Correlations Between (Nonlinear) Combiners of Input and Output of Random Functions and Permutations

Subhabrata Samajder and Palash Sarkar
Applied Statistics Unit
Indian Statistical Institute
203, B.T.Road, Kolkata, India - 700108.
subhabrata.samajder@gmail.com, palash@isical.ac.in

December 15, 2017

Abstract

Daeman and Rijmen had derived the distributions of correlations between linear combinations of the input and output of uniform random functions and uniform random permutations. We generalise their results by deriving the distributions of correlations between arbitrary combinations of the input and the output of uniform random functions and uniform random permutations.
Keywords: correlation, uniform random function, uniform random permutation, block cipher.
Mathematics Subject Classification (2010): 94A60, 11T71, 68P25, 62P99.

1 Introduction

One of the basic tools for analysing symmetric key ciphers is a possible correlation between linear combinations of the input and output of a primitive. If this correlation is different from that of an idealised version of the primitive, then a distinguishing attack becomes possible. Determining whether a distinguishing attack is indeed possible requires the knowledge of the distribution of correlations for the idealised primitives. Two kinds of idealised primitives are usually considered, namely uniform random functions and uniform random permutations. For example, a uniform random permutation is an idealisation of a block cipher while a uniform random function is an idealisation of the state to keystream map in a stream cipher.

The distributions of the correlations between linear combinations of input and output for uniform random functions and uniform random permutations were derived in [4]. For the case of uniform random permutations, the distribution was earlier stated without proof in [6]. The distribution of correlation between linear combinations of input and output for uniform random permutation has proved to be useful in later work. This result formed the basis for an alternative formulation of the wrong key randomisation hypothesis in linear cryptanalysis [3] and has been followed up in later works [2, 1].

In this paper, we extend the results of [4] by considering correlation between arbitrary combiners of the input and output of uniform random functions and uniform random permutations. For any input combiner and any output combiner, the complete distribution of the correlation is derived. The result is more conveniently explained in terms of the weight of the XOR of the input and the output combiner. In the case of a uniform random function, if the output combiner is balanced, then we prove that this weight follows the binomial distribution; on the other hand, if the output combiner is not balanced, then we derive bounds on the probability that the weight deviates from its expected value. In the case of a uniform random permutation, we show that the distribution of the weights of the XOR of the input and output combiner can be expressed in terms of the hypergeometric distribution.

2 Preliminaries

For two binary strings α and β of the same length, $\alpha \oplus \beta$ will denote a binary string obtained by bitwise XOR of α and β.

An m-variable Boolean function f is a map $f : \{0,1\}^m \to \{0,1\}$. The support of f, denoted $\mathsf{supp}(f)$, is defined as follows.

$$\mathsf{supp}(f) = \{\alpha \in \{0,1\}^m : f(\alpha) = 1\}.$$

The weight $\mathsf{wt}(f)$ of f is defined to be the cardinality of the support of f, i.e.,

$$\mathsf{wt}(f) = \#\{\alpha \in \{0,1\}^m : f(\alpha) = 1\}.$$

The function f is said to be balanced if $\mathsf{wt}(f) = 2^{m-1}$.

The imbalance of f will be denoted as $\mathsf{Imb}(f)$ and is defined as follows.

$$\mathsf{Imb}(f) = \frac{1}{2}\left(\#\{\alpha \in \{0,1\}^m : f(\alpha) = 0\} - \#\{\alpha \in \{0,1\}^m : f(\alpha) = 1\}\right) = 2^{m-1} - \mathsf{wt}(f).$$

Let $f, g : \{0,1\}^m \to \{0,1\}$ be two Boolean functions. By $f \oplus g$ we denote the Boolean function $h : \{0,1\}^m \to \{0,1\}$ where $h(\alpha) = f(\alpha) \oplus g(\alpha)$ for all $\alpha \in \{0,1\}^m$. The correlation between f and g is denoted as $C(f,g)$ and is defined to be

$$C(f,g) = \frac{\mathsf{Imb}(f \oplus g)}{2^{m-1}}.$$

An (m,n) function S is a map $S : \{0,1\}^m \to \{0,1\}^n$. Let $\phi : \{0,1\}^m \to \{0,1\}$ and $\psi : \{0,1\}^n \to \{0,1\}$. Given S, ϕ and ψ, we define a Boolean function

$$f_S[\phi,\psi] : \{0,1\}^m \to \{0,1\}, \text{ where } f_S[\phi,\psi](\alpha) = \phi(\alpha) \oplus \psi(S(\alpha)). \tag{1}$$

