



# Linking Stam's Bounds with Generalized Truncation

Bart Mennink<sup>(✉)</sup>

Digital Security Group, Radboud University, Nijmegen, The Netherlands  
b.mennink@cs.ru.nl

**Abstract.** One of the most prominent PRP-to-PRF designs is truncation, a method that found renewed interest with the GCM-SIV authenticated encryption scheme. A long line of research (from 1998 to 2018) shows that truncating an  $n$ -bit random permutation to  $m$  bits achieves tight  $n - m/2$  security. However, it appeared that the result was a direct consequence of a statistical result of Stam from 1978. In this work, we aim to gain better understanding in the possibilities and impossibilities of truncation. We take a closer look at the ancient result, observe that it is much more general, and link it with a generalized truncation function that uses an arbitrary post-processing function after the evaluation of the permutation. The main conclusion is that generalized truncation with any balanced post-processing achieves the same security bound as plain truncation. For unbalanced post-processing, security degrades gradually with the amount of unbalancedness. The results in particular exhibit a use of the Kullback-Leibler divergence for cryptographic indistinguishability proofs, without resorting to the recently popularized chi-squared method.

**Keywords:** Truncation · Generalization · PRF · Stam's bounds

## 1 Introduction

The dominant building block for symmetric cryptographic modes is a pseudorandom permutation (PRP), such as AES [22]. However, for many such modes, most notably stream-based (authenticated) ciphers [24, 28, 39] and message authentication codes [5, 11, 16, 49], security is determined by the level at which the underlying primitive behaves like a *random function* rather than a *random permutation*. Stated differently, these modes benefit from being instantiated with a pseudorandom function (PRF) instead of a PRP. Yet, with an extreme abundance in PRP candidates [1–4, 13, 14, 22] (to name a few), and only very few dedicated PRFs [10, 41], people have resorted to generic methods of transforming a PRP into a PRF.

The well-known PRP-PRF switch [7, 9, 17, 30, 31] shows that an  $n$ -bit PRP behaves as a PRF up to approximately  $2^{n/2}$  evaluations. This “birthday bound” could be inadequate for lightweight block ciphers, and various “beyond birthday bound” modes, schemes that achieve security beyond  $2^{n/2}$  evaluations,

have appeared. These include the xor of permutations [6, 8, 18, 23, 38, 42, 44–46], EDM [19, 23, 40], EDMD [40], and truncation [6, 12, 25–27, 30, 47]. We refer to Mennink and Neves [40, 41] for an extensive discussion of the four variants. In this work, we focus on truncation.

### 1.1 History of Truncation

Let  $n, m \in \mathbb{N}$  be such that  $m \leq n$ , and let  $p$  be an  $n$ -bit PRP. Truncation is defined as simply returning the  $m$  leftmost bits of  $p$ :

$$\text{Trunc}^p(x) = \text{left}_m(p(x)). \quad (1)$$

Hall et al. [30], introduced the truncation construction, and demonstrated security up to around  $2^{n-m/2}$  evaluations, but not for the entire parameter spectrum. Bellare and Impagliazzo [6] gave an improved analysis that demonstrates security for a broader selection of  $n$  and  $m$ . Gilboa and Gueron [25] resolved the remaining gaps by proving security up to  $2^{n-m/2}$  evaluations for any choice of  $n$  and  $m$ . It turned out, however, that the problem was already solved in 1978 by Stam [47], and that Stam’s bound is stronger than the bounds of [6, 25, 30] altogether. Bhattacharya and Nandi [12] transformed Stam’s analysis to the chi-squared method [23], deriving an identical bound. We elaborate on this upper bound in Sect. 4.1. Gilboa et al. [27] presented a detailed comparison of the bounds of Hall et al. [30], Bellare and Impagliazzo [6], Gilboa and Gueron [25], and Stam [47].

With respect to insecurity, Hall et al. [30] also argued tightness of their bound by sketching a distinguisher. Gilboa and Gueron [26] presented a formal derivation of a lower bound, for various choices of  $n, m$ , and the number of evaluations. They showed that the best distinguisher’s success probability is close to 1 for around  $2^{n-m/2}$  evaluations. See Sect. 4.1 for the lower bound.

The truncated permutation construction found application as key derivation function in GCM-SIV [28, 29, 37], although its use is disputed [15, 32].

### 1.2 Stam’s Bounds

Stam’s 1978 bound [47] is more general than suggested in Sect. 1.1. Intuitively (a formal treatment of Stam’s bounds is given in Sect. 3), it covers the idea of  $2^n$  possible outcomes being grouped into  $2^m$  colors (the number of occurrences per color not necessarily equal) and measures the distance between sampling with or without replacement, where the observer learns the color of every sample. In a later publication in 1986, Stam [48] generalized this result to the case where the number of colors and the grouping of the outcomes into the colors differs per sample.

The analysis of Stam is based on the Kullback-Leibler divergence  $KL(X; Y)$  [36] (see Sect. 2.1 for the details), and Pinsker’s inequality [21, 34, 35] stating that

$$\Delta(X, Y) \leq \left( \frac{1}{2} KL(X; Y) \right)^{1/2}, \quad (2)$$

where  $\Delta(X, Y)$  denotes the statistical distance between  $X$  and  $Y$ . The exact same statistical tools were used in the chi-squared method of Dai et al. [23]. However, Dai et al. make an additional step, namely that the Kullback-Leibler divergence  $KL(X; Y)$  is at most the chi-squared divergence  $\chi^2(X; Y)$  (see, again, Sect. 2.1 for the details). In this work, we rely on Stam's results and perform analysis at the level of the Kullback-Leibler divergence.

### 1.3 Generalized Truncation

The goal of this work is to fully understand the implication of Stam's bounds to truncation. To do so, we describe a generalized truncation function  $\text{GTrunc}$  in Sect. 4. The function generalizes simple truncation by the evaluation of a post-processing function  $\text{post} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^m$  after permutation:

$$\text{GTrunc}^p(x) = \text{post}(x, p(x)). \quad (3)$$

The function is depicted in Fig. 1. It covers plain truncation of (1) by taking the post-processing function that ignores its first input and evaluates  $\text{left}_m$  on its second input.

