CTET+: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation

Benoît Cogliati, Jordan Ethan, Virginie Lallemand, Byeonghak Lee, Jooyoung Lee, Marine Minier

IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2021, No. 4, pp. 1–35. DOI:10.46586/tosc.v2021.i4.1-35

CTET$^+$: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation

Benoît Cogliati[1], Jordan Ethan[1], Virginie Lallemand[2], Byeonghak Lee[3], Jooyoung Lee[3] and Marine Minier[2]

[1] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
benoit.cogliati@cispa.de, jordan.ethan@cispa.de
[2] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
virginie.lallemand@loria.fr, marine.minier@loria.fr
[3] Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea
lbh0307@kaist.ac.kr, hicalf@kaist.ac.kr

Abstract. In this work, we propose a construction of 2-round tweakable substitution-permutation networks using a single secret S-box. This construction is based on non-linear permutation layers using independent round keys, and achieves security beyond the birthday bound in the random permutation model. When instantiated with an n-bit block cipher with κ-bit keys, the resulting tweakable block cipher, dubbed CTET$^+$, can be viewed as a tweakable enciphering scheme that encrypts wn-bit messages for any integer $w \geq 2$ using $5n + \kappa$-bit keys and n-bit tweaks, providing $2n/3$-bit security.
Compared to the 2-round non-linear SPN analyzed in [CDK+18], we both minimize it by requiring a single permutation, and weaken the requirements on the middle linear layer, allowing better performance. As a result, CTET$^+$ becomes the first tweakable enciphering scheme that provides beyond-birthday-bound security using a single permutation, while its efficiency is still comparable to existing schemes including AES-XTS, EME, XCB and TET. Furthermore, we propose a new tweakable enciphering scheme, dubbed AES$_6$-CTET$^+$, which is an actual instantiation of CTET$^+$ using a reduced round AES block cipher as the underlying secret S-box. Extensive cryptanalysis of this algorithm allows us to claim 127 bits of security.
Such tweakable enciphering schemes with huge block sizes become desirable in the context of disk encryption, since processing a whole sector as a single block significantly worsens the granularity for attackers when compared to, for example, AES-XTS, which treats every 16-byte block on the disk independently. Besides, as a huge amount of data is being stored and encrypted at rest under many different keys in clouds, beyond-birthday-bound security will most likely become necessary in the short term.

Keywords: tweakable enciphering mode · SPN · beyond-birthday-bound security

1 Introduction

Background. Block ciphers are mainly built around a complex function or permutation on a small domain, which is then extended to a keyed permutation on a larger domain by iterating simple rounds. This is usually achieved by relying on generic structures, which are often either Feistel networks or Substitution-Permutation Networks (SPNs). SPNs can be used to design a block cipher with message space $\{0,1\}^{wn}$ from a small number of n-bit permutations as follows:

Received: 2021-09-01 Accepted: 2021-11-01 Published: 2021-12-03

- iterate the following simple steps:
  - apply a keyed permutation layer to the whole wn-bit state;
  - break down the state into w n-bit blocks;
  - compute an S-box on each block of the state;
- after the last round, apply a keyed permutation layer to the whole wn-bit state.

Block ciphers following the SPN approach include AES [AES01], Serpent [BAK98] and PRESENT [BKL$^+$07]. In order to study the security of those algorithms, it is customary to prove the soundness of the high-level structure in a relevant security model.

Security of SPNs. The first articles investigating the security of SPNs model S-boxes as *secret* random permutations; Iwata and Kurosawa [IK00] showed an attack against 2-round SPNs and proved security for 3-round SPNs against non-adaptive adversaries when used with the linear permutation layer from the SERPENT block cipher. Miles and Viola [MV15] studied the security of various SPN-like block ciphers, but their bound gets worse as the number of rounds of the block cipher increases. They also analyzed the security of several SPNs using the AES S-box against various classes of attacks, notably differential and linear attacks.