The function ϕ is a combiner of the input of S while the function ψ is a combiner of the output of S. There are no restrictions on ϕ and ψ and in particular, they are not required to be linear combiners. Both $\phi(\cdot)$ and $\psi(S(\cdot))$ are m-variable Boolean functions. So, it is meaningful to talk about the correlation between these two functions. This correlation will be denoted as $C_S(\phi,\psi)$ and is equal to

$$C_S(\phi,\psi) \;=\; \frac{\mathsf{Imb}(f_S[\phi,\psi])}{2^{m-1}} = 1 - \frac{\mathsf{wt}(f_S[\phi,\psi])}{2^{m-1}}. \tag{2}$$

So, $C_S(\phi,\psi)$ measures the correlation between the combiner of the input as given by ϕ and the combiner of the output as given by ψ. From (2), determining $C_S(\phi,\psi)$ essentially boils down to determining $\mathsf{wt}(f_S[\phi,\psi])$.

3 Case of Uniform Random Function

Let S be a function picked uniformly at random from the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$. Such an S is a uniform random (m,n) function. An equivalent way to view S is the following. Let $\alpha_0, \ldots, \alpha_{2^m-1}$ be an enumeration of $\{0,1\}^m$. Let $X_i = S(\alpha_i)$, $i = 0, \ldots, 2^m - 1$. Then the random variables $X_0, \ldots, X_{2^m-1}$ are independent and uniformly distributed over $\{0,1\}^n$.

Proposition 1. *Let S be a uniform random (m,n) function. Let ϕ and ψ be m and n-variable Boolean functions respectively. Let $\alpha_0, \ldots, \alpha_{2^m-1}$ be an enumeration of $\{0,1\}^m$. For $0 \le i \le 2^m - 1$, define $W_i = f_S[\phi,\psi](\alpha_i)$. Then $W_i \sim \mathsf{Ber}(p_i)$, where*

$$p_i \;=\; \frac{\mathsf{wt}(\psi) + \phi(\alpha_i)(2^n - 2\mathsf{wt}(\psi))}{2^n}. \tag{3}$$

If ψ is a balanced Boolean function, then $W_i \sim \mathsf{Ber}(1/2)$.

Proof. Let $X_i = S(\alpha_i)$. Since S is a uniform random function, X_i is uniformly distributed over $\{0,1\}^n$. We have

$$W_i \quad = \quad f_S[\phi,\psi](\alpha_i) = \phi(\alpha_i) \oplus \psi(S(\alpha_i)) = \phi(\alpha_i) \oplus \psi(X_i).$$

Let $Y_i = \psi(X_i)$. Then Y_i is a binary valued random variable where Y_i takes the value 1 if and only if X_i lies in the support of ψ. Since X_i is uniformly distributed over $\{0,1\}^n$, the probability that X_i lies in the support of ψ is $\mathsf{wt}(\psi)/2^n$. So, $\Pr[Y_i = 1] = \mathsf{wt}(\psi)/2^n$ and $\Pr[Y_i = 0] = (2^n - \mathsf{wt}(\psi))/2^n$. So,

$$\begin{aligned}
\Pr[W_i = 1] &= \Pr[\phi(\alpha) \oplus \psi(X_i) = 1] \\
&= \Pr[Y_i = 1 \oplus \phi(\alpha_i)] \\
&= \frac{(1-\phi(\alpha_i))\mathsf{wt}(\psi) + \phi(\alpha_i)(2^n - \mathsf{wt}(\psi))}{2^n} \\
&= \frac{\mathsf{wt}(\psi) + \phi(\alpha_i)(2^n - 2\mathsf{wt}(\psi))}{2^n} \\
&= p_i.
\end{aligned}$$

This shows that W_i follows $\mathsf{Ber}(p_i)$. If ψ is a balanced Boolean function, then $\mathsf{wt}(\psi) = 2^{n-1}$ in which case $p_i = 1/2$ and so W_i follows $\mathsf{Ber}(1/2)$. □

We are interested in the weight of the function $f_S[\phi,\psi]$.