However,  $\text{GTrunc}$  is much more general than  $\text{Trunc}$ . Most importantly, it feed-forwards its input  $x$  to the post-processing function  $\text{post}$ . This, on the one hand, gives an adversary more power, but on the other hand, frustrates statistical analysis as the output function is not purely a post-processing function on the output of the permutation  $p$ . We consider the security of  $\text{GTrunc}$  for various types of post-processing functions. In Sect. 4.2 we consider a simplified variant where  $\text{post}$  is balanced and no feed-forward is involved, and show security-wise equivalence of the resulting construction with  $\text{Trunc}$ . In Sect. 4.3 we consider the general  $\text{GTrunc}$  construction with balanced post-processing and link it with the bounds of Stam [47, 48]. The result shows that, in fact,  $\text{GTrunc}$  achieves the same level of security as  $\text{Trunc}$ , regardless of the choice of post-processing function  $\text{post}$  (as long as it is balanced). Finally, we extend the result to arbitrary (possibly unbalanced)  $\text{post}$ , and derive a security bound that is slightly worse, depending on the unbalancedness of  $\text{post}$ . The derivation is based on Stam's bounds, with in addition an analysis of the statistical distance between unbalanced and balanced random samplings with replacement using the Kullback-Leibler divergence.

We comment on the affect of including a pre-processing function  $\text{pre}$  in Sect. 5.

## 2 Security Model

Consider two natural numbers  $n, m \in \mathbb{N}$ . We denote by  $\{0, 1\}^n$  the set of  $n$ -bit strings. The set  $\text{func}(n, m)$  denotes the set of all  $n$ -to- $m$ -bit functions, and  $\text{perm}(n)$  the set of all  $n$ -bit permutations. If  $m \leq n$ , the function  $\text{left}_m : \{0, 1\}^n \rightarrow \{0, 1\}^m$  returns the left  $m$  bits of its input. We denote by  $(m)_n$  the falling factorial  $m(m-1) \cdots (m-n+1) = m!/(m-n)!$ . For a finite set  $\mathcal{X}$ ,  $x \stackrel{\$}{\leftarrow} \mathcal{X}$  denotes the uniform random drawing of  $x$  from  $\mathcal{X}$ .

## 2.1 Statistical Tools

For two distributions  $X, Y$  over a finite space  $\Omega$ , the statistical distance between  $X$  and  $Y$  is defined as

$$\Delta(X, Y) = \frac{1}{2} \sum_{\omega \in \Omega} |\Pr(X = \omega) - \Pr(Y = \omega)| \quad (4)$$

$$= \max_{\Omega^* \subseteq \Omega} \left\{ \sum_{\omega \in \Omega^*} \Pr(X = \omega) - \Pr(Y = \omega) \right\}. \quad (5)$$

The Kullback-Leibler divergence [36] between  $X$  and  $Y$  is defined as

$$KL(X; Y) = \sum_{\omega \in \Omega} \Pr(X = \omega) \log \left( \frac{\Pr(X = \omega)}{\Pr(Y = \omega)} \right), \quad (6)$$

with the condition that  $\Pr(Y = \omega) > 0$  for all  $\omega \in \Omega$  and the convention that  $0 \log(0) = 0$ . Pinsker's inequality [21, 34, 35] gives

$$\Delta(X, Y) \leq \left( \frac{1}{2} KL(X; Y) \right)^{1/2}. \quad (7)$$

*Remark 1.* Dai et al. [23] recently introduced the chi-squared method to cryptography. The chi-squared method also relies on Pinsker's inequality (7), but *in addition* uses that

$$KL(X; Y) \leq \chi^2(X; Y), \quad (8)$$

where

$$\chi^2(X; Y) = \sum_{\omega \in \Omega} \frac{(\Pr(X = \omega) - \Pr(Y = \omega))^2}{\Pr(Y = \omega)} \quad (9)$$

is the chi-squared divergence [20, 43]. What then remains in order to bound  $\Delta(X, Y)$  is an analysis of the chi-squared divergence between  $X$  and  $Y$ . In our work, we do not go that far, but instead, stop at the Kullback-Leibler divergence. (This is no critique on the chi-squared method; in many applications, bounding  $\chi^2(X; Y)$  may be easier to do than bounding  $KL(X; Y)$ ).

## 2.2 Pseudorandom Functions

A distinguisher  $\mathcal{D}$  is an algorithm that is given access to an oracle  $\mathcal{O}$ ; it can make a certain amount of queries to this oracle, and afterwards it outputs  $b \in \{0, 1\}$ . We focus on computationally unbounded distinguishers, whose complexities are measured by the number of oracle queries only. As usual, a scheme is secure if it withstands the strongest possible distinguisher, and we can without loss of generality restrict our focus to deterministic distinguishers. The reason for this is

that for any probabilistic distinguisher there exists a deterministic distinguisher with the same success probability.

Let  $n, m \in \mathbb{N}$  such that  $m \leq n$ . Let  $p \in \text{perm}(n)$ , and consider a function  $F^p \in \text{func}(n, m)$ . We define the pseudorandom function (PRF) security of  $F^p$  as a random function against a distinguisher  $\mathcal{D}$  by

$$\text{Adv}_F^{\text{prf}}(\mathcal{D}) = \left| \Pr(\mathcal{D}^{F^p} = 1) - \Pr(\mathcal{D}^f = 1) \right|, \quad (10)$$

where the first probability is taken over the random drawing of  $p \xleftarrow{\$} \text{perm}(n)$  and the second probability over  $f \xleftarrow{\$} \text{func}(n, m)$ . (Recall that  $\mathcal{D}$  is a deterministic distinguisher).

The definition of PRF security relates to the statistical distance of (4–5) in the following manner. Let  $q \in \mathbb{N}$ , and consider a deterministic distinguisher  $\mathcal{D}$  making  $q$  queries. Let  $X$  denote the probability distribution of interactions with  $F^p$  and  $Y$  the probability distribution of interactions with  $f$ . Let  $\Omega_1$  denote the set of query-response tuples for which distinguisher  $\mathcal{D}$  outputs 1. Then,

$$\text{Adv}_F^{\text{prf}}(\mathcal{D}) = \left| \sum_{\omega \in \Omega_1} \Pr(X = \omega) - \Pr(Y = \omega) \right| \leq \Delta(X, Y). \quad (11)$$

Equality is achieved for distinguisher  $\mathcal{D}$  that returns 1 for any query-response tuple in  $\Omega^*$ , where  $\Omega^*$  is the set for which (5) achieves its maximum [12].

*Remark 2.* The above security model considers  $F^p$  to be “keyed” with a random permutation  $p \xleftarrow{\$} \text{perm}(n)$ . A standard hybrid argument allows us to transform all results in this work to a complexity-theoretic setting where  $p$  is, instead, a block cipher  $E$  with secret key  $K$ , and the distinguisher’s capabilities are also bounded by a time parameter  $t$ .