In the *public* permutation model, Dodis et al. [DKS$^+$17] proved the birthday-bound security for linear and non-linear SPNs using a single public S-box. Later, Cogliati et al. [CDK$^+$18] studied tweakable SPNs when S-boxes for each round are uniformly random and independent. In particular, they proved that the security of a non-linear tweakable SPN is beyond-birthday-bound when the number of rounds is greater than two, and grows towards optimal security with the number of rounds.

Tweakable Enciphering Schemes. SPNs can be viewed as a domain extender for block ciphers [CS06b, Hal07]. Indeed, the underlying S-box can be replaced by another block cipher (e.g. with a public random key) or a large permutation in order to obtain a wide block cipher. In other words, (tweakable) SPNs can be seen as (tweakable) enciphering modes of operations. Various such schemes have been proposed with application to disk encryption, where the design principles are classified into three approaches; encrypt-mix-encrypt [HR03, HR04, Hal04], hash-ECB-hash [CS06b, Hal07], and hash-CTR-hash [WFW05, CS06a, FM07]. All these constructions typically accept inputs of variable length, and their security is proved up to the birthday bound in the secret permutation model. 2-round SPNs can be viewed as extending the hash-ECB-hash approach, or more precisely, the hash-ECB-hash-ECB-hash approach.

1.1 Our Contribution

Beyond-Birthday-Bound Security of Single S-box-based SPNs. In this work, we focus on the security of two-round SPNs using a *single* S-box, where the S-box is modeled as a secret random permutation. In particular, we study the case where $w \geq 2$, since, when $w = 1$, we recover the standard Even-Mansour construction that has already been the focus of a long line of work [EM97, CS14, CLL$^+$14, HT16]. Our first contribution is to prove beyond-birthday-bound multi-user security for the 2-round tweakable SPN structure with a single S-box and independent round keys, with the added benefit that the inner linear permutation can be far simpler than the outer linear permutations. More specifically, we rely on the H-coefficients technique [Pat08] and on computational techniques from [CLL$^+$14, GSWG18, HT16] to prove that the security level of this construction is roughly equivalent to the one of the 2-round SPN structure with *two independent* S-boxes and a strong inner linear layer; Theorem 1 indicates that the multi-user advantage of any

adversary will be small as long as the number of queries she issues is small in front of $2^{2n/3}$.

A New Tweakable Enciphering Scheme. Our security proof is information-theoretic, and hence it has an inherent limit that the security level cannot go beyond the size of the underlying S-box. In the case of real block ciphers, which are based on very small S-boxes and use many rounds, our results might be too weak to provide any insight.

However, when the underlying S-box is instantiated with a secure block cipher such as AES, our construction can be viewed as a tweakable enciphering scheme that encrypts wn-bit messages for any integer $w \geq 2$ using $5n$-bit keys (plus one AES key) and n-bit tweaks, providing $2n/3$-bit security. In this context, we propose an efficient tweakable permutation in the inner permutation layer (as defined in Section 2.2), which might be of independent interest from a practical point of view. To the best of our knowledge, the resulting scheme, dubbed CTET^+, becomes the first tweakable enciphering scheme that provides beyond-birthday-bound security (with respect to the size of the underlying block cipher) using only a single permutation.

A New Wide Tweakable Block Cipher. While our generic construction can be seen as a domain extender for block ciphers, it may also be used as a generic structure to design tweakable block ciphers with a huge block size. Such a block cipher is very useful in the context of disk encryption, where disk sectors are seen as blocks. We propose an actual instantiation dubbed $\mathsf{AES}_6\text{-}\mathsf{CTET}^+$, which uses the block cipher AES-128 reduced to 6 rounds as an underlying S-Box. We justify this choice by extensive cryptanalysis, showing that the good cryptographic properties of 6-round AES combined with the strength of the first and last tweakable permutations lead to the desired security level. In particular, we payed special attention to the yoyo technique [RBH17] and showed that it cannot be extended to our construction.