Proposition 2. *Let S be a uniform random (m,n) function. Let ϕ and ψ be m and n-variable Boolean functions respectively. Let $\alpha_0,\ldots,\alpha_{2^m-1}$ be an enumeration of $\{0,1\}^m$ and $W_i = f_S[\phi,\psi](\alpha_i)$. Let $W = \mathsf{wt}(f_S[\phi,\psi])$. Then $W = \sum_{i=0}^{2^m-1} W_i$.*

Proof. The following calculation shows the result.

$$W \quad = \quad \mathsf{wt}(f_S[\phi,\psi]) = \#\{\alpha_i : f_S[\phi,\psi](\alpha_i) = 1\} = \#\{i : W_i = 1\} = \sum_{i=0}^{2^m-1} W_i.$$

□

Theorem 1. *Let S be a uniform random (m,n) function. Let ϕ and ψ be m and n-variable Boolean functions respectively. If ψ is a balanced Boolean function, then $\mathsf{wt}(f_S[\phi,\psi]) \sim \mathsf{Bin}(2^m, 1/2)$.*

Proof. From Proposition 2, $\mathsf{wt}(f_S[\phi,\psi]) = W = \sum_{i=0}^{2^m-1} W_i$ where $W_i \sim \mathsf{Ber}(p_i)$ with p_i given by (3). If ψ is a balanced Boolean function, then $p_i = 1/2$ and $W_i \sim \mathsf{Ber}(1/2)$. Let $\alpha_0,\ldots,\alpha_{2^m-1}$ be an enumeration of $\{0,1\}^m$ and $X_i = S(\alpha_i)$ as in Proposition 1. Note

$$W_i \quad = \quad f_S[\phi,\psi](\alpha_i) = \phi(\alpha) \oplus \psi(X_i).$$

Since the random variables $X_0,\ldots,X_{2^m-1}$ are independent, so are the random variables $W_0,\ldots,W_{2^m-1}$. As a result, W is a sum of 2^m independent random variables each of which follows $\mathsf{Ber}(1/2)$. So, $W \sim \mathsf{Bin}(2^m, 1/2)$. □

The special case of Theorem 1 where ϕ and ψ are non-trivial linear functions was proved in [4].

In the case where ψ is not a balanced function, p_i takes either the value $\mathsf{wt}(\psi)/2^n$ or $(2^n - \mathsf{wt}(\psi))/2^n$ according as $\phi(\alpha_i)$ equals 0 or 1. So, the W_i's are not identically distributed and hence W does not follow the binomial distribution. In this case, $W_0,\ldots,W_{2^m-1}$ is a sequence of 2^m Poisson trials. It is possible to use the Chernoff bound to get an estimate of the probability that W stays close to the mean.

Theorem 2. *Let S be a uniform random (m,n) function. Let ϕ and ψ be m and n-variable Boolean functions respectively. Then the expected value of $\mathsf{wt}(f_S[\phi,\psi])$ is*

$$\mu = \frac{2^m\mathsf{wt}(\psi)+2^n\mathsf{wt}(\phi)-2\mathsf{wt}(\phi)\mathsf{wt}(\psi)}{2^n}. \tag{4}$$

Further, for any $0<\delta<1$

$$\Pr\left[|\mathsf{wt}(f_S[\phi,\psi])-\mu|\leq\delta\mu\right]\leq e^{-\mu\delta^2/2}. \tag{5}$$

Proof. Let W_i be as in Proposition 1 so that $\mathsf{wt}(f_S[\phi,\psi])=\sum_{i=0}^{2^m-1}W_i$. From Proposition 1, $W_i\sim\mathsf{Ber}(p_i)$ and so the expected value of W_i is p_i. By linearity of expectation, the expected value of $\mathsf{wt}(f_S[\phi,\psi])$ equals

$$\begin{aligned}\sum_{i=0}^{2^m-1}p_i &= \sum_{i=0}^{2^m-1}\frac{\mathsf{wt}(\psi)+\phi(\alpha_i)(2^n-2\mathsf{wt}(\psi))}{2^n}\\ &= \frac{2^m\mathsf{wt}(\psi)+\mathsf{wt}(\phi)(2^n-2\mathsf{wt}(\psi))}{2^n}\\ &= \frac{2^m\mathsf{wt}(\psi)+2^n\mathsf{wt}(\phi)-2\mathsf{wt}(\phi)\mathsf{wt}(\psi)}{2^n}.\end{aligned}$$

As in the proof of Theorem 1, $W_0,\ldots,W_{2^m-1}$ are independent and since $W_i\sim\mathsf{Ber}(p_i)$, these random variables form a sequence of Poisson trials. The Chernoff bound applies (see Section A) leading to (5). □

4 Case of Uniform Random Permutation

Let $m=n$ and we consider the set of all bijections from $\{0,1\}^n$ to itself, i.e., the set of all permutations of $\{0,1\}^n$. There are $2^n!$ such permutations.

