On The Distinguishability of Ideal Ciphers

Roberto Avanzi [1] and Yvo Desmedt [2]

[1] Architecture and Technology Group, ARM Germany
[2] Department of Computer Science, The University of Texas at Dallas

Abstract. We present distinguishing attacks (based on the Birthday Paradox) which show that the use of 2^ℓ permutations for a block cipher is insufficient to obtain a security of ℓ bits in the Ideal Cipher Model.
The context is that of an Oracle that can provide an Adversary the ciphertexts of a very small number of known plaintexts under a large number of (session) keys and IVs/nonces.
Our attacks distinguish an ideal cipher from a "perfectly ideal" block cipher, realised as an Oracle that can always produce new permutations up to the cardinality of the symmetric group on the block space.
The result is that in order to guarantee that an Adversary which is time limited to $O(2^\ell)$ encryption requests has only a negligible advantage, the cipher needs to express $2^{3\ell}$ distinct permutations. This seems to contradict a folklore belief about the security of using a block cipher in the multi-key setting, i.e. to obtain ℓ-bit security it is sufficient to use ℓ- or $2\,\ell$-bit keys depending on the mode of operation and the use case.

Keywords: Block Ciphers, Cryptanalysis, Cryptographic Foundations, Ideal Cipher Model, Random Oracle

1 Introduction

1.1 The Problem

We consider the security in the multi-key (mk) setting of a block-wise operating cipher where the block size is n and the space of the permutations that can be expressed by the cipher has a size of k bits. We note that the *permutation space* is not only indexed by the key, but also by other information such as IVs or nonces if not controlled by the attacker. We call the totality of the information that selects the permutation the *index* (a possible such index would be a *tweakey* [27]).

Here, the Adversary that tries to distinguish the traffic from randomness has access to an Oracle giving the encryption of *a very few constant messages* under various indices. For instance, an Adversary may be able to eavesdrop the first blocks of several HTTPS sessions. As Bernstein remarked [4], the first message block of any such session is often quite predictable, e.g.:

"`GET / HTTP/1.1\r\n`" .

Questions that drive our investigations thus include:

1. *What is the actual* mk *security level of a block cipher with n-bit blocks and a k-bit permutation space?*
2. *How large should the permutation space of a n-bit block cipher be in order to guarantee a* mk *security level of ℓ bits, for a given security parameter ℓ?*

1.2 The State of the Art (Selection)

Bellare, Boldyreva, and Micali proved [2] that attacking any one of t independently keyed instances of the same public-key encryption algorithm has success probability bounded by t times the success probability of attacking a single instance of the algorithm. Their result is expressed in the sense of (computational) indistinguishability, that dates back to Goldwasser and Micali [20] and Yao [44].

Since Yuval's 1979 paper [45] it is known that, by the Birthday Paradox, the length of a hash function has to be at least the double of the desired security. Similar results for encryption are very well known, for instance, many modes of operation offer security only up to the birthday bound, and sometimes the differences between such modes and Beyond the Birthday Bound (BBB) modes can be subtle. For instance, the OCB mode as based on the XEX/XE construction [39] offers indistinguishability from a random Oracle only up to the birthday bound, but BBB if based on a "true" tweakable block cipher (TBC) [31,32].

Mk security degradation for symmetric encryption, mostly studied for specific modes of operation or block cipher constructions [3,24,25,36,42,33,12] (to name a few), is an area where the Birthday Paradox finds natural application.

Furthermore, there has been a large body of contributions in understanding the security of the underlying primitive, the block cipher, in the mk setting – but this research is mostly in the areas of time-memory tradeoffs to find key collisions or related-key security [5,11,19,26]. The applicability of related-key attacks heavily depends on the design of the primitive and its specific use [16]. In the case of the AES [15], a significant body of research [6,29,8,7,18,9,10] has been devoted to the related-key security of its versions with 192 and 256 bit keys, eventually reducing their security to at most 176 and 99 bits respectively.

1.3 The Results

We describe simple distinguishing attacks that can tell an Ideal Block Cipher (IBC) from the uniform sampling of *all* permutations, where the running time of the distinguisher will yield the security level. The set of all permutations forms a "perfectly ideal" cipher that intends to capture the maximal level of security for a given block size. Hence, we study how close we should get to that "perfect ideal" in order to achieve a desired security level.

We follow the Ideal Cipher Model (ICM) which (see e.g., [14]) consists in having an Oracle uniformly and independently sample 2^ℓ permutations from the set of all n-bit permutations. The definition of an IBC naturally translates from keys to indices, since, for instance, in an ideal TBC, the tweak shall provide the same level of uniformity in the selection of the permutations as the key.

Our Adversaries only requests encryption from the Oracle, but this is only a limitation for the Adversaries, not for the Oracle. Adversaries that also request decryptions may be more powerful, not less.

The analysis based on the Birthday Paradox: in a set of 2^k permutations, it takes only $O(2^{k/2})$ random draws before we pick the same permutation twice. In this *Gedankenexperiment*, the permutations are compared on a few inputs (w.l.o.g. 0, 1, 2 and so on). Clearly, any such partial comparison may yield false positives. The actual complexity of the distinguisher will thus depend on the number of allowed comparisons. We analyse the security of IBCs against attacks based on these distinguishers, according to the following classical definition.

Definition 1. *Let ℓ be a security parameter. An ideal cipher is* secure *w.r.t. the security parameter ℓ, or, in other words, achieves a* security level of ℓ bits *if, for any Adversary upper bounded by $O(2^\ell)$ queries, the advantage of the Adversary is* negligible *in ℓ, i.e. at most $O(2^{-\ell})$ [21].*

Our main result is that *to get a security level of ℓ bits we need to use indices of at least $k = 3\,\ell$ bits.* This result can be applied to several modes of operation. For instance, the XTS mode, widely used for full disk encryption [34], if instantiated with AES-128 and *two* independent keys (and a 128-bit IV) is more secure (in the mk, indistinguishability setting) than if used with just one single 128-bit key (and a 128-bit IV) – See Remark 9 in § 5.2. This contradicts Liskov and Minematsu's assertion that a single key should be used [30]. Since XTS and OCB are both based on the XEX construction, a similar argument could be made for the use of two distinct keys in OCB (of course, OCB is also known to not offer BBB security). An exhaustive analysis of all modes of operation is beyond the scope of this paper. We offer baseline results applicable to many different contexts, to determine the parameters to achieve the desired security level.

Under the weaker security definition that *an attack based on a distinguisher shall have time complexity at least 2^ℓ*, we must have $k \gtrsim 2n$ and $n \geqslant \ell$.

Outline of the paper. In § 2 we introduce our notations and provide background information. We formalise in § 3 the interaction between Adversary and Oracle and present a simple strategy exploiting the Birthday Paradox: this strategy serves mostly as an example to present the techniques used later. In § 4 we introduce the Time-Advantage Trade-Off. In § 5 we discuss a more powerful attack strategy that shows that, in contrast to authentication, doubling key sizes is not enough to prevent distinguishing attacks. § 6 focuses on the index size choice in order to defend against our attacks. We conclude in § 7. Technical proofs are in the Appendix.

2 Notation and Background

2.1 Notation

Following the ICM, we assume the Oracle has chosen 2^k permutations. We let n, resp. k be the block size, resp. index size of the ideal block cipher in bits.

Definition 2. *A request (by the attacker) to the Oracle is a* $(d+1)$*-tuple* $(a, m^1, \ldots, m^d)$ *with* $a \in \mathbb{N} \cup \{\perp\}$ *and* $m^j \in \{0,1\}^n$*. If* $d = 1$*, the exponents are omitted. The symbol* $\perp$ *means "new", as being independently (and uniformly) drawn. In a sequence* $\left[(a_i, m_i^0, \ldots m_i^{d-1})\right]_{i \geqslant 1}$ *of requests, the* $a_i \in \mathbb{N} \cup \{\perp\}$ *satisfy the following: In the first tuple, we have* $a = \perp$*, i.e.,* $a_1 = \perp$*; We then continue recursively by letting*

$$L_j = \{i \mid a_i = \perp, \text{ where } 1 \leqslant i \leqslant j\}$$

be the list of already sampled indices and requiring that $a_{j+1} \in [1, |L_j|] \cup \{\perp\}$.

In other words, the first element of a request means "give me encryptions with a fresh selected permutation, or with a specified, already sampled one." The returned permutations are indexed as π_a. Upon receiving $\perp$, the Oracle is *allowed to return a previously sampled permutation*, so it may be $\pi_{a'} = \pi_{a''}$ for indices $a' \neq a''$.

2.2 Mathematical Background

We recall some facts about the Birthday Paradox [17, §§ II.3, II.7]. When having t balls and u bins and we throw t balls each in a uniformly, randomly chosen bin, let $P_{t,u}$ be the probability that *no* bin contains two balls. Provided $t \leqslant u$, it is:

$$P_{t,u} = \prod_{i=0}^{t-1} \left(1 - \frac{i}{u}\right) \ .$$

Then, $1 - P_{t,u}$ is the probability that after t balls have been thrown, at least one bin contains two balls. Put

$$\mathfrak{p}_{t,u} = e^{-\frac{t(t-1)}{2u}} \ .$$

It is

$$e^{-\frac{(t-1)^2}{2u}} \geqslant \mathfrak{p}_{t,u} \geqslant P_{t,u} \geqslant e^{-\frac{t^2}{2u}}, \quad \text{and}$$
$$1 - e^{-\frac{t^2}{2u}} \geqslant 1 - P_{t,u} \geqslant 1 - e^{-\frac{(t-1)^2}{2u}} \ .$$

3 The Distinguishing Attack

3.1 The Setting and the Protocol Between Adversary and Oracle

An Adversary $\mathcal{A}$ faces an Oracle $\mathcal{O}$. $\mathcal{O}$ chooses randomly one of two sets, either

$$\mathcal{S}_0 = \{\pi : \{0,1\}^n \to \{0,1\}^n\} = \Sigma_{2^n} \ ,$$

which is the set of all permutations on 2^n elements and that we use to model a "perfectly ideal" block cipher, and a multiset

$$\mathcal{S}_{1,v} = \mathcal{S}_{1,2^k} = \{E_K \in_R \mathcal{S}_0 \mid \forall K \in \{0,1\}^k\} \subseteq \mathcal{S}_0$$

Protocol 1: Interaction Between Oracle and Adversary

Step 1 The Oracle $\mathcal{O}$ flips a fair coin giving as outcome $b \in \{0,1\}$.

Step 2 The Adversary sets $i := 0$.

Step 3 The Adversary lets $i := i+1$ and requests the Oracle $(a_i, m_i^0, \ldots, m_i^{d-1})$, where the request $(d+1)$-tuple satisfies Definition 2.

Step 4 *If* $a_i = \perp$, *then* $\mathcal{O}$ chooses uniformly a permutation $\pi_{|L_i|} \in \mathcal{S}_b$ and sends

$$\left(O_i^0, \ldots, O_i^{d-1}\right) = \left(\pi_{|L_i|}(m_i^0), \ldots, \pi_{|L_i|}(m_i^{d-1})\right)$$

to the Adversary; *else* $\mathcal{O}$ returns

$$\left(O_i^0, \ldots, O_i^{d-1}\right) = \left(\pi_{a_i}(m_i^0), \ldots, \pi_{a_i}(m_i^{d-1})\right) \quad .$$

Step 5 The Adversary decides whether to continue with this attack. If so, then we go to **Step 3**, else the Adversary outputs b'.

of size 2^k of uniformly and independently sampled permutations, indexed by k bit strings, in other words an IBC. In the following the Oracle will lazily assign a permutation to an index once a new permutation is requested, which is equivalent to requesting that the Adversary choose a new random string for the index.

