Theorem 4.1 we have that

$$|\mathcal{N}^{n,n}| = 2^n! + \sum_{i=1}^{n}(-1)^i \binom{n}{i} \cdot |C^n_{1,2,\cdots i}|, \tag{31}$$

$$= 2^n! - |C^n_1| \cdot \left[ \sum_{i=1}^{n}(-1)^i \binom{n}{i} \cdot \frac{C^n_{1,2,\cdots i}}{|C^n_1|} \right], \tag{32}$$

$$= 2^n! - |C^n_1|(1 + o(1)). \tag{33}$$

□

**Corollary 4.2**

$$\frac{|\mathcal{N}|}{2^n!} = 1 + o\left(\frac{\sqrt{2^n}}{2^{2^{n-1}+n-1}}\right). \tag{34}$$

*proof.* Using estimates of the factorial function we have that

$$\frac{|\mathcal{N}^{n,n}|}{2^n!} = 1 + \frac{|C^n_1|(1 + o(1))}{2^n!}, \tag{35}$$

$$= 1 + \frac{\binom{2^{n-1}}{2^{n-2}}(1 + o(1))}{2^n!}, \tag{36}$$

$$= 1 + o\left(\frac{\sqrt{2^n}}{2^{2^{n-1}+n-1}}\right). \tag{37}$$

□

# 5 Conclusion

Our main theorem states that nonlinearity and nondegeneracy are naturally occurring properties for permutations. The the denseness of nonlinear permutations is not unexpected given that the the set of nondegenerate permutations are dense (there are only two linear functions that are nondegenerate, viz. $f = x_1 \oplus x_2 \cdots x_n$, $\overline{f} = x_1 \oplus x_2 \cdots x_n \oplus 1$). These result provide strong evidence that DES is both nondegenerate and nonlinear, which has been justified previously through theoretical arguments [13], and empirical results [17]. The inclusion-exclusion principle provides a convenient form for asymptotic estimates. In the case of degenerate functions, the coefficients of the expansion are exponentially decreasing in magnitude, and the first coefficient of the expansion provides an asymptotic estimates of the sum itself. We may be able to apply similar techniques to decide whether or not most permutations are correlation immune, or satisfy the strict avalanche criterion.

Acknowledgements

The author would like to thank Prabhakar Ragde for his helpful comments in the preparation of this manuscript.

# References

[1] A. Adams and S. Tavares. The structured design of cryptographically good S-boxes. *Journal of Cryptology*, 3(1):27–41, 1990.

[2] F. Ayoub. Probabilistic completeness of substitution-permutation encryption networks. *IEE proceedings*, 129, part E(5):196–199, 1982.

[3] D. Chaum and J. H. Everste. Cryptanalysis of DES with a reduced number of rounds. *Advances in Cryptology, CRYPTO 85, H. C. Williams ed., Lecture Notes in Computer Science, vol. 218, Springer-Verlag*, pages 192–211, 1986.

[4] D. Coppersmith and E. Grossman. Generators for certain alternating groups with applications to cryptography. *SIAM Journal of Applied Mathematics*, 29(4):624–627, 1974.

[5] S. Even and O. Goldreich. DES-like functions can generate the alternating group. *IEEE Transactions on Information Theory*, IT-29(6):863–865, 1983.

[6] H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, 1973.

[7] H. Feistel, W. A. Notz, and J. Lynn Smith. Some cryptographic techniques for machine-to-machine data communications. *proceedings of the IEEE*, 63(11):1545–1554, 1975.

[8] J. Gordon and H. Retkin. Are big S-boxes best? In T. Beth, editor, *Cryptography, proceedings, Burg Feuerstein*, pages 257–262, 1982.

[9] M. A. Harrison. *Introduction to Switching and Automata Theory.* McGraw-Hill, Inc., 1965.

[10] S. T. Hu. *Mathematical Theory of Swithcing Circuits and Automata.* Berkeley, University of California Press, 1968.

[11] J. B. Kam and G. I. Davida. A structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*, 28(10):747–753, 1979.

[12] A. Konheim. *Cryptography: a primer.* Wiley, 1981.

[13] C. Meyer. Ciphertext/plaintext and ciphertext/key dependence vs. number of rounds for the data encryption standard. In *AFIPS Conference proceedings, 47*, pages 1119–1126, 1978.

[14] C. Mitchell. Enumerating boolean functions of cryptographic significance. *Journal of Cryptology*, 2(3):155–170, 1990.

[15] D. S. Mitrinovic. *Analytic Inequalities.* Springer–Verlag, 1970.

[16] L O'Connor. Enumerating nondegenerate permutations. Technical Report 2527, University of Waterloo, Waterloo, Ontario, Canada, 1991.

[17] W. L. Price and D. W. Davies. *Security for computer networks.* Wiley, 1984.

[18] R. A. Rueppel. *Design and Analysis of Stream Ciphers.* Springer–Verlag, 1986.