Proposition 3. *Let S be a permutation of $\{0,1\}^n$; let ϕ and ψ be n-variable Boolean functions. Let x be an integer such that $0\leq x\leq\min(\mathsf{wt}(\phi),\mathsf{wt}(\psi))$. Then*

$$\#\{\alpha:\phi(\alpha)=1 \text{ and } \psi(S(\alpha))=1\}=x$$

if and only if

$$\mathsf{wt}(f_S[\phi,\psi])=\mathsf{wt}(\phi)+\mathsf{wt}(\psi)-2x.$$

Proof. Define

$$\begin{aligned}A_{0,0} &= \{\alpha:\phi(\alpha)=0,\psi(S(\alpha))=0\};\\ A_{0,1} &= \{\alpha:\phi(\alpha)=0,\psi(S(\alpha))=1\};\\ A_{1,0} &= \{\alpha:\phi(\alpha)=1,\psi(S(\alpha))=0\};\\ A_{1,1} &= \{\alpha:\phi(\alpha)=1,\psi(S(\alpha))=1\}.\end{aligned}$$

The sets $A_{0,0},A_{0,1},A_{1,0}$ and $A_{1,1}$ are mutually disjoint; $A_{0,0}\cup A_{0,1}=\{\alpha:\phi(\alpha)=0\}$; $A_{1,0}\cup A_{1,1}=\{\alpha:\phi(\alpha)=1\}$ and so

$$\begin{aligned}\#A_{0,0}+\#A_{0,1} &= 2^n-\mathsf{wt}(\phi),\\ \#A_{1,0}+\#A_{1,1} &= \mathsf{wt}(\phi).\end{aligned} \tag{6}$$

Further, $A_{0,0} \cup A_{1,0} = \{\alpha : \psi(S(\alpha)) = 0\}$. Since S is a permutation, $\{\alpha : \psi(S(\alpha)) = 0\} = \{\beta : \psi(\beta) = 0\}$. So, $A_{0,0} \cup A_{1,0} = \{\beta : \psi(\beta) = 0\}$ and similarly, $A_{0,1} \cup A_{1,1} = \{\beta : \psi(\beta) = 1\}$ leading to

$$\begin{array}{rcl} \#A_{0,0} + \#A_{1,0} & = & 2^n - \mathsf{wt}(\psi), \\ \#A_{0,1} + \#A_{1,1} & = & \mathsf{wt}(\psi). \end{array} \tag{7}$$

Equations (6) and (7) imply that $\#A_{1,1} = x$ if and only if $\#A_{0,1} + \#A_{1,0} = \mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x$.

Note that the support of $f_S[\phi, \psi]$ is $A_{0,1} \cup A_{1,0}$ and $A_{1,1} = \{\alpha : \phi(\alpha) = 1, \psi(S(\alpha)) = 1\}$. So, $\#\{\alpha : \phi(\alpha) = 1, \psi(S(\alpha)) = 1\} = x$ if and only if $\mathsf{wt}(f_S[\phi, \psi]) = \mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x$. □

From Proposition 3, given the functions ϕ and ψ, the possible weights that $f_S[\phi, \psi]$ can take for any permutation S of $\{0,1\}^n$ are the elements of the set

$$\{\mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x : 0 \leq x \leq \min(\mathsf{wt}(\phi), \mathsf{wt}(\psi))\}. \tag{8}$$

Suppose S is picked uniformly from the set of all permutations of $\{0,1\}^n$. We are interested in the probability that $f_S[\phi, \psi]$ takes a value from the set given by (8).