The task of the Adversary is to find with a non negligible bias which set the Oracle has chosen. Of course it is no surprise that one can distinguish between these two choices: One will clearly get sampling collisions more often in $\mathcal{S}_1$ than in $\mathcal{S}_0$, as long as $2^k \ll (2^n)!$. By Stirling's Formula this means $k \ll (n - \log_2 e)2^n + O(n)$. The parameters we are interested in are when this will happen and its likelihood. We describe this formally in Protocol 1.

3.2 A Simplified Strategy

The Adversary $\mathcal{A}$ executes Protocol 1 in which the Adversary chooses a sequence of requests and outputs b' depending on the decision she is capable of making within the running time t allowed. Since the time t is a parameter, we define $\mathcal{A}_{|t}$ as the restriction of $\mathcal{A}$ to being able to request only t queries from the Oracle, to be more precise, i.e., executing the strategy with a specific time bound t.

The first Strategy of the Adversary is as follows:

Strategy 1 *Fix $d = 1$. The Adversary always picks $m_i = 0$. If there exists a $j < i$ such that $O_i = O_j$, then return $b' = 1$; if after iteration $i = t$ no such collision was observed, then return $b' = 0$; else increase i and continue.*

As mentioned in the introduction, this strategy serves mostly as an example to showcase the techniques that are later used in the general case.

3.3 Preliminary Observations

We analyse the attack, for now, in the case $d = 1$, and by assuming that $S_{1,v}$ has $v = 2^k$ random permutations, where $k = n$ is a special case.

Even though Oracles for the ICM are assumed to be bidirectional, our attacker only requests encryptions. For the moment, as only encryptions of 0 are requested, we can introduce a *multi-set* D_1 formed by the 2^k encryptions of 0 through all 2^k permutations in $\mathcal{S}_{1,v}$ – where repeated values are included with their multiplicity. We now analyse this multi-set. We observe that:

1. The Oracle $\mathcal{O}$ choosing 2^k permutations, implies that it chooses a multi-set D_1 of size 2^k with repetition allowed out of 2^n possible values.
2. When the attacker requests a "fresh" index and an encryption of 0, then $\mathcal{O}$ will choose a random value out of the multi-set D_1.

3.4 Analysis

Definition 3. *We define the* security *of $\mathcal{S}_{1,v}$ against an Adversary $\mathcal{A}$ requesting t queries from the Oracle $\mathcal{O}$ as*

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) = \left|\mathbb{P}[\mathcal{A}_{|t}(\mathcal{S}_{1,v}) = 1] - \mathbb{P}[\mathcal{A}_{|t}(\mathcal{S}_0) = 1]\right| \ .$$

Definition 4. *We also define the* absolute advantage *of the Adversary $\mathcal{A}$ as*

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}) = \max_t \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) \ , \tag{1}$$

the maximum taken over the instances of $\mathcal{A}$ making t queries, for all $t \in \mathbb{N}$.

Let us define two positive quantities u and u:

$$u = 2^n \quad \text{and} \quad v = 2^k \ . \tag{2}$$

The main result of this section is the following Theorem:

Theorem 1. *Consider Adversary $\mathcal{A}$ executing Protocol 1, with n and k natural numbers satisfying $k \geqslant n$, and $u = 2^n$, $v = 2^k$. The advantage of $\mathcal{A}$ satisfies*

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}) \leqslant \left(\frac{v}{u+v}\right)^{v/u} \cdot \frac{u}{u+v} + O\left(\max\left\{\frac{1}{\sqrt{u}}, \frac{1}{\sqrt{v}}\right\}\right)$$

where the maximum is attained for some $t = \widetilde{\Theta}\big(\sqrt{\min\{u,v\}}\big)$. In particular, if $u = v$, this maximum is $\approx \frac{1}{4}$ and in general it is $\approx \chi \frac{1}{1+2^{k-n}}$ where $1 < \chi < \frac{1}{e}$.

Hence, an IBC with a block size of n and equal index size can be distinguished by Adversary $\mathcal{A}$ from truly random permutations in time $O(2^{n/2})$.

The proof of Theorem 1 relies on some technical Lemmas. The first two Lemmas establish that we can study analytic approximations of the advantage instead of exact probabilities. We use them – and Lemma 3 – in this section with $u = 2^n$ and $v = 2^k$, but they hold with greater generality.

Lemma 1. *Let $u, v, t \in \mathbb{N}$, with $1 \leqslant t \leqslant \min\{u, v\}$. The security of $\mathcal{S}_{1,v}$ against an Adversary $\mathcal{A}$ requesting t queries from the Oracle satisfies:*

$$e^{-\frac{(t-1)^2}{2u}}\left(1-e^{-\frac{t^2}{2v}}\right) \geqslant \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) \geqslant e^{-\frac{t^2}{2u}}\left(1-e^{-\frac{(t-1)^2}{2v}}\right) \tag{3}$$

and

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) \approx \mathfrak{p}_{t,u}\,(1-\mathfrak{p}_{t,v}) \quad . \tag{4}$$

The error in (4) will be bounded in Lemma 2. These bounds are in general meaningful for $t \leqslant \min\{u, v\}$ only. For larger t the likelihoods become trivial, the approximation for $P_{t,u}$ breaks down, and the cases have to be treated separately.

Proof. We evaluate the advantage piecewise.

First, $\mathbb{P}[\mathcal{A}_{|t}(\mathcal{S}_0) = 1]$ is the likelihood that for any multi-set of t functions from $\mathcal{S}_0$, once they are all evaluated at the same point (which we can assume w.l.o.g. to be the value 0), they result in a collision. Since $\mathcal{S}_0$ is the whole symmetric group, this is the same as picking a multi-set of t values from $[0, 2^{n-1}]$. In other words, $\mathbb{P}[\mathcal{A}_{|t}(\mathcal{S}_0) = 1] = 1 - P_{t,u}$.

For $\mathcal{S}_{1,v}$ there are *two* ways a collision can occur:

Way A The Oracle when returning an encryption of zero, chooses indices i and j in D_1 (see § 3.3) that are identical. When doing t experiments the probability this happens follows from the Birthday Paradox and is $1 - P_{t,v}$. Obviously, in this case, the condition $\pi_i(0) = \pi_j(0)$ is satisfied.

Way B The Oracle when returning an encryption of zero chooses indices that are all different. This happens with probability $P_{t,v}$. However, it is still possible that for two different indices i and j, the values in the corresponding pigeonholes are the same! This is due to the first choice of the Oracle – i.e. when it built the IBC. This probability is $1 - P_{t,u}$.

Hence $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) = \big((1 - P_{t,v}) + P_{t,v}(1 - P_{t,u})\big) - (1 - P_{t,u})$ and finally

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) = P_{t,u}(1 - P_{t,v}) \quad . \tag{5}$$

Now, the bounds given in § 2.2 imply Equations (3) and (4), the second one being clearly between the bounds of the first one. □

Lemma 2. *Put*

$$\varepsilon_{t,u} = \min\left\{1, \frac{t^3}{6\,(u-(t-1))^2}\right\} \quad . \tag{6}$$

Then the error in Lemma 1 is bounded as follows:

$$\begin{aligned}\left|\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) - \mathfrak{p}_{t,u}\,(1-\mathfrak{p}_{t,v})\right| &< (\varepsilon_{t,u} + \varepsilon_{t,v}\,\mathfrak{p}_{t,v})\,\mathfrak{p}_{t,u} < \varepsilon_{t,u}\,\mathfrak{p}_{t,u} + \varepsilon_{t,v}\,\mathfrak{p}_{t,v} \\ &< \varepsilon_{t,u} + \varepsilon_{t,v} \quad .\end{aligned} \tag{7}$$

Proof. Let $0 < \mathfrak{p}_{t,u} - P_{t,u} = \mathbb{E}_{t,u}\,\mathfrak{p}_{t,u}$ be the error in the approximation of $P_{t,u}$ by $\mathfrak{p}_{t,u}$. Sayrafiezadeh [41] proved that $\mathbb{E}_{t,u} < \frac{t^3}{6\,(u-(t-1))^2}$. This bound is very good

for small t but it becomes increasingly less precise as t approaches u. However, by the obvious inequality $\mathbb{E}_{t,u} = \mathfrak{p}_{t,u} - P_{t,u} \leqslant \mathfrak{p}_{t,u}$ we get $\mathbb{E}_{t,u} < \varepsilon_{t,u}$ where $\varepsilon_{t,u}$ is defined as in (6). The error in approximation (4) can now be easily bounded:

$$\begin{aligned}
\left|\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) - \mathfrak{p}_{t,u}\,(1-\mathfrak{p}_{t,v})\right| &= \left|-P_{t,u}\,(1-P_{t,v}) + \mathfrak{p}_{t,u}\,(1-\mathfrak{p}_{t,v})\right| \\
&= \left|-P_{t,u}\,(1-P_{t,v}) + \mathfrak{p}_{t,u}\,(1-P_{t,v}) - \right. \\
&\qquad \left. - \mathfrak{p}_{t,u}\,(1-P_{t,v}) + \mathfrak{p}_{t,u}\,(1-\mathfrak{p}_{t,v})\right| \\
&= \left|(\mathfrak{p}_{t,u} - P_{t,u})\,(1-P_{t,v}) - \mathfrak{p}_{t,u}\,(\mathfrak{p}_{t,v} - P_{t,v})\right| \\
&\leqslant |\,\mathfrak{p}_{t,u} - P_{t,u}\,|\,(1-P_{t,v}) + \mathfrak{p}_{t,u}\,|\,\mathfrak{p}_{t,v} - P_{t,v}\,| \\
&< \varepsilon_{t,u}\,\mathfrak{p}_{t,u} + \varepsilon_{t,v}\,\mathfrak{p}_{t,u}\,\mathfrak{p}_{t,v} < \varepsilon_{t,u}\,\mathfrak{p}_{t,u} + \varepsilon_{t,v}\,\mathfrak{p}_{t,v} \\
&< \varepsilon_{t,u} + \varepsilon_{t,v}\ . \qquad \square
\end{aligned}$$

Remark 1. We note that $\frac{t^3}{6\,(u-(t-1))^2} < 1$ for all $u \geqslant 2$, $t \leqslant u^{2/3}$. Furthermore, for $t = \sqrt[3]{6}\,u^{2/3}$ it is $\frac{t^3}{6\,(u-(t-1))^2} > 1$, and for all $\epsilon > 0$ there is a u_ϵ such that for all $u > u_\epsilon$, $\frac{t^3}{6\,(u-(t-1))^2} < 1$ holds with $t = (\sqrt[3]{6} - \epsilon)\,u^{2/3}$.