### 3 Stam's Bounds

Consider a finite set of  $N$  elements, of  $M$  types/colors. Denote the partition of the  $N$  elements into the  $M$  colors by  $A_1 \cup \dots \cup A_M$ . For color  $j$ , write  $a_j = |A_j| > 0$ , such that

$$a_1 + \dots + a_M = N. \quad (12)$$

Let  $q \in \mathbb{N}$ . Denote by  $X$  the probability distribution of the obtained colors when sampling  $q$  elements *without* replacement, and by  $Y$  the probability distribution of the obtained colors when sampling *with* replacement. Both  $X$  and  $Y$  have range  $\{1, \dots, M\}^q$ . Stam [47] measures the distance between  $X$  and  $Y$ , and proves the following bound<sup>1</sup>.

<sup>1</sup> Note that our definition of distance has a factor  $\frac{1}{2}$  compared to that of Stam.

**Theorem 1 (Stam’s bound [47, Theorems 2.2 and 2.3]).** *Let  $q, N, M \in \mathbb{N}$  such that  $M \leq N$ , and consider the configuration of  $M$  colors of color sizes  $(a_1, \dots, a_M)$  as in (12). Consider the two distributions  $X$  and  $Y$  over range  $\{1, \dots, M\}^q$ . We have,*

$$\Delta(X, Y) \leq \frac{1}{2} \left( \frac{(M-1)q(q-1)}{(N-1)(N-q+1)} \right)^{1/2}. \tag{13}$$

*Proof.* We include Stam’s proof (in our terminology) for completeness.

Write  $X = (X_1, \dots, X_q)$  and  $Y = (Y_1, \dots, Y_q)$ . Denote, for brevity,  $\mathbf{X}_i = (X_1, \dots, X_i)$  and  $\mathbf{Y}_i = (Y_1, \dots, Y_i)$  for  $i = 1, \dots, q$ . The Kullback-Leibler divergence (6) can be rewritten as

$$KL(X; Y) \leq KL(X_1; Y_1) + \sum_{i=1}^{q-1} KL(X_{i+1}; Y_{i+1} \mid \mathbf{X}_i, \mathbf{Y}_i), \tag{14}$$

where

$$KL(X_{i+1}; Y_{i+1} \mid \mathbf{X}_i, \mathbf{Y}_i) = \sum_{\mathbf{j}_i \in \{1, \dots, M\}^i} \Pr(\mathbf{X}_i = \mathbf{j}_i) \cdot \sum_{j=1}^M \Pr(X_{i+1} = j \mid \mathbf{X}_i = \mathbf{j}_i) \log \left( \frac{\Pr(X_{i+1} = j \mid \mathbf{X}_i = \mathbf{j}_i)}{\Pr(Y_{i+1} = j \mid \mathbf{Y}_i = \mathbf{j}_i)} \right). \tag{15}$$

We have

$$\Pr(X_{i+1} = j \mid \mathbf{X}_i = \mathbf{j}_i) = \frac{a_j - h}{N - i}, \tag{16}$$

$$\Pr(Y_{i+1} = j \mid \mathbf{Y}_i = \mathbf{j}_i) = \frac{a_j}{N}, \tag{17}$$

where  $h$  denotes the number of occurrences of  $j$  in sample  $\mathbf{j}_i$ . Thus,

$$KL(X_{i+1}; Y_{i+1} \mid \mathbf{X}_i, \mathbf{Y}_i) \tag{18}$$

$$= \sum_{j=1}^M \sum_{\mathbf{j}_i \in \{1, \dots, M\}^i} \Pr(\mathbf{X}_i = \mathbf{j}_i) \cdot \frac{a_j - h}{N - i} \cdot \log \left( \frac{\frac{a_j - h}{N - i}}{\frac{a_j}{N}} \right) \tag{19}$$

$$= \sum_{j=1}^M \sum_{h=0}^{\min\{i, a_j - 1\}} \Pr(HG_{a_j}^N(i) = h) \cdot \frac{a_j - h}{N - i} \cdot \log \left( \frac{\frac{a_j - h}{N - i}}{\frac{a_j}{N}} \right), \tag{20}$$

where  $HG_{a_j}^N(i)$  is a random variable of  $i$  hypergeometrically distributed draws from  $N$  elements with  $a_j$  success elements. We have

$$\Pr(HG_{a_j}^N(i) = h) \cdot \frac{a_j - h}{N - i} = \binom{i}{h} \frac{(a_j)_h (N - a_j)_{i-h}}{(N)_i} \cdot \frac{a_j - h}{N - i} \tag{21}$$

$$= \binom{i}{h} \frac{(a_j - 1)_h (N - a_j)_{i-h}}{(N - 1)_i} \cdot \frac{a_j}{N} \tag{22}$$

$$= \Pr(HG_{a_j - 1}^{N-1}(i) = h) \cdot \frac{a_j}{N}. \tag{23}$$

Note furthermore that

$$\sum_{h=0}^{\min\{i, a_j-1\}} h \cdot \Pr\left(HG_{a_j-1}^{N-1}(i) = h\right) = \mathbf{Ex}\left(HG_{a_j-1}^{N-1}(i)\right) = \frac{i(a_j-1)}{N-1}. \tag{24}$$

We subsequently derive the following for (20), where in the first bounding we use Jensen's inequality (log is concave) and in the second bounding we use that  $\log(\alpha) \leq \alpha - 1$  (for any  $\alpha > 0$ ):

$$KL(X_{i+1}; Y_{i+1} \mid \mathbf{X}_i, \mathbf{Y}_i) \tag{25}$$

$$= \sum_{j=1}^M \frac{a_j}{N} \cdot \sum_{h=0}^{\min\{i, a_j-1\}} \Pr\left(HG_{a_j-1}^{N-1}(i) = h\right) \cdot \log\left(\frac{\frac{a_j-h}{N-i}}{\frac{a_j}{N}}\right) \tag{26}$$

$$\leq \sum_{j=1}^M \frac{a_j}{N} \cdot \log\left(\sum_{h=0}^{\min\{i, a_j-1\}} \Pr\left(HG_{a_j-1}^{N-1}(i) = h\right) \cdot \frac{\frac{a_j-h}{N-i}}{\frac{a_j}{N}}\right) \tag{27}$$

$$= \sum_{j=1}^M \frac{a_j}{N} \cdot \log\left(\frac{N}{a_j(N-i)} \left(a_j - \mathbf{Ex}\left(HG_{a_j-1}^{N-1}(i)\right)\right)\right) \tag{28}$$

$$= \sum_{j=1}^M \frac{a_j}{N} \cdot \log\left(\frac{N}{a_j(N-i)} \left(a_j - \frac{i(a_j-1)}{N-1}\right)\right) \tag{29}$$

$$= \sum_{j=1}^M \frac{a_j}{N} \cdot \log\left(1 + \frac{(N-a_j)i}{a_j(N-1)(N-i)}\right) \tag{30}$$

$$\leq \sum_{j=1}^M \left(1 - \frac{a_j}{N}\right) \cdot \frac{i}{(N-1)(N-i)} \tag{31}$$

$$= \frac{(M-1)i}{(N-1)(N-i)}. \tag{32}$$

The theorem is concluded by combining (7), (14), and (32). □

It is interesting to note that the bound depends on  $q$ ,  $N$ , and  $M$ , *but not on the  $a_i$ 's*. This is caused by the observation that the outcomes are hypergeometrically distributed and that the  $a_j$ 's drop out due to concavity of the function log.