Implementation Results. Table 1 compares the CTET^+ scheme to well-known constructions XTS [IEE08, Dwo10], EME [HR04], XCB [FM07] and TET [Hal07]. When it comes to efficiency, we implemented all the constructions using AES, and our experiments are done in the Skylake microarchitecture (i7-6700 CPU @ 3.40GHz) which support PCLMUL, AVX, SSE and AES instructions. We used GNU C Compiler 7.4.0 in O2 optimization level. We checked out the performance on 512 bytes with $w = 32$ (which is the traditional sector size) and 4096 bytes with $w = 256$ (which is the standard page size of Linux, and the sector size of modern hard drives and flash drives). Execution time is measured by the average number of core clocks for at least 2^{24} runs using the RDPMC (Read Performance Monitoring Counters) instruction. In order to make a fair comparison, we implemented EME (instead of the IEEE P1619.2 standard EME^*) and a simplified version of XCB without using partial blocks. All variables that can be precomputed were computed at the key scheduling time, and this time was ignored in the benchmark.

AES-XTS is the fastest, while we note that AES-XTS is not a strong pseudorandom permutation as a wide block cipher, providing only a weaker notion of security; a modification to a single n-bit block will affect only the corresponding n-bit block in the ciphertext. Overall, the efficiency of $\mathsf{AES}_6\text{-}\mathsf{CTET}^+$ is comparable to the existing schemes. With the cost of memory consumption, $\mathsf{AES}_6\text{-}\mathsf{CTET}^+$ will become faster for a larger value of w as the portion of a constant amount of the computational overload becomes negligible. The main drawback of our scheme seems to be the large key size when compared with other candidates. However, we stress that keys can be derived from a single seed, on a case-by-case basis. For example, if the keys are derived from a password, this step can be left to the key-derivation algorithm. In the case of disk encryption, a full uniformly random key can easily be stored on the disk (e.g. as is currently done in LUKS headers).

Table 1: Comparison of different tweakable enciphering schemes. XTS, EME, XCB and TET are based on an n-bit block cipher using κ-bit keys, while CTET$^+$ is based on an n-bit permutation. The efficiency is estimated when they are instantiated with AES-128. AES$_6$-CDK denotes the generic 2-round SPN construction from [CDK+18] using AES$_6$ as a public permutation.

Scheme	Key size	Security	Efficiency (cycles/byte)		References
			512 bytes	4096 bytes	
XTS	2κ	$n/2$	0.80	0.66	[IEE08, Dwo10]
EME	κ	$n/2$	1.66	1.50	[HR04]
XCB	κ	$n/2$	1.40	1.15	[FM07]
TET	2κ	$n/2$	1.49	1.47	[Hal07]
AES$_6$-CDK	$6n$	$2n/3$	1.91	1.83	[CDK+18]
AES$_6$-CTET$^+$	$5n + \kappa$	$2n/3$	1.55	1.46	This work
AES-CTET$^+$			2.32	2.22	

Applicability Of Our Constructions. In 2008, an actor like Google processed tens of petabytes of data every day [DG08], and this number must have significantly increased during the last decade. Indeed, as of 2018, [RGR18] estimated that 33 zettabytes of data has been processed worldwide, and predicted this number would grow to 175 zettabytes by 2025. This amounts to a huge amount of data being stored and encrypted at rest (most likely exabytes of data, which is close to the birthday bound of 2^{64} blocks), under many different keys (i.e. in a multi-user scenario). Besides, the current standard disk encryption algorithm, AES-XTS, only offers security up to the birthday bound, and suffers from the fact that, as a sector is rewritten, an adversary can learn information on the plaintexts with a granularity of 16 bytes. Given such information, it seems reasonable to upgrade the underlying encryption scheme to an algorithm that offers worse granularity to the adversary[1], as well as beyond-birthday-bound security.

Comparison With [CDK+18]. Our goal in this paper is to provide an enciphering scheme based on an underlying block cipher. Hence, we consider our SPN construction in the secret permutation model, whereas [CDK+18] focused on the use of public permutations. Besides, CTET$^+$ improves on the generic 2-round SPN construction from [CDK+18] in two distinct ways:

1. we use the same S-box for both rounds of the SPN, which can help reducing the memory requirements of our scheme;
2. we remark that the middle linear layer can actually have weaker properties than the other two linear layers, which allows the use of a significantly more efficient key-independent matrix multiplication, as can be seen in Table 1.