Now we can use (4) to approximate the advantages, so we set out to analyse it as a function of $t > 1$. Define

$$\mathfrak{f}(t) := \mathfrak{p}_{t,u}\,(1-\mathfrak{p}_{t,v}) = e^{-\frac{t(t-1)}{2\,u}}\left(1 - e^{-\frac{t(t-1)}{2\,v}}\right)\ . \tag{8}$$

Lemma 3. *The function $\mathfrak{f}(t)$ defined in (8) is positive for $t \geqslant 1$, with $\mathfrak{f}(1) = 0$, and $\lim_{t\to\infty} \mathfrak{f}(x) = 0$ and has only one maximum for $t = t_0$ where*

$$t_0 = \frac{1}{2}\left(1 + \sqrt{4\,R+1}\right) \approx \sqrt{R} \quad \textit{with} \quad R = 2\,v\ln\left(1+\frac{u}{v}\right)\ . \tag{9}$$

Asymptotically in u, say for a fixed ratio $\sigma = \frac{v}{u}$, or $\frac{\ln v}{\ln u}$, and $u \to \infty$ we have:

$$t_0 \approx \begin{cases} \sqrt{2\,u} & \textit{for } v \geqslant u, \textit{ and} \\ \sqrt{2\,v\ln\left(1+\frac{u}{v}\right)} & \textit{for } u > v\ . \end{cases} \tag{10}$$

More precisely, we have the following general bounds

$$\frac{1}{2} + \sqrt{2\,v\ln\left(1+\frac{u}{v}\right)} \leqslant t_0 \leqslant 1 + \sqrt{2\,v\ln\left(1+\frac{u}{v}\right)}\ . \tag{11}$$

Proof. The result will be established by looking at the extrema for $t > 1$. We start by observing that $\mathfrak{f}(t)$ is a differentiable function and

$$\mathfrak{f}'(t) = (2\,t-1)\left[\left(\frac{1}{2\,u} + \frac{1}{2\,v}\right)e^{-\frac{t(t-1)}{2\,v}} - \frac{1}{2\,u}\right]e^{-\frac{t(t-1)}{2\,u}}\ .$$

Now it is easy to check that $\mathfrak{f}'(t) = 0$ for $t > 1$ if and only if

$$e^{-\frac{t(t-1)}{2\,v}} = \frac{v}{u+v}\ . \tag{12}$$

Taking logarithms

$$-\frac{t(t-1)}{2v} = \ln\left(\frac{v}{u+v}\right) \ ,$$

i.e.

$$t^2 - t - R = 0 \ , \quad \text{where} \quad R := 2\,v \ln\left(1+\frac{u}{v}\right) > 0 \ .$$

This quadratic equation is easy to solve and it has only one positive solution

$$t_0 = \frac{1}{2}\left(1+\sqrt{4\,R+1}\right) \approx \sqrt{R} \tag{13}$$

which, together with $\mathfrak{f}(1) = 0$ and $\lim_{x\to\infty} \mathfrak{f}(x) = 0$, establishes (9). The different asymptotic behaviours of t_0 in the two cases where $v \geqslant u$ and $u > v$, given in (10), are trivial to prove.

From (13) we obtain $t_0 = \frac{1}{2} + \sqrt{\frac{1}{4} + R}$ with $R = 2\,v \ln\left(1+\frac{u}{v}\right)$ we immediately get the lower bound of (11), whereas the upper bound of (11) follows upon application of $\sqrt{x+y} \leqslant \sqrt{x} + \sqrt{y}$ for $x, y \geqslant 0$. □

We are now ready to prove Theorem 1.

Proof (Theorem 1). In order to estimate the absolute advantage according to (1), we can directly replace $t_0^2 - t_0$ with R in (8):

$$\begin{aligned}\max_t \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) = \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t_0}) \approx \mathfrak{f}(t_0) &= e^{-\frac{R}{2u}}\left(1-e^{-\frac{R}{2v}}\right) \\ = e^{-\frac{v}{u}\ln\left(\frac{u+v}{v}\right)}\left(1-e^{-\ln\left(\frac{u+v}{v}\right)}\right) &= \left(\frac{v}{u+v}\right)^{v/u} \cdot \frac{u}{u+v} \ . \end{aligned} \tag{14}$$

In the particular case where $k = n$ we have $u = v$ and therefore

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t_0}) \approx \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$$

which is a positive advantage independent of n. Also, by (13) we have

$$t_0 \approx \frac{1}{2} + \sqrt{2\ln 2}\cdot\sqrt{u} \approx 1.17741\cdot 2^{n/2} + 0.5 \ .$$

This implies that an IBC with a block size of n and equal index size can be distinguished from truly random permutations in time $O(2^{n/2})$.

For the general case, put now $\sigma = \frac{v}{u}$. Expression (14) becomes

$$\mathfrak{f}_{|t=t_0}(u) = \left(\frac{\sigma}{1+\sigma}\right)^{\sigma} \cdot \frac{u}{u+v} \ .$$

The function $\chi(\sigma) = \left(\frac{\sigma}{1+\sigma}\right)^{\sigma}$ is monotonically decreasing for $\sigma \geqslant 0$ with $\chi(0) = 1$, $\chi(1) = \frac{1}{2}$ and $\lim_{\sigma\to\infty} \chi(\sigma) = \frac{1}{e}$. This completes the proof. □

4 The Time-Advantage Trade-Off

In this section we introduce a different definition of security which uses our type of distinguisher as a "traditional" cryptanalytic distinguisher, i.e. as a procedure that can be repeatedly run until a bias is measured with certainty.

Definition 5. *Let $a = \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t})$ be the advantage of Adversary $\mathcal{A}$. In order to observe a bias the distinguisher must be repeated $O(1/a)$ times (possibly in parallel by several independent instances of $\mathcal{A}$). The resulting (cumulative) running time is t/a. We call such an expression a* Time-Advantage Trade-Off (TATO)*.*

Remark 2. The relation between minimising the TATO and optimising Time-Memory Trade-Offs is the following. A run of the distinguisher will take time t and also require $O(t)$ memory. The contents of this memory are ignored and reused for each of the $1/\mathfrak{f}(t_0)$ runs of the distinguisher, whereas in Time-Memory Trade-Offs the memory is not erased. Increasing t and with it the memory complexity will increase the success likelihood of a single run of the distinguisher, thus reducing the number of required runs. Note that this is not an equivalence, and a general study of Time-Memory Trade-Offs is out of the scope of this paper.

Remark 3. Indistinguishability implies TATO security.

The next result follows immediately from the proof of Theorem 1.

Corollary 1. *It is*

$$\frac{t_0}{\mathfrak{f}(t_0)} = \begin{cases} \approx \frac{\sqrt{2}}{\chi}\frac{u+v}{\sqrt{u}} = \Theta\big(\frac{v}{\sqrt{u}}\big) & \text{for } v \geqslant u, \text{ with } \chi \to \frac{1}{e} \\ c\sqrt{2v\ln\big(1+\frac{u}{v}\big)} = \Theta\Big(\sqrt{v\ln\big(1+\frac{u}{v}\big)}\Big) & \text{for } v \leqslant u, \text{ with } c \in (\tfrac{1}{4}, 1)\ . \end{cases}$$

Another consequence of Theorem 1 is the following.

Corollary 2. *Let $2^n \geqslant 40$. For the TATO $t/\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t})$ to be at least 2^n or, in other words, for a n bit IBC with and an index size of k bits to retain a TATO security level of n bits against Adversary $\mathcal{A}$, the parameters n and k must satisfy*

$$k \geqslant \frac{3}{2}\,n - c \quad \text{for some absolute constant } c\ . \tag{15}$$

Proof. In the setting of the proof of Theorem 1, we want to determine when $t/\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t}) \geqslant 2^n$. Let us assume first $v < u$. By Theorem 1 and (11) we have

$$\frac{1+\sqrt{2\,v\ln\big(1+\frac{u}{v}\big)}}{\frac{1}{2}\,\frac{u}{u+v}} \geqslant \frac{t_0}{\mathfrak{f}(t_0)}\ . \tag{16}$$

If $t_0/\mathfrak{f}(t_0) \geqslant u$, then the r.h.s. of (16) must be $\geqslant u$ as well. From this we obtain $2\,u > 2\,v\ln\big(1+\frac{u}{v}\big) > \big(\frac{1}{2}\frac{u^2}{u+v}-1\big)^2 > \big(\frac{u}{4}-1\big)^2$. However, $2\,u > \big(\frac{u}{4}-1\big)^2$ cannot hold for $u \geqslant 8\sqrt{6}+20 \approx 39.595$. Thus it must be $v \geqslant u$. In this case, from Corollary 1 we get $\Theta\big(\frac{v}{\sqrt{u}}\big) \geqslant 2^n$, and (15) follows upon taking logarithms. □

Remark 4. Corollary 2 to Theorem 1 tells us that we need to increase index lengths by at least 50% in order to obtain TATO security against our type of Adversary. However, this bound is not necessarily tight: Indeed, Theorem 5 will show that index lengths must be doubled instead.

It is natural to ask whether the TATO $t/\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t})$ can be improved. The next Theorem will show that the results just proved are substantially tight.

Theorem 2. *Similarly to Theorem 1, let us consider the Adversary $\mathcal{A}$ executing Protocol 1, where the natural numbers n and k satisfy $n, k \geqslant 8$. Put $u = 2^n$ and $v = 2^k$ as in (2). The TATO of $\mathcal{A}$ has a global minimum at $t = t_*$ where*

(a) *for $v \geqslant u$ it is*

$$\frac{t_*}{\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t_*})} = \Theta\left(\frac{v}{\sqrt{u}}\right) \quad \textit{and} \quad t_* \in \left[\sqrt{\frac{uv}{u+v}} - 2, \sqrt{u}\right] = \Theta(\sqrt{u})\,; \quad \textit{and} \tag{17}$$

(b) *for $v < u$ it is*

$$\frac{t_*}{\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t_*})} = \Theta\left(\sqrt{v}\right) \quad \textit{and} \quad t_* \in \left[\sqrt{\frac{uv}{u+v}} - 2, 2\sqrt{v} + \frac{3}{2}\right] = \Theta(\sqrt{v}) \ . \tag{18}$$

Theorem 2 is proved in three steps. We first establish in Lemma 4 ranges where the TATO is always increasing or always decreasing, leaving only a tight interval I in which it may have a minimum. This is done directly from the definition of the probabilities $P_{t,u}$, since for very small and very large t the approximations by exponentials are not sufficiently precise for our purposes. We then bound the error between the TATO and the approximations by exponentials, in Lemma 5, which is luckily very good over the interval I. Finally, we estimate the TATO itself using the approximations and the bounds on the errors. Note that the constants in Theorem 2 can be computed explicitly, but we do not need them for our purposes. Omitting them simplifies the proofs.

We define the functions that represents the TATO, resp. its approximation by exponentials as

$$\mathfrak{h}(t) := \frac{t}{\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t})} \quad \text{resp.} \quad \mathfrak{g}(t) := \frac{t}{\mathfrak{f}(t)} = \frac{t}{\mathfrak{p}_{t,u}\,(1 - \mathfrak{p}_{t,v})} \approx \mathfrak{h}(t) \ . \tag{19}$$

Lemma 4. *Let $u, v \geqslant 64$. The following statements hold:*

(i) *For $t < \xi - 2$, where $\xi = \sqrt{\frac{uv}{u+v}}$, it is $\mathfrak{h}(t+1) < \mathfrak{h}(t)$;*
(ii) *For $t > \sqrt{u}$ it is $\mathfrak{h}(t+1) > \mathfrak{h}(t)$; and*
(iii) *For $t > 2\sqrt{v} + \frac{3}{2}$ it is $\mathfrak{h}(t+1) > \mathfrak{h}(t)$.*

The proof of Lemma 4 can be found in Appendix A.1.