This fact allowed Stam to generalize his result to partitions varying with  $i = 1, \dots, q$  at little effort [48]. More formally, consider a finite set of  $N$  elements, this time with  $q$  partitions into  $M_i$  types/colors  $A_{i,1} \cup \dots \cup A_{i,M_i}$  for  $i = 1, \dots, q$ . For color  $j$  in sample  $i$ , write  $a_{i,j} = |A_{i,j}| > 0$ , such that for all  $i = 1, \dots, q$ ,

$$a_{i,1} + \dots + a_{i,M_i} = N. \tag{33}$$

Let  $q \in \mathbb{N}$ . Denote by  $X$  the probability distribution of the obtained colors when sampling  $q$  elements *without* replacement, and by  $Y$  the probability distribution

of the obtained colors when sampling *with* replacement. Both  $X$  and  $Y$  have range

$$\{1, \dots, M_1\} \times \dots \times \{1, \dots, M_q\}. \tag{34}$$

Stam [48] proves the following bound for the distance between  $X$  and  $Y$ .

**Theorem 2 (Stam’s bound [48, Theorem 1]).** *Let  $q, N, M_1, \dots, M_q \in \mathbb{N}$  such that  $M_1, \dots, M_q \leq N$ , and consider the configuration of  $M_i$  colors of color sizes  $\{(a_{i,1}, \dots, a_{i,M_i})\}$  for  $i = 1, \dots, q$  as in (33). Consider the two distributions  $X$  and  $Y$  over range  $\{1, \dots, M_1\} \times \dots \times \{1, \dots, M_q\}$ . We have,*

$$\Delta(X, Y) \leq \frac{1}{2} \left( \sum_{i=1}^{q-1} \frac{2(M_{i+1} - 1)i}{(N - 1)(N - q + 1)} \right)^{1/2}. \tag{35}$$

*Proof.* The proof is a straightforward extension of that of Theorem 1: the only differences are that the indices in the summations and summands of (15) are updated to the new range  $\{1, \dots, M_1\} \times \dots \times \{1, \dots, M_q\}$  and color sizes  $a_{i+1,j}$ . In particular, for fixed  $i \in \{1, \dots, q\}$ , (31–32) is superseded by

$$KL(X_{i+1}; Y_{i+1} \mid \mathbf{X}_i, \mathbf{Y}_i) \leq \sum_{j=1}^{M_{i+1}} \left( 1 - \frac{a_{i+1,j}}{N} \right) \frac{i}{(N - 1)(N - i)} \tag{36}$$

$$= \frac{(M_{i+1} - 1)i}{(N - 1)(N - i)}. \tag{37}$$

The result then immediately follows. □

If  $M_1 = \dots = M_q = M$  (but not necessarily with identical color sizes  $\{(a_{i,1}, \dots, a_{i,M})\}$  for every sampling), the bound of Theorem 2 obviously simplifies to that of Theorem 1.

## 4 Generalized Truncation

We consider a generalization of Trunc of (1) to arbitrary post-processing function. As before, let  $n, m \in \mathbb{N}$  such that  $m \leq n$ , and  $p \in \text{perm}(n)$ . Let  $\text{post} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^m$  be an arbitrary post-processing function. Generalized truncation is defined as

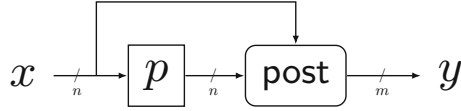
$$\text{GTrunc}^p(x) = \text{post}(x, p(x)). \tag{38}$$

Generalized truncation is depicted in Fig. 1. For fixed  $x \in \{0, 1\}^n$  and  $y \in \{0, 1\}^m$ , we define

$$\text{post}[x]^{-1}(y) = \{z \in \{0, 1\}^n \mid \text{post}(x, z) = y\}. \tag{39}$$

The differences between GTrunc and Trunc are subtle but quite significant, depending on the choice of post.





**Fig. 1.** GTrunc of (38) based on  $n$ -bit permutation  $p \in \text{perm}(n)$ .  $\text{post}$  is any function.

- The generalized description covers Trunc of (1) by setting  $\text{post}(x, z) = \text{left}_m(z)$ . In Sect. 4.1, we revisit the state of the art on Trunc and re-derive the best security bound;
- In Sect. 4.2, we consider GTrunc with *balanced and  $x$ -independent post-processing*, i.e., where the feed-forward of  $x$  is discarded, and demonstrate that its security is equivalent to the security of Trunc;
- In Sect. 4.3, we consider GTrunc with *balanced post-processing* (not necessarily discarding the feed-forward). In this case a direct reduction to Trunc seems impossible but we resort to Stam's generalized bound of Theorem 2;
- In Sect. 4.4, we consider GTrunc with *arbitrary post-processing*. Also in this case, we resort to Theorem 2, but additional analysis is needed to make the result carry over.

We elaborate on using a pre-processing function in Sect. 5.

#### 4.1 Plain Truncation

We consider the case of plain truncation: Trunc of (1), or equivalently GTrunc of (38) with  $\text{post}(x, z) = \text{left}_m(z)$ .

Truncation first appeared in Hall et al. [30]. It is known to be secure up to approximately  $2^{n-m/2}$  queries [6, 12, 25, 30, 47]. We describe the bound as a direct implication of Stam's bound of Theorem 1. For educational interest, Bhattacharya and Nandi [12] gave a self-contained proof of this result in the chi-squared method: they derived the exact same bound, which should not come as surprise in light of Remark 1 in Sect. 2.1.