Theorem 3. *Let S be a permutation of $\{0,1\}^n$; let ϕ and ψ be n-variable Boolean functions. Then for $0 \leq x \leq \min(\mathsf{wt}(\phi), \mathsf{wt}(\psi))$,*

$$\Pr[\mathsf{wt}(f_S[\phi, \psi]) = \mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x] \quad = \quad \frac{\binom{\mathsf{wt}(\phi)}{x}\binom{2^n - \mathsf{wt}(\phi)}{\mathsf{wt}(\psi) - x}}{\binom{2^n}{\mathsf{wt}(\psi)}}. \tag{9}$$

If both ϕ and ψ are balanced functions, then

$$\Pr[\mathsf{wt}(f_S[\phi, \psi]) = \mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x] \quad = \quad \frac{\binom{2^{n-1}}{x}^2}{\binom{2^n}{2^{n-1}}}. \tag{10}$$

Proof. Let $\alpha_0, \ldots, \alpha_{2^n-1}$ be an enumeration of $\{0,1\}^n$ and let $X_i = S(\alpha_i)$. Unlike the case where S is a uniform random function, the random variables $X_0, \ldots, X_{2^n-1}$ are not independent. Instead, it is more convenient to view these random variables in the following manner. Consider an urn containing balls labelled $\alpha_0, \ldots, \alpha_{2^n-1}$. Balls are picked one by one from the urn *without replacement* and we number the trials from 0 to $2^n - 1$. Then the random variable X_i is the label of the ball picked in trial number i.

Consider the random Boolean function $g(\alpha) = \psi(S(\alpha))$. A Boolean function is defined by its support. So, it is sufficient to choose $\mathsf{wt}(\psi)$ balls from the urn and let the labels of these balls define the support of g. From Proposition 3, the probability that $\mathsf{wt}(f_S[\phi, \psi]) = \mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x$ is equal to the probability that the cardinality of the set

$$A_{1,1} = \{\alpha : \phi(\alpha) = 1 \text{ and } \psi(S(\alpha)) = 1\} = \{\alpha : \phi(\alpha) = 1 \text{ and } g(\alpha) = 1\}$$

is x.

To obtain this probability, we consider the following equivalent random experiment. Consider the urn as before containing balls labelled $\alpha_0, \ldots, \alpha_{2^n-1}$. Further, say that a ball labelled α_i is 'red' if $\phi(\alpha_i) = 1$ and otherwise it is 'black'. Now, consider that $\mathsf{wt}(\psi)$ balls are drawn from this urn which defines the support of g. The event that we are interested in is that x of these $\mathsf{wt}(\psi)$ are 'red' while the other $\mathsf{wt}(\psi) - x$ are 'black'. The probability of this event is the probability that $\#A_{1,1} = x$ which is given by the right hand side of (9). From Proposition 3, it follows that $\mathsf{wt}(f_S[\phi, \psi]) = \mathsf{wt}(\phi) + \mathsf{wt}(\psi) - 2x$ if and only if $\#A_{1,1} = x$. This shows (9).

In the case where both ϕ and ψ are balanced functions, both their weights are equal to 2^{n-1}. So, substituting 2^{n-1} for $\mathsf{wt}(\phi)$ and $\mathsf{wt}(\psi)$ in (9) and using $\binom{2^{n-1}}{2^{n-1}-x} = \binom{2^{n-1}}{x}$ yields (10). □

The expression given on the right hand side of (9) is the probability mass function of the hypergeometric distribution. In the special case where ϕ and ψ are non-trivial linear functions, the distribution given by (10) was proved in [4].

References

[1] Tomer Ashur, Tim Beyne, and Vincent Rijmen. Revisiting the wrong-key-randomization hypothesis. *IACR Cryptology ePrint Archive*, 2016:990, 2016.

[2] Céline Blondeau and Kaisa Nyberg. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. *Des. Codes Cryptography*, 82(1-2):319–349, 2017.

[3] Andrey Bogdanov and Elmar Tischhauser. On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2. In *Fast Software Encryption*, pages 19–38. Springer, 2014.

[4] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.

[5] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Chapman & Hall/CRC, 2010.

[6] Luke O'Connor. Properties of linear approximation tables. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 131–136. Springer, 1994.

A Chernoff Bounds

We briefly recall the Chernoff bound. This result can be found in standard texts [5].

Theorem 4. *Let $X_1, X_2, \ldots, X_\lambda$ be a sequence of independent Poisson trials such that for $1 \leq i \leq \lambda$, $\Pr[X_i = 1] = p_i$. Then for $X = \sum_{i=1}^{\lambda} X_i$ and $\mu = E[X] = \sum_{i=1}^{\lambda} p_i$ the following bounds hold:*

$$\text{For any } 0 < \delta \leq 1,\ \Pr[X \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}. \tag{11}$$

$$\text{For any } 0 < \delta < 1,\ \Pr[X \leq (1-\delta)\mu] \leq e^{-\mu\delta^2/2}. \tag{12}$$