Lemma 5. *Assume $u, v \geqslant 64$. It is*

$$\mathfrak{h}(t) = \mathfrak{g}(t)\,(1 + O\,(c))\quad . \tag{20}$$

with

$$c = \begin{cases} 1 - \left(1 - \frac{6}{\sqrt{u}}\right)\left(1 - \frac{9\,u}{128\,v}\right) & \text{for } v \geqslant u \\ 1 - \left(1 - \frac{8}{\sqrt{v}}\right)\left(1 - \frac{9\,v}{128\,u}\right) & \text{for } v < u \end{cases} \tag{21}$$

over the interval

$$I = \begin{cases} \left[\,\xi - 2,\quad \sqrt{u}\qquad\right] = \left[\,(1-\epsilon_a)\sqrt{u} - 2,\quad \sqrt{u}\qquad\right] & \text{for } v \geqslant u \\ \left[\,\xi - 2, 2\,\sqrt{v} + \frac{3}{2}\,\right] = \left[\,(1-\epsilon_b)\sqrt{v} - 2, 2\,\sqrt{v} + \frac{3}{2}\,\right] & \text{for } v < u\ . \end{cases} \tag{22}$$

where $\epsilon_a \to 0$ as $u/v \to \infty$ and where $\epsilon_b \to 0$ as $v/u \to \infty$.

The proof of Lemma 5 is given in Appendix A.2.
We now give the proof of Theorem 2.

Proof (Theorem 2). In this proof, c_i denotes absolute constants for $i = 1, 2$, etc.
It is clear that

$$\max_{t\in I} \mathfrak{g}(t) \leqslant \frac{\max_{t\in I} t}{\min_{t\in I} \mathfrak{p}_{t,u}\,(1 - \max_{t\in I} \mathfrak{p}_{t,v})} \quad \text{and}$$
$$\min_{t\in I} \mathfrak{g}(t) \geqslant \frac{\min_{t\in I} t}{\max_{t\in I} \mathfrak{p}_{t,u}\,(1 - \min_{t\in I} \mathfrak{p}_{t,v})}\ .$$

For $v \geqslant u$ we have

$$\frac{\xi - 2}{\mathfrak{p}_{\xi-2,u}\left(1 - \mathfrak{p}_{\sqrt{u},v}\right)} \leqslant \mathfrak{g}(t) \leqslant \frac{\sqrt{u}}{\mathfrak{p}_{\sqrt{u},u}\,(1 - \mathfrak{p}_{\xi-2,v})}\ . \tag{23}$$

Note that $\frac{1}{2} < \mathfrak{p}_{\xi-2,u} < 1$ (for $u \geqslant 20$) and $\frac{1}{1-e^{-1/x}} > x$ whence

$$\frac{\xi - 2}{\mathfrak{p}_{\xi-2,u}\left(1 - \mathfrak{p}_{\sqrt{u},v}\right)} \geqslant \left(\sqrt{\frac{u}{2}} - 2\right)\frac{2\,v}{u - \sqrt{u}} = c_1\frac{v}{\sqrt{u}} + O\left(\frac{v}{u}\right)\quad . \tag{24}$$

Now, for $v, u \geqslant 64$ we have

$$\mathfrak{p}_{\xi-2,v} = e^{-\frac{(\xi-2)(\xi-3)}{2\,v}} < e^{-\frac{u}{8\,(u+v)}} < \frac{1}{1 + \frac{u}{8\,(u+v)}} = \frac{8\,u + 8\,v}{9\,u + 8\,v}\ , \tag{25}$$

whence

$$\frac{\sqrt{u}}{\mathfrak{p}_{\sqrt{u},u}\,(1 - \mathfrak{p}_{\xi-2,v})} \leqslant \sqrt{u}\cdot\sqrt{e}\cdot\frac{17}{8}\frac{v}{u} = c_2\frac{v}{\sqrt{u}}\ . \tag{26}$$

Summarising, for $v \geqslant u \geqslant 64$, using (23), (24) and (26), we obtain

$$\mathfrak{g}(t) = \Theta\left(\frac{v}{\sqrt{u}}\right) + O\left(\frac{v}{u}\right)\quad . \tag{27}$$

From (27) and (20) with (21) for $v \geqslant u$ we have

$$\mathfrak{h}(t) = \left(\Theta\left(\frac{v}{\sqrt{u}}\right) + O\left(\frac{v}{u}\right)\right)\left(1 + O\left(\frac{1}{\sqrt{u}}\right) + O\left(\frac{u}{v}\right)\right)$$

and thus (17) follows.

For $u > v$ we have

$$\frac{\xi - 2}{\mathfrak{p}_{\xi-2,u}\left(1 - \mathfrak{p}_{2\sqrt{v}+\frac{3}{2},v}\right)} \leqslant \mathfrak{g}(t) \leqslant \frac{2\sqrt{v} + \frac{3}{2}}{\mathfrak{p}_{2\sqrt{v}+\frac{3}{2},u}\left(1 - \mathfrak{p}_{\sqrt{\frac{4v}{5}},v}\right)} \ . \tag{28}$$

We use the fact that $\frac{1}{\mathfrak{p}_{\xi-2,u}} > 1$ to get the following estimate:

$$\frac{\xi - 2}{\mathfrak{p}_{\xi-2,u}\left(1 - \mathfrak{p}_{2\sqrt{v}+\frac{3}{2},v}\right)} \geqslant \left(\sqrt{\frac{v}{2}} - 2\right)\left(2 + O\left(\frac{1}{\sqrt{v}}\right)\right) = c_3\sqrt{v} + O(1) \ . \tag{29}$$

Now (25) holds as in Case (a), but this time, being $u > v$, we have $\frac{1}{1-\mathfrak{p}_{\xi-2,v}} < 17$ and thus

$$\frac{2\sqrt{v} + \frac{3}{2}}{\mathfrak{p}_{2\sqrt{v}+\frac{3}{2},u}\left(1 - \mathfrak{p}_{\xi-2,v}\right)} < 17 \cdot \left(2\sqrt{v} + \frac{3}{2}\right) = c_4\sqrt{v} + O(1) \ . \tag{30}$$

Now, for $u \geqslant v \geqslant 64$, using (28), (29) and (30), we do obtain (18), but with $\mathfrak{g}(t)$ in place of $\mathfrak{h}(t)$. The desired result follows upon application of Lemma 5. □

5 Comparing More Message Blocks

We now return to the classical definition of security and discuss a more complex adversarial strategy. This strategy will be able to distinguish Ideal Ciphers from truly random permutations even if the Oracle chooses for example 2^{2^ℓ} permutations where ℓ is the security parameter.

The Adversary and the Oracle execute Protocol 1 in which the Adversary chooses the sequence (a_i, m_i) and outputs b' as defined by the following strategy.

Strategy 2 *Assuming $d = 2$, the Adversary always picks $m_i = 0$ except if there exists a $j < i$ such that $O_i = O_j$ and $m_i = m_j = 0$, in which case she requests from the Oracle $(a'_j, m'_j) = (j, 1)$ receiving O'_j, and $(a'_i, m'_i) = (i, 1)$ receiving O'_i. At this point if also $O'_i = O'_j$ then she returns $b' = 1$. If after iteration $i = t$ no such collision has been observed, then she returns $b' = 0$, else continues with the next value of i.*

Remark 5. Note that, as opposed to Protocol 1, (a_i, m_i) may not correspond with the attacker's i-th request. However, it is at most the $2i$-th request. Therefore, for an attack with a given t, the running time is at most $2\,t$.

Remark 6. It is now obvious how to define Strategy 2 for larger d: if $O_i = O_j$, then compare O'_i with O'_j, and if these match request encryptions of 2, obtaining O''_i and O''_j. Now compare them and continue until we compare $O_i^{(d-1)}$ to $O_j^{(d-1)}$. If any of these comparisons fails, abort this series of comparisons and increase i, otherwise return $b' = 1$. After the t-th iteration return $b' = 0$.

In order to simplify the analysis of the advantage, we shall instead consider the following equivalent strategy.

Strategy 3 *Let $d \in \mathbb{N}$. The Adversary always picks $m_i^a = a$ for $0 \leqslant a < d$. If $\left(O_i^0, \ldots, O_i^{d-1}\right) = \left(O_j^0, \ldots, O_j^{d-1}\right)$ for some $j < i$, then she returns $b' = 1$. If after iteration $i = t$ no such collision has been observed, then she returns $b' = 0$, else she continues with the next value of i.*

Remark 7. Strategies 2 and 3 are equivalent in the sense that the second strategy requests the encryptions of at least as many and at most d times as many blocks as the first one. Conversely, Strategy 3 reduces to Strategy 2 by making the encryption requests lazy and with early abort. Therefore we shall optimise as before for t, and the running time will be $O(t)$.

This observation is important in order to consider optimality of these strategies. In fact, as usual we start by ignoring adversaries that make "useless" comparisons, such as comparing two encryptions of 1 if the encryptions of 0, or asking for only one encryption of some new text. Only adversaries following Strategy 2 (as generalised for all d) are left in the end.

Definition 6. *Let $d \in \mathbb{N}$. We define the security of $\mathcal{S}_{1,v}$ against an Adversary $\mathcal{A}^d$ using the for loop until t as*

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t}) = \left|\mathbb{P}[\mathcal{A}^d_{|t}(\mathcal{S}_{1,v}) = 1] - \mathbb{P}[\mathcal{A}^d_{|t}(\mathcal{S}_0) = 1]\right| \ .$$

5.1 Analysis of the Advantage for $d = 2$

Let us fix $d = 2$ for now. Let $\mathcal{A}^2$ be an Adversary following Strategy 3 and $\mathcal{A}^2_{|t}$ be the restriction of $\mathcal{A}^2$ to at most t iterations of the loop in Protocol 1.

We start with analysing $\mathbb{P}[\mathcal{A}^2_{|t}(\mathcal{S}_{1,v}) = 1]$. We proceed similarly as in the proof of Lemma 1 and conclude that $b' = 1$ can occur in two different ways:

Way A The Oracle when returning an encryption of 0, chooses identical permutations π_i and π_j. When doing t experiments the probability that this happens is $1 - P_{t,2^k}$. Obviously, in this case, the conditions $\pi_i(0) = \pi_j(0)$ and $\pi_i(1) = \pi_j(1)$ are satisfied.

Way B The Oracle when returning an encryption of 0 had chosen different permutations. This happens with probability $P_{t,2^k}$. However, it is still possible that $b' = 1$. For this to be satisfied we need both collisions $O_i^0 = O_j^0$ and $O_i^1 = O_j^1$.
We now want to determine the probability corresponding to this case. Note that in the arguments in § 3.3, we can replace the multi-set of

encryptions of 0 with the multi-set of ordered *pairs* of encryptions of 0 and 1. The two elements of the pair must be different, so we have $2^n(2^n-1)$ such pairs. The analysis from § 3.4 carries over with $u = 2^n$ replaced by $u = 2^n(2^n-1)$. So, the conditional probability we are interested in is: $1 - P_{t,2^n(2^n-1)}$.

Summarising, we get

$$\begin{aligned}\mathbb{P}[\mathcal{A}^2_{|t}(\mathcal{S}_0) = 1] &= 1 - P_{t,2^n\,(2^n-1)} \quad \text{and} \\ \mathbb{P}[\mathcal{A}^2_{|t}(\mathcal{S}_{1,v}) = 1] &= (1 - P_{t,2^k}) + P_{t,2^k}(1 - P_{t,2^n(2^n-1)}) \ ,\end{aligned}$$

which we combine into

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^2_{|t}) = P_{t,u} \cdot (1 - P_{t,v}) \tag{31}$$

where

$$u = 2^n\,(2^n - 1) \quad \text{and} \quad v = 2^k \ . \tag{32}$$

Going back to (5), with the bounds given in § 2.2 we get

$$e^{-\frac{(t-1)^2}{2\,u}}\left(1 - e^{-\frac{t^2}{2\,v}}\right) \geqslant \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^2_{|t}) \geqslant e^{-\frac{t^2}{2\,u}}\left(1 - e^{-\frac{(t-1)^2}{2\,v}}\right) \ .$$

We can define $\mathfrak{f}(t)$ as in (8) with u defined as in (32). Lemma 3 and its proof also remains valid and in particular $\mathfrak{f}'(t) = 0$ for $t > 1$ if and only if (12) is satisfied. The entire analysis up to (14) included remains valid without changes.