**Theorem 3 (Security of Trunc).** *Let  $q, n, m \in \mathbb{N}$  such that  $m \leq n$ . Consider GTrunc of (38) with  $\text{post}(x, z) = \text{left}_m(z)$ . For any distinguisher  $\mathcal{D}$  making at most  $q$  queries,*

$$\text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}) \leq \frac{1}{2} \left( \frac{(2^m - 1)q(q - 1)}{(2^n - 1)(2^n - q + 1)} \right)^{1/2}. \quad (40)$$

*Proof.* Fix a deterministic distinguisher  $\mathcal{D}$  that makes  $q$  queries. Let  $X^{\text{Trunc}^p}$  denote the probability distribution of interactions with  $\text{Trunc}^p$  for  $p \xleftarrow{\$} \text{perm}(n)$ , and  $Y^f$  the probability distribution of interaction with  $f \xleftarrow{\$} \text{func}(n, m)$ . By (11),

$$\text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}) \leq \Delta(X^{\text{Trunc}^p}, Y^f). \quad (41)$$

Put  $N = 2^n$ ,  $M = 2^m$ , and define the  $M$  colors by the first  $m$  bits of the sampling, i.e., two elements  $z, z' \in \{0, 1\}^n$  have the same color if  $\text{left}_m(z) = \text{left}_m(z')$ . Consider the samplings  $X$  and  $Y$  of Sect. 3. Clearly,  $\Delta(X, X^{\text{Trunc}^p}) = 0$ : in  $X^{\text{Trunc}^p}$  one samples without replacement and only reveals the first  $m$  bits of the drawing, which is equivalent to revealing the color. As all color sets are of equal size  $a_1 = \dots = a_{2^m} = 2^{n-m}$ , we also have  $\Delta(Y^f, Y) = 0$ . Thus, by the triangle inequality,

$$\text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}) \leq \Delta(X^{\text{Trunc}^p}, Y^f) = \Delta(X, Y). \tag{42}$$

The result now immediately follows from Theorem 1. □

A simple simplification simplifies the bound of Theorem 3 to  $\left(\binom{q}{2}/2^{2n-m}\right)^{1/2}$ . The bound is known to be tight: Hall et al. [30] already presented a distinguisher  $\mathcal{D}$  meeting this bound up to a constant, but their distinguisher did not come with an exact analysis. Gilboa and Gueron presented a more detailed attack [26], and we repeat a simplification of their bound.

**Theorem 4 (Insecurity of Trunc [26, Proposition 2, simplified]).** *Let  $n, m \in \mathbb{N}$  such that  $m \leq n$ . Consider  $\text{GTrunc}$  of (38) with  $\text{post}(x, z) = \text{left}_m(z)$ . There exists a distinguisher  $\mathcal{D}$  making  $q = 2^{n-m/2-3}$  queries, such that*

$$\text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}) \geq \frac{1}{400} \left(1 - e^{-1/306}\right). \tag{43}$$

## 4.2 Balanced and $x$ -Independent Post-processing

We consider security of  $\text{GTrunc}$  in a limited setting where  $\text{post}$  is independent of its first input  $x$  ( $\text{post}(\cdot, z)$  is constant for all  $z$ ) and where it is balanced (the set  $\text{post}[x]^{-1}(y)$  is of the same size for all  $x, y$ ). Already in the original introduction, Hall et al. [30] remarked that the analysis of  $\text{Trunc}$  carries over to balanced post-processing functions, and it also follows immediately from Theorem 1 (with different color sets, but still all of equal size  $2^{n-m}$  as the function is balanced). As a bonus, we present an analysis of this case that reduces the security of  $\text{GTrunc}$  with balanced and  $x$ -independent  $\text{post}$  to  $\text{Trunc}$ .

**Theorem 5 (Security of  $\text{GTrunc}$  with balanced and  $x$ -independent  $\text{post}$ ).** *Let  $q, n, m \in \mathbb{N}$  such that  $m \leq n$ . Consider  $\text{GTrunc}$  of (38) with balanced and  $x$ -independent  $\text{post}$ . For any distinguisher  $\mathcal{D}$ ,*

$$\text{Adv}_{\text{GTrunc}}^{\text{prf}}(\mathcal{D}) = \text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}). \tag{44}$$

*Proof.* Without loss of generality, consider  $\text{post} : \{0, 1\}^n \rightarrow \{0, 1\}^m$  and write  $\text{GTrunc}^p$  as

$$\text{GTrunc}^p(x) = \text{post} \circ p(x). \tag{45}$$

As  $\text{post}$  is balanced, there exists a balanced function  $\text{post}' : \{0, 1\}^n \rightarrow \{0, 1\}^n$  such that

$$\text{post} = \text{left}_m \circ \text{post}'. \quad (46)$$

Let  $p \stackrel{\$}{\leftarrow} \text{perm}(n)$ , and consider any distinguisher  $\mathcal{D}$  whose goal it is to distinguish  $\text{GTrunc}^p$  from  $f \stackrel{\$}{\leftarrow} \text{func}(n, m)$ . Defining  $p' = \text{post}' \circ p$ , we obtain that

$$\text{GTrunc}^p = \text{post} \circ p = \text{left}_m \circ \text{post}' \circ p = \text{left}_m \circ p' = \text{Trunc}^{p'}, \quad (47)$$

and thus that

$$\text{Adv}_{\text{GTrunc}}^{\text{prf}}(\mathcal{D}) = \text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}), \quad (48)$$

as  $p' \stackrel{\$}{\leftarrow} \text{perm}(n)$  iff  $p \stackrel{\$}{\leftarrow} \text{perm}(n)$  (because  $\text{post}'$  is  $n$ -to- $n$  and balanced).  $\square$

### 4.3 Balanced Post-processing

We consider security of  $\text{GTrunc}$  in a more general setting:  $\text{post}$  is any *balanced* function. We consider this to be the most interesting configuration, as for unbalanced post-processing, security decreases (see Sect. 4.4).

**Theorem 6 (Security of  $\text{GTrunc}$  with balanced post).** *Let  $q, n, m \in \mathbb{N}$  such that  $m \leq n$ . Consider  $\text{GTrunc}$  of (38) with balanced  $\text{post}$ . For any distinguisher  $\mathcal{D}$  making at most  $q$  queries,*

$$\text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}) \leq \frac{1}{2} \left( \frac{(2^m - 1)q(q - 1)}{(2^n - 1)(2^n - q + 1)} \right)^{1/2}. \quad (49)$$

*Proof.* Fix a deterministic distinguisher  $\mathcal{D}$  that makes  $q$  queries. Let  $X^{\text{GTrunc}^p}$  denote the probability distribution of interactions with  $\text{GTrunc}^p$  for  $p \stackrel{\$}{\leftarrow} \text{perm}(n)$ , and  $Y^f$  the probability distribution of interaction with  $f \stackrel{\$}{\leftarrow} \text{func}(n, m)$ . By (11),

$$\text{Adv}_{\text{GTrunc}}^{\text{prf}}(\mathcal{D}) \leq \Delta(X^{\text{GTrunc}^p}, Y^f). \quad (50)$$