The case $u = v$ has minor changes. Since $u = 2^n(2^n-1) \approx 2^{2\,n}$, when $k = 2\,n$ we can continue as in the treatment of the case $u = v$ of the proof of Theorem 1. This means that

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t_0}) \approx \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$$

however t_0 is much larger now, i.e., by (13) with the new value of u

$$t_0 \approx \sqrt{2\ln 2} \cdot 2^n \approx 1.17741\ldots \cdot 2^n \ .$$

This implies that an IBC with a block size of n and double index size, i.e., $2\,n$ can be distinguished from truly random permutations in time $O(2^n)$.

Remark 8. To better understand the impact of this result: it seems to be a common understanding that a block cipher with a key size of k bits should require an exhaustive search to be secure. However, even doubling the key size is not sufficient against our distinguishing attack.

5.2 The Case of General d

So far in this section we have considered an Adversary who would ask encryptions of 0 and 1. We now consider an Adversary who will ask encryptions of 0, 1, …, $d-1$. Adversary and Oracle execute Protocol 1 with Strategy 3.

To simplify our analysis we assume that d is a constant (i.e., independent of n). The previous analysis carries over mostly unchanged. In the case of **Way B**, we only have to consider d-tuples instead of pairs. Then, (31) generalises into:

$$\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t}) = P_{t,u} \cdot (1 - P_{t,v}) \ , \tag{33}$$

where

$$u = 2^n(2^n - 1)(2^n - 2) \cdots (2^n - d + 1) \ . \tag{34}$$

With this, the rest of the proof of Lemma 1 carries over verbatim, so we get

$$e^{-\frac{(t-1)^2}{2u}} \left(1 - e^{-\frac{t^2}{2v}}\right) \geqslant \mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t}) \geqslant e^{-\frac{t^2}{2u}} \left(1 - e^{-\frac{(t-1)^2}{2v}}\right) \tag{35}$$

with u defined as in (34). We also still obtain $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t_0}) \approx 1/4$, but t_0 is $O(2^{dn/2})$ and $k = d\,n$. Similarly, also the results in Section 4 hold. We have thus proved the following result.

Theorem 3. *Let $\mathcal{A}^d$ be an Adversary executing Protocol 1 against the Oracle $\mathcal{O}$. $\mathcal{A}^d$ follows Strategy 3, with parameters n, k, d, and $t \in \mathbb{N}$. Put $u = 2^{dn}$ and $v = 2^k$ instead of (2). Then, the results of Theorem 1, Corollary 1, and Theorem 2 all hold also with the more general definition of u.*

Remark 9. Note that we never compare O^i_a with O^j_b for $a \neq b$. In fact, all our distinguishers and their analysis work also assuming that the sets of permutations used to encrypt different (but fixed!) messages are different as well, and in this case it is the *set* of permutations applied to 0, 1, etc. that is selected by the index. This allows to directly consider modes of operation that further change the permutation applied to each block in a deterministic and message-independent way such as OCB, GCM [35], XEX, Counter-in-Tweak [38], and so on.

Note, that being the messages blocks of which we compare the encryptions fixed in advance, even this condition on the permutation being message-independent can be lifted. If the mode of operation has two passes where the output of the first is a ν-bit value that is used to nonce the second pass (as in synthetic IV modes [40,37], for instance GCM-SIV [23]), this means that the message itself will contribute up to ν bits to the cumulative index length. Also for basic GCM, the value ν is not larger than 96 even if the IV is longer, since in that case it must be hashed to 96 bits before use.

6 Parameters to Satisfy Security Definitions

Clearly, ideal cipher parameters must take other attacks than distinguishing attacks into account. A classical attack is the Codebook Attack [28] in which the encryptions of different texts for a fixed index are exhaustively collected.

From now on we shall therefore assume that we want an IBC which is secure against a Codebook Attack, so, we assume $n \geqslant \ell$. For the same reason we bound the *time* complexity of an attack to $O(2^n)$, which is the time to build a Codebook

for a given index. (We are not assuming *a priori* that $k \geqslant \ell$ since the index space is possibly larger than the key space, brute forcing the keys can be done for a known nonce/IV, and thus take time smaller than 2^k.)

Furthermore, d can be bounded in terms of the other parameters.

Proposition 1. *For our distinguishers we can assume w.l.o.g. that*

$$d \leqslant \left\lceil \frac{k+\ell}{n} \right\rceil \quad . \tag{36}$$

Proof. It is easy to see that the difference between the advantages of two adversaries $\mathcal{A}^{d'}$ and $\mathcal{A}^{d''}$ with $d'' > d' \geqslant \lceil \frac{k+\ell}{n} \rceil$, being all other parameters equal, is negligible, i.e. $O(2^{-\ell})$. This is comes from the fact that if $d' \geqslant \lceil \frac{k+\ell}{n} \rceil$, then a collision between two requests performed by $\mathcal{A}^{d'}$ implies that the indices are the same with likelihood at least $1 - 2^{-\ell}$. This implies that a complete security analysis can be performed even if restricting d to satisfy (36). □

Proposition 2. *For our distinguishers, when studying TATO security we can assume w.l.o.g. that*

$$d \leqslant \left\lceil \frac{k}{n} \right\rceil \quad . \tag{37}$$

Proof. By Theorem 3, Theorem 2 states that the TATO of our Attacker is $\Theta(2^{k-\frac{dn}{2}})$ if $k \geqslant dn$ and $\Theta(2^{\frac{dn}{2}})$ if $k < dn$. Hence, if d' is the largest number such that $k \geqslant d'n$, the TATO will not decrease further for $d > d'$. □

6.1 Indistinguishability

Theorem 4. *Let us consider an IBC with n-bit blocks and k-bit index. In order for the IBC to have security of ℓ bits according to Definition 1 and against a Codebook Attack, the parameters n and k must satisfy*

$$k \geqslant 3\ell \qquad \textit{and} \qquad n \geqslant \ell \ .$$

Remark 10. This result is particularly broad in light of Remark 9: if a n-bit block cipher based encryption algorithm wants to achieve strict n-bit security, the index length shall be at least $3n$.

Proof. We start by discussing the case that d (see § 5.2) is a constant, and then later we do a sanity check that this case is valid. Since

$$u = 2^{dn} + O\big(2^{(d-1)n}\big)$$

we can use this approximation to analyse (33). We first have the following lemma.

Lemma 6. *Let t_0 be the value of t for which $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t})$ is maximum and let the Adversary be bounded above by $O(2^\ell)$ queries. In order to determine when $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t})$ is always negligible,* if $t_0 < 2^\ell$, then *we need to check that $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t_0})$ is negligible,* otherwise, *that $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|2^\ell})$ is negligible.*

Proof. From the proof of Lemma 3 we know that the function $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t})$ in t has one maximum and that the function is concave. So, the case $t_0 \leqslant 2^\ell$ is trivial. Now when $t_0 > 2^\ell$, then using $t = t_0$ to perform the attack is beyond the resources of the bounded Adversary. Since the function is concave, the time $t = 2^\ell$ will give the Adversary the largest advantage obtainable. □

We resume the Proof of Theorem 4. Using Lemma 6 we now analyse how to ensure $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t})$ to be negligible.

Case 1 when $t_0 < 2^\ell$. We have two subcases, being:

Case 1 (a) when $v \geqslant u$, which when taking $u = 2^{dn}$ and $v = 2^k$ gives:

$$d\,n \leqslant k \qquad \text{and} \qquad t_0 \approx \sqrt{2^{dn+1}} < 2^\ell \ . \tag{38}$$

In other words, $d\,n + 1 < 2\,\ell$. We need to check when $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t_0})$ will be negligible, in other words using the left inequality in (35) and approximating by taking $u = 2^{dn}$ we need

$$e^{-\frac{(\sqrt{2^{d\,n+1}}-1)^2}{2\cdot 2^{d\,n}}}\left(1 - e^{-\frac{2^{d\,n+1}}{2\cdot 2^k}}\right)$$

to be negligible when the conditions in (38) are satisfied, which means that $1 - e^{-\frac{2^{d\,n+1}}{2\cdot 2^k}}$ should be negligible. *This will happen when* $k \geqslant d\,n + \ell$. Note that k is independent of d and negligibility should hold for all d. Now note that when we have $k \geqslant n + \ell$, and we want to protect against the Codebook Attack, we need $n \geqslant \ell$, giving $k \geqslant 2\,\ell$. For the parameters of n and k being $n \geqslant \ell$ and $k \geqslant n + \ell$, which guarantee the negligibility, we see that when we now consider $d > 1$, that the condition that $t_0 < 2^\ell$ is violated. *So, we will later need to do a sanity check on choosing the parameters* $k \geqslant n + \ell$ and $n \geqslant \ell$.

Case 1 (b) when $u > v$ which with an analysis similar as before, but now using a simplified version of (10) gives:

$$d\,n > k \qquad \text{and} \qquad t_0 \approx \sqrt{2^{k+1}} < 2^\ell \ . \tag{39}$$

In other words, $k + 1 < 2\,\ell$. We then need to check when $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|t_0})$ will be negligible, in other words using the left inequality in (35) and approximating by taking $u = 2^{dn}$ we need

$$e^{-\frac{(\sqrt{2^{k+1}}-1)^2}{2\cdot 2^{d\,n}}}\left(1 - e^{-\frac{2^{k+1}}{2\cdot 2^k}}\right)$$

to be negligible when the conditions in (39) are satisfied. which means that $e^{-\frac{(\sqrt{2^{k+1}}-1)^2}{2\cdot 2^{d\,n}}}$ should be negligible. *This will happen when* $2^k \geqslant 2^{dn+\ell}$, which contradicts with (39). So, this case is void. (Using the more accurate (10) still leads to a void case.)

Case 2 when $t_0 \geqslant 2^\ell$. We have two subcases, being:

Case 2 (a) when $v \geqslant u$, which when taking $u = 2^{dn}$ and $v = 2^k$ gives:

$$d\,n \leqslant k \qquad \text{and} \qquad t_0 \approx \sqrt{2^{dn+1}} \geqslant 2^\ell \ . \tag{40}$$

In other words, $d\,n + 1 \geqslant 2\,\ell$, which implies that $k + 1 \geqslant 2\,\ell$. We then need to check when $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|2^\ell})$ will be negligible, in other words using the left inequality in (35) with $u \approx 2^{dn}$ we need

$$e^{-\frac{(2^\ell-1)^2}{2\cdot 2^{dn}}}\left(1 - e^{-\frac{2^{2\,\ell}}{2\cdot 2^k}}\right)$$

to be negligible when the conditions in (40) are satisfied. Since $d\,n + 1 \geqslant 2\,\ell$, $e^{-\frac{(2^\ell-1)^2}{2\cdot 2^{dn}}}$ can *not* be negligible. That means that we need $k + 1 \geqslant 3\,\ell$ provided that $d\,n \leqslant k$, which will be violated for large d. *So, we will later need to do a sanity check on choosing the parameters $k \geqslant 3\,\ell - 1$ and $n \geqslant \ell$*, the last condition when protecting against the Codebook Attack.