Put  $N = 2^n$ ,  $M = 2^m$ . For ease of reasoning, assume (for now) that the distinguisher makes queries  $x_1, \dots, x_q$ . For each query  $x_i$  ( $i = 1, \dots, q$ ), define the  $M$  colors by the sets  $A_{i,j} := \text{post}^{-1}[x_i](j)$  for  $j \in \{0, 1\}^m$ . The  $q$  queries thus define  $q$  partitions of the  $N$  elements into  $M$  colors  $A_{i,1} \cup \dots \cup A_{i,M}$  for  $i = 1, \dots, q$ . Consider the samplings  $X$  and  $Y$  of Sect. 3. Clearly,  $\Delta(X, X^{\text{GTrunc}^p}) = 0$  as in the proof of Theorem 3. As  $\text{post}$  is balanced, all color sets are of equal size  $a_{i,1} = \dots = a_{i,M} = 2^{n-m}$  for  $i = 1, \dots, q$ . We therefore also have  $\Delta(Y^f, Y) = 0$ . Thus, by the triangle inequality,

$$\text{Adv}_{\text{GTrunc}}^{\text{prf}}(\mathcal{D}) \leq \Delta(X, Y). \quad (51)$$

We obtain our bound on the remaining distance from Theorem 2. As this bound holds for any possible distinguisher, and any possible selection of

inputs  $x_1, \dots, x_q$ , we can maximize over all possible deterministic distinguishers. (Formally, the analysis of Theorem 2 consists of a *per-query* analysis of  $KL(X_{i+1}; Y_{i+1} \mid \mathbf{X}_i, \mathbf{Y}_i)$ , where the derived bound in (37) is independent of the  $a_{i+1,j}$ 's and thus of the input  $x_{i+1}$ .) This completes the proof.  $\square$

It is not straightforward to analyze tightness for the general GTrunc construction, i.e., to derive a lower bound. As demonstrated by Gilboa and Gueron [26], the analysis for plain truncation is already highly involved: including a feed-forward of the input only frustrates the analysis, and influences the per-query probability of a response to occur (unlike the case of plain Trunc of Sect. 4.1 and GTrunc without feed-forward of Sect. 4.2). However, it is possible to argue tightness for a reasonable simplification of GTrunc. In detail, if  $\text{post} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^m$  is linear in  $x$ , i.e.,

$$\text{post}(x, y) = \mathbf{A} \cdot x \oplus \text{post}'(y) \tag{52}$$

for some matrix  $\mathbf{A} \in \{0, 1\}^{m \times n}$  and arbitrary  $\text{post}' : \{0, 1\}^n \rightarrow \{0, 1\}^m$ , an adversary can “undo the feed-forward” by deciding to attack

$$(\text{GTrunc}')^p(x) = \text{GTrunc}^p(x) \oplus \mathbf{A} \cdot x \tag{53}$$

$$= \text{post}'(p(x)). \tag{54}$$

In this way, it returns to the simpler case of Theorem 5. More involved post-processing functions, where  $x$  is used to transform  $y$  (e.g., by rotation or multiplication) do not fall victim to this technique.

#### 4.4 Arbitrary Post-processing

We finally consider GTrunc with arbitrary post-processing, where we only assume that any value  $y \in \{0, 1\}^m$  occurs with positive probability. Let  $\gamma \in \mathbb{N} \cup \{0\}$  be such that  $|\text{post}^{-1}[x](y) - 2^{n-m}| \leq \gamma$  for any  $x \in \{0, 1\}^n$  and  $y \in \{0, 1\}^m$ . This value  $\gamma$  measures the unbalancedness of  $\text{post}$ : for  $\gamma$  close to 0,  $\text{post}$  is close to a balanced function.

**Theorem 7 (Security of GTrunc with arbitrary post).** *Let  $q, n, m \in \mathbb{N}$  such that  $m \leq n$ . Consider GTrunc of (38) with arbitrary  $\text{post}$ . For any distinguisher  $\mathcal{D}$  making at most  $q$  queries,*

$$\text{Adv}_{\text{Trunc}}^{\text{prf}}(\mathcal{D}) \leq \frac{1}{2} \left( \frac{(2^m - 1)q(q - 1)}{(2^n - 1)(2^n - q + 1)} \right)^{1/2} + \left( \frac{1}{2} q \left( \frac{\gamma}{2^{n-m}} \right)^2 \right)^{1/2}. \tag{55}$$

*Proof.* The proof is identical to that of Theorem 6, with one important exception:  $\text{post}$  does not need to be balanced, and hence  $\Delta(Y^f, Y) \geq 0$ . We will use Pinsker’s inequality (7) on the chi-squared divergence (9) to bound this term. For any  $i = 1, \dots, q$ ,  $\mathbf{j}_{i-1} \in \{1, \dots, 2^m\}^{i-1}$ , and  $j \in \{1, \dots, 2^m\}$ ,

$$\Pr((Y^f)_i = j \mid (\mathbf{Y}^f)_{i-1} = \mathbf{j}_{i-1}) = \Pr((Y^f)_i = j) = \frac{1}{2^m}, \tag{56}$$

$$\Pr(Y_i = j \mid \mathbf{Y}_{i-1} = \mathbf{j}_{i-1}) = \Pr(Y_i = j) = \frac{a_{i,j}}{2^n}. \tag{57}$$

In particular, for both  $Y^f$  and  $Y$  the drawing of the  $i$ -th element is independent of the first  $i - 1$  samples. From the chi-squared divergence (9), for which we translate its inductive formula [23] to our setting, we obtain

$$\chi^2(Y; Y^f) \leq \sum_{i=1}^q \sum_{j=1}^{2^m} \frac{(\Pr(Y_i = j) - \Pr((Y^f)_i = j))^2}{\Pr((Y^f)_i = j)} \quad (58)$$

$$= \sum_{i=1}^q \sum_{j=1}^{2^m} \frac{1}{2^{2n-m}} (a_{i,j} - 2^{n-m})^2. \quad (59)$$

Using that  $|a_{i,j} - 2^{n-m}| \leq \gamma$ , we can proceed:

$$\chi^2(Y; Y^f) \leq \sum_{i=1}^q \sum_{j=1}^{2^m} \frac{\gamma^2}{2^{2n-m}} \quad (60)$$

$$= q \left( \frac{\gamma}{2^{n-m}} \right)^2. \quad (61)$$

The proof is completed using Pinsker's inequality (7).  $\square$

The first part of the bound of Theorem 7 is identical to that of Theorem 6, and the comments on tightness carry over. The second part of the bound comes from the bounding of  $\Delta(Y^f, Y)$ , and in this bounding we use the estimation  $|a_{i,j} - 2^{n-m}| \leq \gamma$ , which is non-tight for most of the choices for  $(i, j)$ . We see no way of attacking the scheme with query complexity around  $(2^{n-m}/\gamma)^2$ , but it is reasonable to assume that the security degrades with the bias in the balancedness of post.