Case 2 (b) when $u > v$ which with an analysis similar as before, but now using a simplified version of (10) gives:

$$d\,n > k \qquad \text{and} \qquad t_0 \approx \sqrt{2^{k+1}} \geqslant 2^\ell \ . \tag{41}$$

In other words, $k + 1 \geqslant 2\,\ell$. We then need to check when $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|2^\ell})$ will be negligible, in other words using the left inequality in (35) and approximating by taking $u = 2^{dn}$ we need

$$e^{-\frac{(2^\ell-1)^2}{2\cdot 2^{dn}}}\left(1 - e^{-\frac{2^{2\,\ell}}{2\cdot 2^k}}\right)$$

to be negligible when the conditions in (41) are satisfied. Trying to make $e^{-\frac{(2^\ell-1)^2}{2\cdot 2^{dn}}}$ negligible leads to a contradiction with (41). So, we need to have $1 - e^{-\frac{2^{2\,\ell}}{2\cdot 2^k}}$ negligible, which implies $k + 1 \geqslant 3\,\ell$, provided $d\,n > k$.

Note that **Case 2 (a)** and **Case 2 (b)** both lead to negligibile advantages. Their discussions could have been merged, but at the price of making the analysis more complicated.

We now summarise the findings and discuss the sanity checks.

First note that the parameters k and n which guarantee security, should only depend on ℓ and be independent of d (see § 5.2), even though our case study was heavily dependent on d. In particular, we assumed that d is a constant, which needs to be checked. We postpone this check until later.

We now proceed with the *sanity checks* we encountered in our case study, which occurred when:

- $k \geqslant n + \ell$ and $n \geqslant \ell$. From **Case 1 (a)** we know that when $d = 1$, the security is satisfied. We now check $d > 1$. As pointed out in **Case 1 (a)**, then $t_0 > 2^\ell$, and so dependent on whether $d\,n \leqslant k$ or $d\,n > k$, we end up respectively in **Case 2 (a)** or **Case 2 (b)**. So, we need $k + 1 \geqslant 3\,\ell$ to make the parameters independent of d.

– $k \geqslant 3\ell - 1$ and $n \geqslant \ell$ in **Case 2 (a)**. It is easy to check from **Case 2 (b)** that this is satisfied.

Finally, we justify why d was chosen as a constant. Fix some $k \geqslant 3\ell$ and $n \geqslant \ell$ and let d vary. In **Case 1 (a)** $d \leqslant 2$, **Case 1 (b)** is a contradiction, in **Case 2**, we use $t = 2^\ell$ and so from (35), we see that increasing d and since $u \approx 2^{dn}$ it decreases $\mathsf{Adv}_{\mathcal{S}_{1,v}}(\mathcal{A}^d_{|2^\ell})$. So, large values of d are useless (i.e. they will not improve advantages). This concludes the proof. □

6.2 TATO Security

In § 5.2 we generalised Theorem 1 and most of its consequences for all $d \geqslant 1$.

We discuss now a generalisation of Corollary 2 for all d.

Theorem 5. *Let $n \geqslant 7$. For the TATO $t/\mathsf{Adv}^d_{\mathcal{S}_{1,v}}(\mathcal{A}_{|t})$ to be at least 2^n for any $d \geqslant 1$ or, in other words, for a n bit IBC with and an index size of k bits to retain a TATO security level of n bits, the parameters n and k must satisfy*

$$k \geqslant 2\,n - c \quad \textit{for some absolute constant } c \ .$$

Proof. Let k_0 be the smallest value of k such that a TATO security level of exactly n bits is attained. We want this value to be at least 2^n in either case. Theorem 2 with Theorem 3 gives:

(a) $k_0 - \frac{dn}{2} + \epsilon = n$ if $k_0 \geqslant d\,n$ with $|\epsilon| < c''$ for some absolute constant c''.
(b) $k_0/2 + \epsilon = n$ if $k_0 \leqslant d\,n$ with $|\epsilon| < c'$ for some absolute constant c'.

In both cases we obtain $d \leqslant 2 + \epsilon/n$, which means that for n sufficiently large it is $d \leqslant 2$ (note that this is substantially the same logic of Proposition 2).

The case $d = 1$ by Corollary 2 implies $k \geqslant \frac{3}{2}n - c$.

Let us consider the case $d = 2$. As in the proof of Corollary 2 we begin with the case $v < u$. Equation (16) holds unchanged, but with $\frac{t_0}{\mathfrak{f}(t_0)} \geqslant 2^n = \sqrt{u}$. From this, we obtain $2\,v \ln\left(1 + \frac{u}{v}\right) > \left(\frac{1}{2}\frac{u\sqrt{u}}{u+v} - 1\right)^2 > \left(\frac{u^{1/2}}{4} - 1\right)^2$. Now $\left(\frac{u^{1/2}}{4} - 1\right)^2 \geqslant \frac{u}{20}$ for any $u \geqslant 37.888$, so we can restrict to this range of u and solve $40 \ln\left(1 + \frac{u}{v}\right) > \frac{u}{v}$. The last inequality (solved numerically) is satisfied for $\frac{u}{v} > 215.013$, and thus, we get that for $u \geqslant 37.888$, which is satisfied already for $n \geqslant 3$, it must be $k \geqslant 2\,n - 7.748$. For the case $v \geqslant u$ we easily get a tautology. Therefore for $d = 2$, we obtain that as long $n \geqslant 3$, it must be $k \geqslant 2\,n - 7.748$. □

7 Conclusions and Open Problems

To prevent a distinguishing attack on n-bit block ciphers, we have shown that to get a security of ℓ bits with $\ell \geqslant n$ we need to choose $2^{3\ell}$ permutations. When we want to exclude Codebook Attacks as well, $n \geqslant \ell$ as well and thus $n = \ell$.

Our paper indicates that a distinguisher having the resources to mount an attack which is time limited to 2^{128} request can distinguish AES-256 with a large

advantage. The security of AES-256 against a mk distinguisher attack seems lower than 128 bits, as this security level would need 384 bit keys, and possibly approach 85 bits (which would be tight it this were also the block size). So, the key lengths in ciphers like the AES should be revised and possibly upgraded if they are to be used in modes of operation that inherit this security degradation.

Even under the weaker requirements that an attack based on our distinguishers shall have complexity at least 2^{128}, 256-bit keys are the minimum for the AES, especially if used in modes that provide another 128 bits of index space. Since we know that in the post-quantum context it is already known that $\ell \leqslant k/2$ due to Grover's algorithm [22], moving to 256 bit keys is already advisable.

Remarks 9 and 10 explain how that these results apply to block cipher modes of operation. The practical impact comes from the observation that, in some real world protocols, messages begin with known or restricted blocks. The result is that in order to guarantee n bits of security in this context a block cipher mode of operation should have a cumulative minimum of $3\,n$ bits of key and nonce/IV material and a minimum of n bits blocks. Considering cryptanalytic attacks to the key only for known nonce/IVs, the underlying cipher should have $2\,n$ bits of key to attain a TATO security level of n bits.

Preliminary versions of these results indeed motivated the choice of key and tweak sizes for the TBC QARMA [1]. QARMA-128, for instance aims at offering at least 128 bits of "tradeoff" security with 256 bit keys. This could be achieved using the theory of FX-constructions and Even-Mansour ciphers to get a (hopefully) solid key schedule with a security proof. There tradeoff means that an attack taking time 2^{128} would require either data or memory to be at least 2^{128} as well. The size of key plus tweak is indeed $3\,n = 384$ bits. The key size is $2\,n = 256$ bits, whence for any fixed tweak TATO security is achieved as well.

Finally, in light of the fact that quantum computers could perform birthday attacks in cubic root time [13], how much could our distinguishing attacks on classical implementations of ciphers be improved on such a machine?

Acknowledgements. Some computations in this paper have been performed with the help of SageMath, the Sage Mathematics Software System, Version 8.7 [43].

References

1. Roberto Avanzi. The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric Even-Mansour constructions with non-involutory central rounds, and search heuristics for low-latency S-Boxes. *IACR Trans. Symmetric Cryptol.*, 2017(1):4–44, 2017.
2. Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 259–274. Springer, 2000.
3. Mihir Bellare and Björn Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016 - Proceedings, Part I*, volume 9814 of *LNCS*, pages 247–276. Springer, 2016.

4. Daniel J. Bernstein. Some challenges in heavyweight cipher design. https://cr.yp.to/talks/2016.01.15/slides-djb-20160115-a4.pdf.
5. Eli Biham. How to decrypt or even substitute DES-encrypted messages in 2^{28} steps. *Inf. Process. Lett.*, 84(3):117–124, 2002.
6. Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Ronald Cramer, editor, *EUROCRYPT 2005, Proceedings*, volume 3494 of *LNCS*, pages 507–525. Springer, 2005.
7. Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In Henri Gilbert, editor, *EUROCRYPT 2010, Proceedings*, volume 6110 of *LNCS*, pages 299–319. Springer, 2010.
8. Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *ASIACRYPT 2009, Proceedings*, volume 5912 of *LNCS*, pages 1–18. Springer, 2009.
9. Alex Biryukov and Dmitry Khovratovich. Feasible attack on the 13-round AES-256. *IACR Cryptology ePrint Archive*, 2010:257, 2010.
10. Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić. Distinguisher and related-key attack on the full AES-256. In Shai Halevi, editor, *CRYPTO 2009, Proceedings*, volume 5677 of *LNCS*, pages 231–249. Springer, 2009.
11. Alex Biryukov, Sourav Mukhopadhyay, and Palash Sarkar. Improved time-memory trade-offs with multiple data. In Bart Preneel and Stafford E. Tavares, editors, *SAC 2005 Workshop Revised Selected Papers*, volume 3897 of *LNCS*, pages 110–127. Springer, 2005.
12. Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Proceedings, Part I*, volume 10820 of *LNCS*, pages 468–499. Springer, 2018.
13. Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In Claudio L. Lucchesi and Arnaldo V. Moura, editors, *LATIN '98: Theoretical Informatics, Third Latin American Symposium, Proceedings*, volume 1380 of *LNCS*, pages 163–169. Springer, 1998.
14. Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin. The random oracle model and the ideal cipher model are equivalent. In David A. Wagner, editor, *CRYPTO 2008, Proceedings*, volume 5157 of *LNCS*, pages 1–20. Springer, 2008.
15. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.
16. Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 393–410. Springer, 2010.
17. William Feller. *An Introduction to Probability Theory and Its Applications*, volume I. Wiley, New York, 1957.
18. Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000 Workshop Proceedings*, volume 1978 of *LNCS*, pages 213–230. Springer, 2000.
19. Pierre-Alain Fouque, Antoine Joux, and Chrysanthi Mavromati. Multi-user collisions: Applications to discrete logarithm, Even-Mansour and PRINCE. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Proceedings, Part I*, volume 8873 of *LNCS*, pages 420–438. Springer, 2014.

20. Shafi Goldwasser and Silvio Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In Harry R. Lewis, Barbara B. Simons, Walter A. Burkhard, and Lawrence H. Landweber, editors, *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, pages 365–377. ACM, 1982.
21. Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.
22. Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.
23. Shay Gueron and Yehuda Lindell. GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015*, pages 109–119. ACM, 2015.
24. Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016 - Proceedings, Part I*, volume 9814 of *LNCS*, pages 3–32. Springer, 2016.
25. Viet Tung Hoang and Stefano Tessaro. The multi-user security of double encryption. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Proceedings, Part II*, volume 10211 of *LNCS*, pages 381–411, 2017.
26. Jin Hong and Palash Sarkar. New applications of time memory data tradeoffs. In Bimal K. Roy, editor, *ASIACRYPT 2005, Proceedings*, volume 3788 of *LNCS*, pages 353–372. Springer, 2005.
27. Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Proceedings, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.
28. John Kelsey, Bruce Schneier, and Niels Ferguson. Yarrow-160: Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In Howard M. Heys and Carlisle M. Adams, editors, *SAC'99 Workshop Proceedings*, volume 1758 of *LNCS*, pages 13–33. Springer, 1999.
29. Jongsung Kim, Seokhie Hong, and Bart Preneel. Related-key rectangle attacks on reduced AES-192 and AES-256. In Alex Biryukov, editor, *FSE 2007 Workshop Proceedings*, volume 4593 of *LNCS*, pages 225–241. Springer, 2007.
30. Moses Liskov and Kazuhiko Minematsu. Comments on XTS-AES (On the Use of Two Keys). https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/xts/xts_comments-liskov_minematsu.pdf, September 2008.
31. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.
32. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. *Journal of Cryptology*, 24(3):588–613, 2011.
33. Atul Luykx, Bart Mennink, and Kenneth G. Paterson. Analyzing multi-key security degradation. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Proceedings, Part II*, volume 10625 of *LNCS*, pages 575–605. Springer, 2017.
34. Luther Martin. XTS: A mode of AES for encrypting hard disks. *IEEE Security & Privacy*, 8(3):68–69, 2010.

35. David A. McGrew and John Viega. The security and performance of the Galois/Counter Mode (GCM) of operation. In Anne Canteaut and Kapalee Viswanathan, editors, *INDOCRYPT 2004, Proceedings*, volume 3348 of *LNCS*, pages 343–355. Springer, 2004.
36. Nicky Mouha and Atul Luykx. Multi-key security: The Even-Mansour construction revisited. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015, Proceedings, Part I*, volume 9215 of *LNCS*, pages 209–223. Springer, 2015.
37. Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton. Reconsidering generic composition. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014, Proceedings*, volume 8441 of *LNCS*, pages 257–274. Springer, 2014.
38. Thomas Peyrin and Yannick Seurin. Counter-in-Tweak: Authenticated encryption modes for tweakable block ciphers. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Proceedings, Part I*, volume 9814 of *LNCS*, pages 33–63. Springer, 2016.
39. Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In Michael K. Reiter and Pierangela Samarati, editors, *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security.*, pages 196–205. ACM, 2001.
40. Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In Serge Vaudenay, editor, *EUROCRYPT 2006, Proceedings*, volume 4004 of *LNCS*, pages 373–390. Springer, 2006.
41. Mahmoud Sayrafiezadeh. The birthday problem revisited. *Mathematics Magazine*, 67(3):220–223, 1994.
42. Stefano Tessaro. Optimally secure block ciphers from ideal primitives. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Proceedings, Part II*, volume 9453 of *LNCS*, pages 437–462. Springer, 2015.
43. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.7)*, 2019. Available from https://www.sagemath.org.
44. Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago*, pages 80–91. IEEE, 1982.
45. Gideon Yuval. How to swindle Rabin. *Cryptologia*, 3(3):187–191, 1979.

A Appendices

A.1 Proof of Lemma 4

We start with some general observations. Clearly, $\mathfrak{h}(t+1) \geqslant \mathfrak{h}(t)$ if and only if $\mathfrak{h}(t)/\mathfrak{h}(t+1) \leqslant 1$. Using (5), we can write

$$\frac{\mathfrak{h}(t)}{\mathfrak{h}(t+1)} = \frac{t}{t+1}\frac{P_{t+1,u}\cdot(1-P_{t+1,v})}{P_{t,u}\cdot(1-P_{t,v})} = \frac{t}{t+1}\left(1-\frac{t}{u}\right)\frac{1-P_{t+1,v}}{1-P_{t,v}} \ ,$$

which is $\leqslant 1$ if and only if

$$\left(1-\frac{t}{u}\right)(1-P_{t+1,v}) \leqslant \left(1+\frac{1}{t}\right)(1-P_{t,v})$$

which, replacing $P_{t+1,v}$ by $\left(1-\frac{t}{v}\right)P_{t,v}$, becomes

$$P_{t,v} \leqslant \mathfrak{L}_{u,v}(t) := \frac{\frac{1}{t}+\frac{t}{u}}{\frac{1}{t}+\frac{t}{u}+\frac{t}{v}-\frac{t^2}{uv}} = \frac{t^2 v + uv}{t^2(u+v)+uv-t^3} \ . \tag{42}$$

Similarly, $\mathfrak{h}(t+1) \leqslant \mathfrak{h}(t)$ is equivalent to

$$P_{t,v} \geqslant \mathfrak{L}_{u,v}(t)$$

and these results hold also with '$<$' and '$>$' in place of '$\leqslant$' and '$\geqslant$' throughout.

Proof of Claim (i). We know that $\mathfrak{h}(t+1) \leqslant \mathfrak{h}(t)$ if and only if $P_{t,v} \geqslant \mathfrak{L}_{u,v}(t)$. Since $P_{t,v} \geqslant e^{-\frac{t^2}{2v}} \geqslant 1-\frac{t^2}{2v}$, it will suffice to prove that for $t < \sqrt{\frac{uv}{u+v}} - 2$ it is

$$1-\frac{t^2}{2v} \geqslant \mathfrak{L}_{u,v}(t) \ ,$$

which simplifies to

$$t^3 - (u+v)t^2 - 2\,v\,t + uv \geqslant 0 \ .$$

Now put

$$\varphi(t) = t^3 - (u+v)t^2 - 2\,v\,t + uv \quad \text{and} \quad \xi = \sqrt{\frac{uv}{u+v}} \ .$$

We claim that the three roots of $\varphi(t)=0$ lie in the following disjoint intervals

$$\rho_0 \in (-\infty, 0), \quad \rho_1 \in (\xi-2, \xi), \quad \text{and} \quad \rho_2 \in (u+v, \infty) \ . \tag{43}$$

We first note that these intervals are indeed disjoint: it is easily verified that $\xi > 2$ (because $u, v > 8$) and that $\xi < \sqrt{u} < u+v$. Now, being $\varphi(t)$ monic of degree 3, (43) will imply that $\varphi(t)$ is positive over the interval (ρ_0, ρ_1) and in particular over $[0, \xi-2]$. We shall establish (43) by proving that: (a) $\varphi(0) > 0$; (b) $\varphi(\xi-2) > 0$; (c) $\varphi(\xi) < 0$; and (d) $\varphi(u+v) < 0$. The arguments follow:

(a) It is $\varphi(0) = uv > 0$.
(b) Observe that

$$\varphi(\xi-2) = \xi^3 - (u+v+6)\xi^2 + 2\,\xi(2\,u+v+6) + (uv - 4\,u - 8) > 0$$

if and only if

$$\xi\left[\xi^2 + 2\,(2\,u+v+6)\right] > \xi^2(u+v+6) - (uv - 4\,u - 8)$$

i.e., replacing ξ^2 with $\frac{uv}{u+v}$:

$$\xi\,[uv + 2\,(2\,u+v+6)(u+v)] > uv(u+v+6) - (uv - 4\,u - 8)(u+v) \ ,$$

or

$$\xi > \frac{4\,u^2 + 10\,uv + 8\,(u+v)}{2\,v^2 + 4\,u^2 + 7\,uv + 12\,(u+v)} \ . \tag{44}$$

Upon squaring and replacing ξ^2 with $\frac{uv}{u+v}$ again, (44) becomes

$$\begin{aligned} 16\,u^5(v-1)+8\,(7\,v^2-8)\,u^4+(65\,v^3+84\,v^2-144\,v-64)\,u^3+\\ +4\,v(7\,v^3+29\,v^2-24\,v-48)\,u^2+\\ +4\,v^2(v^3+12\,v^2-4\,v-48)\,u-64\,v^3>0\ . \end{aligned} \tag{45}$$

Now, for $u,v>8$, we see that all coefficients of the powers of u are non-negative. Considering the coefficient of u^3, if we subtract v^3 from it we obtain $64\,v^3+84\,v^2-144\,v-64$ which is also positive. The sum of the difference and of the known term, $v^3u^3-64\,v^3$ is positive as well. Hence (45) is strictly positive.

(c) It is $\varphi(\xi)=\xi^3-(u+v)\frac{v}{u+v}\,u-2\,v\xi+uv=\xi\left(\frac{u}{u+v}-2\right)v<0$.

(d) Clearly, $\varphi\,(u+v)=-(u+2\,v)v<0$.

We have established that $\varphi(t)$ is positive for $0\leqslant t\leqslant\xi-2$ and thus $\mathfrak{h}(t)$ is decreasing over the same interval, which is Claim (i). □

Proof of Claim (ii). Since $P_{t,v}\leqslant e^{-\frac{t(t-1)}{2v}}<\left(1+\frac{t(t-1)}{2v}\right)^{-1}=\frac{2v}{2v+t(t-1)}$ it will suffice to prove that

$$\frac{2v}{2v+t(t-1)}<\mathfrak{L}_{u,v}(t) \tag{46}$$

for $t>\sqrt{u}$: indeed, (46) is easily seen to be equivalent to $t^2-u>0$ if $t<u,v$. □

Proof of Claim (iii). We proceed as in Claim (ii) but we need a tighter estimate

$$P_{t,v}\leqslant e^{-\frac{t(t-1)}{2v}}<\mathfrak{M}_v(t):=\left(1+\frac{t(t-1)}{2v}+\frac{1}{2}\left(\frac{t(t-1)}{2v}\right)^2\right)^{-1}\ .$$

If we can prove that $\mathfrak{L}_{u,v}(t)\geqslant\mathfrak{M}_v(t)$, this will a fortiori imply that $\mathfrak{L}_{u,v}(t)\geqslant P_{t,v}$. Let us study then when

$$\begin{aligned} &\mathfrak{L}_{u,v}(t)-\mathfrak{M}_v(t)=\\ &\quad=\frac{tv\left(t^5-2t^4+t^3(1+u+4\,v)+t^2(4\,v-2\,u)-tu(4\,v-1)-4\,uv\right)}{(t^4-2t^3+t^2(4\,v+1)-4tv+8v^2)\,(t^2(u+v)+uv-t^3)}\geqslant 0\ . \end{aligned}$$

For $2\leqslant t\leqslant u,v$, the sign of $\mathfrak{L}_{u,v}(t)-\mathfrak{M}_v(t)$ is equal to the sign of

$$\psi_{u,v}(t):=t^5-2\,t^4+t^3(1+u+4\,v)+t^2(4\,v-2\,u)-tu(4\,v-1)-4\,uv\ .$$

Put $t_1=2\,\sqrt{v}+\frac{3}{2}$ and let us compute $\psi_{u,v}(t)$ at $t=t_1$:

$$\begin{aligned} \psi_{u,v}\left(2\,\sqrt{v}+\frac{3}{2}\right)=\frac{1}{32}\big(2048\,v^{5/2}+5632\,v^2+5440\,v^{3/2}+2160\,v+\\ +(112\,u+324)\sqrt{v}+(12\,u+27)\big)>0\ . \end{aligned}$$

Note that $\psi_{u,v}(2\sqrt{v}+a)$ becomes negative for $u \gg v$ for any $a \leqslant \frac{3}{2}$. This implies that also the coefficient 2 of $\sqrt{v}$ is tight.