It is interesting to note that, had we used the Kullback-Leibler divergence (6) instead of the chi-squared divergence (9), we would have derived

$$KL(Y; Y^f) \leq q \left( 1 + \frac{\gamma}{2^{n-m}} \right) \log \left( 1 + \frac{\gamma}{2^{n-m}} \right), \quad (62)$$

which is in turn at most

$$q \left( 1 + \frac{\gamma}{2^{n-m}} \right) \left( \frac{\gamma}{2^{n-m}} \right) \quad (63)$$

as  $\log(\alpha) \leq \alpha - 1$  (for any  $\alpha > 0$ ). In other words, the non-tightness of  $|a_{i,j} - 2^{n-m}| \leq \gamma$  would have amplified into a slightly worse overall bound. We remark that this does not contradict (8).

## 5 Note on Including Pre-processing Function

One might consider generalizing GTrunc of (38) even further to include an arbitrary pre-processing function  $\text{pre} : \{0, 1\}^n \rightarrow \{0, 1\}^n$  as well:

$$(\text{GTrunc}')^p(x) = \text{post}(x, p(\text{pre}(x))). \quad (64)$$

However, we see no justification for doing so. If  $\text{pre}$  is balanced, it is necessarily invertible and one can “absorb” it into  $p$  as done in the analysis of Sect. 4.2. If it is unbalanced, this means that there exist distinct  $x, x'$  such that  $\text{pre}(x) = \text{pre}(x')$ , and consequently, the evaluations  $(\text{GTrunc}')^p(x)$  and  $(\text{GTrunc}')^p(x')$  use the same source of randomness:

$$p(\text{pre}(x)) = p(\text{pre}(x')). \quad (65)$$

This does not immediately lead to an attack, most importantly as  $\text{post}$  only outputs  $m \leq n$  bits. If, in particular,  $m \ll n$ , a distinguisher may not note that the same randomness is employed. Nevertheless, unbalanced  $\text{pre}$ 's seem to set the stage for a weaker generalized truncation.

**Acknowledgments.** Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017. The author would like to thank the reviewers for their detailed comments and suggestions.

## References

1. Adams, C.: The CAST-128 encryption algorithm. Request for Comments (RFC) 2144, May 1997. <http://tools.ietf.org/html/rfc2144>
2. Aoki, K., et al.: Specification of Camellia – a 128-bit Block Cipher, Version 2.0 (2001). <https://info.isl.ntt.co.jp/crypt/eng/camellia/dl/01espec.pdf>
3. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: a small present - towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer, Cham (2017). [https://doi.org/10.1007/978-3-319-66787-4\\_16](https://doi.org/10.1007/978-3-319-66787-4_16)
4. Beierle, C., et al.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). [https://doi.org/10.1007/978-3-662-53008-5\\_5](https://doi.org/10.1007/978-3-662-53008-5_5)
5. Bellare, M., Guérin, R., Rogaway, P.: XOR MACs: new methods for message authentication using finite pseudorandom functions. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 15–28. Springer, Heidelberg (1995). [https://doi.org/10.1007/3-540-44750-4\\_2](https://doi.org/10.1007/3-540-44750-4_2)
6. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999). <http://eprint.iacr.org/1999/024>
7. Bellare, M., Kilian, J., Rogaway, P.: The security of cipher block chaining. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 341–358. Springer, Heidelberg (1994). [https://doi.org/10.1007/3-540-48658-5\\_32](https://doi.org/10.1007/3-540-48658-5_32)
8. Bellare, M., Krovetz, T., Rogaway, P.: Luby-Rackoff backwards: increasing security by making block ciphers non-invertible. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 266–280. Springer, Heidelberg (1998). <https://doi.org/10.1007/BFb0054132>

9. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006). [https://doi.org/10.1007/11761679\\_25](https://doi.org/10.1007/11761679_25)
10. Bernstein, D.J.: SURF: simple unpredictable random function (1997). <https://cr.yp.to/papers.html#surf>
11. Bernstein, D.J.: How to stretch random functions: the security of protected counter sums. *J. Cryptol.* **12**(3), 185–192 (1999). <https://doi.org/10.1007/s001459900051>
12. Bhattacharya, S., Nandi, M.: A note on the chi-square method: a tool for proving cryptographic security. *Cryptogr. Commun.* **10**(5), 935–957 (2018). <https://doi.org/10.1007/s12095-017-0276-z>
13. Biham, E., Anderson, R., Knudsen, L.: Serpent: a new block cipher proposal. In: Vaudenay, S. (ed.) FSE 1998. LNCS, vol. 1372, pp. 222–238. Springer, Heidelberg (1998). [https://doi.org/10.1007/3-540-69710-1\\_15](https://doi.org/10.1007/3-540-69710-1_15)
14. Bogdanov, A., et al.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). [https://doi.org/10.1007/978-3-540-74735-2\\_31](https://doi.org/10.1007/978-3-540-74735-2_31)
15. Bose, P., Hoang, V.T., Tessaro, S.: Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 468–499. Springer, Cham (2018). [https://doi.org/10.1007/978-3-319-78381-9\\_18](https://doi.org/10.1007/978-3-319-78381-9_18)
16. Brassard, G.: On computationally secure authentication tags requiring short secret shared keys. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) *Advances in Cryptology*, pp. 79–86. Springer, Boston, MA (1983). [https://doi.org/10.1007/978-1-4757-0602-4\\_7](https://doi.org/10.1007/978-1-4757-0602-4_7)
17. Chang, D., Nandi, M.: A short proof of the PRP/PRF switching lemma. *Cryptology ePrint Archive, Report 2008/078* (2008). <http://eprint.iacr.org/2008/078>
18. Cogliati, B., Lampe, R., Patarin, J.: The indistinguishability of the XOR of  $k$  permutations. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 285–302. Springer, Heidelberg (2015). [https://doi.org/10.1007/978-3-662-46706-0\\_15](https://doi.org/10.1007/978-3-662-46706-0_15)
19. Cogliati, B., Seurin, Y.: EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 121–149. Springer, Heidelberg (2016). [https://doi.org/10.1007/978-3-662-53018-4\\_5](https://doi.org/10.1007/978-3-662-53018-4_5)
20. Csiszár, I.: Eine informationstheoretische Ungleichung und ihre Anwendung auf den Beweis der Ergodizität von Markoffschen Ketten. *Magyar. Tud. Akad. Mat. Kutató Int. Közl.* **8**, 85–108 (1963)
21. Csiszár, I.: Information-type measure of difference of probability distributions and indirect observations. *Stud. Sci. Math. Hung.* **2**, 299–318 (1967)
22. Daemen, J., Rijmen, V.: *The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography*. Springer, Heidelberg (2002). <https://doi.org/10.1007/978-3-662-04722-4>
23. Dai, W., Hoang, V.T., Tessaro, S.: Information-theoretic indistinguishability via the chi-squared method. In: Katz, J., Shacham, H., (eds.) [33], pp. 497–523. [https://doi.org/10.1007/978-3-319-63697-9\\_17](https://doi.org/10.1007/978-3-319-63697-9_17)
24. Dworkin, M.: NIST SP 800–38A: Recommendation for block cipher modes of operation: methods and techniques (2001)
25. Gilboa, S., Gueron, S.: Distinguishing a truncated random permutation from a random function. *Cryptology ePrint Archive, Report 2015/773* (2015). <http://eprint.iacr.org/2015/773>