We want to prove that $\psi_{u,v}(t)$ is positive for all $t \geqslant t_1$. Note that

$$\begin{aligned}
\frac{\partial}{\partial t}\psi_{u,v}(t) &= 5\,t^4 - 8\,t^3 + 3\,t^2(u+4\,v+1) - 4\,t(u-2\,v) + u - 4\,uv \ , \\
\frac{\partial}{\partial t}\psi_{u,v}(t_1) &= \frac{1}{16}\big(128\,uv + 160\,u\sqrt{v} + 28\,u + \\
&\qquad + 2048\,v^2 + 4224\,v^{3/2} + 2832\,v + 720\sqrt{v} + 81\big) > 0 \ , \ \text{and} \\
\frac{\partial^2}{\partial t^2}\psi_{u,v}(t) &= 20t^3 - 24t^2 + 6\,t(u+4\,v+1) + 4\,(2\,v-u) \\
&= 4\,t^2(5\,t-6) + u(6\,t-4) + 6\,t(4\,v+1) + 8\,v \ .
\end{aligned}$$

The second derivative of $\psi_{u,v}(t)$ is always positive for $t \geqslant 2$, regardless of u, v (recall $u, v > 0$). Then, the first derivative of $\psi_{u,v}(t)$ is always increasing for $t \geqslant 2$, and since it is positive for $t = t_1$, then it is always positive for all $t \geqslant t_1$. Similarly, since $\psi_{u,v}(t) > 0$ holds for $t = t_1$, then it holds for all $t \geqslant t_1$. This completes the proof. □

A.2 Proof of Lemma 5

Proof. Let us define

$$\overline{\mathfrak{g}}(t) = \frac{t}{e^{-\frac{t^2}{2\,u}}\left(1 - e^{-\frac{(t-1)^2}{2\,v}}\right)} \quad \text{and} \quad \underline{\mathfrak{g}}(t) = \frac{t}{e^{-\frac{(t-1)^2}{2\,u}}\left(1 - e^{-\frac{t^2}{2\,v}}\right)}$$

where clearly

$$\overline{\mathfrak{g}}(t) > \mathfrak{g}(t), \mathfrak{h}(t) > \underline{\mathfrak{g}}(t)$$

with $\mathfrak{h}(t)$ and $\mathfrak{g}(t)$ defined as in (19).

We want to give lower bounds for

$$\frac{\underline{\mathfrak{g}}(t)}{\overline{\mathfrak{g}}(t)} = \frac{e^{-\frac{t^2}{2\,u}}}{e^{-\frac{(t-1)^2}{2\,u}}} \cdot \frac{1 - e^{-\frac{(t-1)^2}{2\,v}}}{1 - e^{-\frac{t^2}{2\,v}}} = e^{-\frac{2\,t-1}{2\,u}} \cdot \frac{1 - e^{-\frac{(t-1)^2}{2\,v}}}{1 - e^{-\frac{t^2}{2\,v}}} \ . \tag{47}$$

Note that $t \mapsto e^{-\frac{2\,t-1}{2\,u}}$ is monotonically decreasing in t and $t \mapsto \frac{1-e^{-\frac{(t-1)^2}{2\,v}}}{1-e^{-\frac{t^2}{2\,v}}}$ is monotonically increasing for $t \geqslant 1$ with limit at infinity equal to 1.

We distinguish two cases: (a) $v \geqslant u$; (b) $v < u$; For both cases we first determine intervals on which to evaluate the TATO and (47), and which are comfortable for the computations, and then perform these evaluations.

Case (a): $v \geqslant u$. Consider the interval $I_a = [\,\xi - 2, \sqrt{u}\,] = [\,(1-\epsilon_a)\sqrt{u} - 2, \sqrt{u}\,]$. The limit of ϵ_a is easily proven: $\epsilon_a = 1 - \sqrt{\frac{v}{u+v}} = 1 - \sqrt{\frac{1}{1+u/v}} < \frac{u}{2\,v}$. This implies that ϵ_a can be taken arbitrarily small for fixed u and sufficiently large v (for instance, when increasing key length for a fixed block length) or when $v = u^s$

for $s > 1$ (such as when the ratio of key length to block length is fixed and we study the asymptotic behaviour). For the upper bound for (47) we have

$$\frac{\underline{\mathfrak{g}}(t)}{\overline{\mathfrak{g}}(t)} \geqslant e^{-\frac{1}{\sqrt{u}}} \cdot \frac{1 - e^{-\frac{\left(\sqrt{\frac{uv}{u+v}}-3\right)^2}{2v}}}{1 - e^{-\frac{\left(\sqrt{\frac{uv}{u+v}}-2\right)^2}{2v}}} \geqslant e^{-\frac{1}{\sqrt{u}}} \cdot \frac{1 - e^{-\frac{\left(\sqrt{\frac{u}{2}}-3\right)^2}{2v}}}{1 - e^{-\frac{\left(\sqrt{\frac{u}{2}}-2\right)^2}{2v}}}$$
$$\geqslant \left(1 - \frac{1}{\sqrt{u}}\right)\left(\frac{\sqrt{\frac{u}{2}} - 3}{\sqrt{\frac{u}{2}} - 2}\right)^2 \left(1 - \frac{9\,u}{128\,v}\right) \tag{48}$$

for $u, v \geqslant 32$ (see Appendix A.3), and $\left(\frac{\sqrt{u}-3\sqrt{2}}{\sqrt{u}-2\sqrt{2}}\right)^2 = 1 - \frac{2\sqrt{2}}{\sqrt{u}} - \frac{6}{u} - \frac{8\sqrt{2}}{u^{3/2}} - \frac{16}{u^2} + \frac{128}{u^3} - \cdots \geqslant 1 - \frac{5}{\sqrt{u}}$ for $u \geqslant 18$, hence

$$\geqslant \left(1 - \frac{1}{\sqrt{u}}\right)\left(1 - \frac{5}{\sqrt{u}}\right)\left(1 - \frac{9\,u}{128\,v}\right) \geqslant \left(1 - \frac{6}{\sqrt{u}}\right)\left(1 - \frac{9\,u}{128\,v}\right) \quad .$$

Case (b): $v < u$. We evaluate over the interval $I_b = \left[(1-\epsilon_b)\sqrt{v}, 2\sqrt{v} + \frac{3}{2}\right]$. The statement about ϵ_b is proved exactly as the limit of ϵ_a, where u and v are swapped. We obtain the following bound (see Appendix A.3):

$$\frac{\underline{\mathfrak{g}}(t)}{\overline{\mathfrak{g}}(t)} \geqslant e^{-\frac{2\sqrt{v}+\frac{3}{2}}{u}} \cdot \frac{1 - e^{-\frac{\left(\sqrt{\frac{uv}{u+v}}-3\right)^2}{2v}}}{1 - e^{-\frac{\left(\sqrt{\frac{uv}{u+v}}-2\right)^2}{2v}}} \geqslant \left(1 - \frac{2\sqrt{v} + \frac{3}{2}}{u}\right)\left(\frac{\sqrt{\frac{v}{2}} - 3}{\sqrt{\frac{v}{2}} - 2}\right)^2$$
$$\geqslant \left(1 - \frac{3}{\sqrt{v}}\right)\left(1 - \frac{5}{\sqrt{v}}\right)\left(1 - \frac{9\,v}{128\,u}\right) \geqslant \left(1 - \frac{8}{\sqrt{v}}\right)\left(1 - \frac{v+1}{256\,u}\right) \quad . \tag{49}$$

For both cases we thus have proved that $\frac{\underline{\mathfrak{g}}(t)}{\overline{\mathfrak{g}}(t)} \geqslant 1 - c$ with c defined as in (21). Now, $\overline{\mathfrak{g}}(t) - \underline{\mathfrak{g}}(t) \geqslant c \cdot \overline{\mathfrak{g}}(t)$ and thus $\mathfrak{g}(t) \geqslant (1-c) \cdot \overline{\mathfrak{g}}(t)$. Turning to (20), we note that, since both $\mathfrak{h}(t)$ and $\mathfrak{g}(t)$ lie between $\overline{\mathfrak{g}}(t)$ and $\underline{\mathfrak{g}}(t)$, we have $|\mathfrak{h}(t) - \mathfrak{g}(t)| \leqslant c\,\overline{\mathfrak{g}}(t) \leqslant \frac{c}{1-c}\,\mathfrak{g}(t)$ which implies $\mathfrak{h}(t) = \mathfrak{g}(t)\left(1 + O\left(\frac{c}{1-c}\right)\right)$, but since $1 - c$ is bounded from below by $\frac{3}{16}$, it is $O\left(\frac{c}{1-c}\right) = O(c)$ and (20) follows. □

A.3 Proof of Bounds (48) and (49)

Consider the function

$$\gamma(x) = \frac{1 - e^{-\frac{(x-a)^2}{w}}}{1 - e^{-\frac{(x-b)^2}{w}}}$$

with $a, b \geqslant 0$ for $x \geqslant a, b$. It is straightforward to show that $\gamma(x)$ is increasing if $a > b$ and decreasing if $a < b$. We apply this fact to $x = \sqrt{\frac{uv}{u+v}}$, $a = 3$ and $b = 2$. We see that the function has smaller values for smaller values of x.

Assume that $v \geqslant u$. Then $\frac{uv}{u+v} \geqslant \frac{u}{2}$ and

$$\frac{1-e^{-\frac{(\xi-3)^2}{2\,v}}}{1-e^{-\frac{(\xi-2)^2}{2\,v}}} \geqslant \frac{1-e^{-\frac{\left(\sqrt{\frac{u}{2}}-3\right)^2}{2\,v}}}{1-e^{-\frac{\left(\sqrt{\frac{u}{2}}-2\right)^2}{2\,v}}} = (*) \ .$$

Now we use the inequalities $1-e^{-x} \geqslant x(1-\frac{x}{2})$ and $\frac{1}{1-e^{-x}} \geqslant \frac{1}{2}+\frac{1}{x}$ and

$$\begin{aligned}
(*) &\geqslant \frac{\left(\sqrt{\frac{u}{2}}-3\right)^2}{2\,v}\left(1-\frac{\left(\sqrt{\frac{u}{2}}-3\right)^2}{4\,v}\right)\left(\frac{1}{2}+\frac{2\,v}{\left(\sqrt{\frac{u}{2}}-2\right)^2}\right) \\
&\geqslant \frac{\left(\sqrt{\frac{u}{2}}-3\right)^2}{\left(\sqrt{\frac{u}{2}}-2\right)^2}\left(1-\frac{u}{8\,v}\right)\left(1+\frac{\left(\sqrt{\frac{u}{2}}-2\right)^2}{4\,v}\right) \\
&\geqslant \frac{\left(\sqrt{\frac{u}{2}}-3\right)^2}{\left(\sqrt{\frac{u}{2}}-2\right)^2}\left(1-\frac{u}{8\,v}\right)\left(1+\frac{u}{16\,v}\right) > \left(\frac{\sqrt{\frac{u}{2}}-3}{\sqrt{\frac{u}{2}}-2}\right)^2\left(1-\frac{9\,u}{128\,v}\right)
\end{aligned}$$

the last approximation holding because $0 < \frac{u}{v} \leqslant 1$.

Bound (49) follows by swapping u with v. □