26. Gilboa, S., Gueron, S.: The advantage of truncated permutations. CoRR abs/1610.02518 (2016). <http://arxiv.org/abs/1610.02518>
27. Gilboa, S., Gueron, S., Morris, B.: How many queries are needed to distinguish a truncated random permutation from a random function? *J. Cryptol.* **31**(1), 162–171 (2018). <https://doi.org/10.1007/s00145-017-9253-0>
28. Gueron, S., Langley, A., Lindell, Y.: AES-GCM-SIV: specification and analysis. Cryptology ePrint Archive, Report 2017/168 (2017). <http://eprint.iacr.org/2017/168>
29. Gueron, S., Lindell, Y.: GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte. In: Ray, I., Li, N., Kruegel, C. (eds.) Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015, pp. 109–119. ACM, New York (2015). <https://doi.org/10.1145/2810103.2813613>
30. Hall, C., Wagner, D., Kelsey, J., Schneier, B.: Building PRFs from PRPs. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 370–389. Springer, Heidelberg (1998). <https://doi.org/10.1007/BFb0055742>
31. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 8–26. Springer, New York (1990). [https://doi.org/10.1007/0-387-34799-2\\_2](https://doi.org/10.1007/0-387-34799-2_2)
32. Iwata, T., Seurin, Y.: Reconsidering the security bound of AES-GCM-SIV. *IACR Trans. Symmetric Cryptol.* **2017**(4), 240–267 (2017). <https://doi.org/10.13154/tosc.v2017.i4.240-267>
33. Katz, J., Shacham, H. (eds.): Advances in Cryptology - CRYPTO 2017–37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017, Proceedings, Part III. LNCS, vol. 10403. Springer, Heidelberg (2017). <https://doi.org/10.1007/978-3-319-63697-9>
34. Kemperman, J.H.: On the optimum rate of transmitting information. *Ann. Math. Stat.* **40**(6), 2156–2177 (1969). <https://doi.org/10.1214/aoms/1177697293>
35. Kullback, S.: A lower bound for discrimination information in terms of variation (corresp.). *IEEE Trans. Inf. Theory* **13**(1), 126–127 (1967). <https://doi.org/10.1109/TIT.1967.1053968>
36. Kullback, S., Leibler, R.A.: On information and sufficiency. *Ann. Math. Stat.* **22**(1), 79–86 (1951). <https://doi.org/10.1214/aoms/1177729694>
37. Lindell, Y., Langley, A., Gueron, S.: AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption. Internet-Draft draft-irtf-cfrg-gcmsiv-05, Internet Engineering Task Force, May 2017, Work in Progress. <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-gcmsiv-05>
38. Lucks, S.: The sum of PRPs is a secure PRF. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 470–484. Springer, Heidelberg (2000). [https://doi.org/10.1007/3-540-45539-6\\_34](https://doi.org/10.1007/3-540-45539-6_34)
39. McGrew, D.A., Viega, J.: The security and performance of the Galois/Counter Mode (GCM) of operation. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 343–355. Springer, Heidelberg (2004). [https://doi.org/10.1007/978-3-540-30556-9\\_27](https://doi.org/10.1007/978-3-540-30556-9_27)
40. Mennink, B., Neves, S.: Encrypted Davies-Meyer and its dual: towards optimal security using mirror theory. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10403, pp. 556–583. [https://doi.org/10.1007/978-3-319-63697-9\\_19](https://doi.org/10.1007/978-3-319-63697-9_19)
41. Mennink, B., Neves, S.: Optimal PRFs from blockcipher designs. *IACR Trans. Symmetric Cryptol.* **2017**(3), 228–252 (2017). <https://doi.org/10.13154/tosc.v2017.i3.228-252>



42. Mennink, B., Preneel, B.: On the XOR of multiple random permutations. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 619–634. Springer, Cham (2015). [https://doi.org/10.1007/978-3-319-28166-7\\_30](https://doi.org/10.1007/978-3-319-28166-7_30)
43. Morimoto, T.: Markov processes and the  $H$ -theorem. J. Phys. Soc. Jpn. **18**(3), 328–331 (1963). <https://doi.org/10.1143/JPSJ.18.328>
44. Patarin, J.: A proof of security in  $O(2^n)$  for the Xor of two random permutations. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 232–248. Springer, Heidelberg (2008). [https://doi.org/10.1007/978-3-540-85093-9\\_22](https://doi.org/10.1007/978-3-540-85093-9_22)
45. Patarin, J.: Introduction to mirror theory: analysis of systems of linear equalities and linear non equalities for cryptography. Cryptology ePrint Archive, Report 2010/287 (2010). <http://eprint.iacr.org/2010/287>
46. Patarin, J.: Security in  $O(2^n)$  for the Xor of two random permutations - proof with the standard  $h$  technique-. Cryptology ePrint Archive, Report 2013/368 (2013). <http://eprint.iacr.org/2013/368>
47. Stam, A.J.: Distance between sampling with and without replacement. Stat. Neerl. **32**(2), 81–91 (1978). <https://doi.org/10.1111/j.1467-9574.1978.tb01387.x>
48. Stam, A.J.: A note on sampling with and without replacement. Stat. Neerl. **40**(1), 35–38 (1986). <https://doi.org/10.1111/j.1467-9574.1986.tb01162.x>
49. Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**(3), 265–279 (1981). [https://doi.org/10.1016/0022-0000\(81\)90033-7](https://doi.org/10.1016/0022-0000(81)90033-7)