2 Preliminaries

Throughout this work, we fix positive integers w and n, and we denote $[w] = \{1, \ldots, w\}$. An element x in $\{0,1\}^{wn}$ can be viewed as a concatenation of w blocks, each of which is

[1] For all the other algorithms studied in Table 1, blocks would consist in a whole sector instead of a single 16-byte word.

of length n. The i-th block of this representation will be denoted x_i for $i = 1, \ldots, w$, so we have $x = x_1 \| x_2 \| \cdots \| x_w$, sometimes written as $x = (x_1, \ldots, x_w)$, identifying $\{0,1\}^{wn}$ and $(\{0,1\}^n)^w$. Assuming $2^n \geq w + 3$, we fix a finite field with 2^n elements, denoted $\mathbb{F}$, and naturally identify $\mathbb{F}$ (resp. $\mathbb{F}^w$) and $(\{0,1\}^n)^w$.

For a set R and an integer $s \geq 1$, R^{*s} denotes the set of all sequences that consists of s pairwise distinct elements of R. For any integer r such that $r \geq s$, we will write $(r)_s = r!/(r-s)!$. If $|R| = r$, then $(r)_s$ becomes the size of R^{*s}. The sets of non-negative integers and non-negative real numbers are denoted $\mathbb{N}$ and $\mathbb{R}^{\geq 0}$, respectively.

2.1 Tweakable Permutations

For an integer $m \geq 1$, the set of all permutations on $\{0,1\}^m$ will be denoted $\mathsf{Perm}(m)$. A tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $\widetilde{P} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that, for any tweak $t \in \mathcal{T}$,

$$x \mapsto \widetilde{P}(t, x)$$

is a permutation of $\mathcal{X}$. The set of all tweakable permutations with tweak space $\mathcal{T}$ and message space $\{0,1\}^m$ will be denoted $\widetilde{\mathsf{Perm}}(\mathcal{T}, m)$.

A keyed tweakable permutation with key space $\mathcal{K}$, tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $T : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that, for any key $k \in \mathcal{K}$,

$$(t, x) \mapsto T(k, t, x)$$

is a tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$. We will sometimes write $T(k, t, x)$ as $T_k(t, x)$ or $T_{k,t}(x)$. In particular, $T_{k,t}$ is a permutation of $\mathcal{X}$ for each $(k, t) \in \mathcal{K} \times \mathcal{T}$.

Blockwise Universality. The core of our security proof is to compute a lower bound on the number of possible intermediate values that map a tuple of plaintexts to a tuple of ciphertexts, given some conditions on the permutation. A key point in such proofs is the ability to control collisions between inputs to the inner primitive S. Hence, we are going to need our keyed layers to satisfy a universality property as follows.

Definition 1. A keyed tweakable permutation

$$T : \mathcal{K} \times \mathcal{T} \times \{0,1\}^{wn} \longrightarrow \{0,1\}^{wn}$$

is called (δ, δ')-*blockwise universal* ((δ, δ')-*BU*) if the following conditions hold.

1. For all distinct (t, x, i), $(t', x', i') \in \mathcal{T} \times \{0,1\}^{wn} \times \{1, \ldots, w\}$, we have

$$\mathsf{Pr}\left[k \xleftarrow{\$} \mathcal{K} : T_{k,t}(x)_i = T_{k,t'}(x')_{i'}\right] \leq \delta.$$

2. For all $(t, x, i, c) \in \mathcal{T} \times \{0,1\}^{wn} \times \{1, \ldots, w\} \times \{0,1\}^n$, we have

$$\mathsf{Pr}\left[k \xleftarrow{\$} \mathcal{K} : T_{k,t}(x)_i = c\right] \leq \delta'.$$

Let

$$T^{-1} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^{wn} \longrightarrow \{0,1\}^{wn}$$

be a keyed tweakable permutation such that $T^{-1}(k, t, x) = (T_{k,t})^{-1}(x)$ for each $(k, t, x) \in \mathcal{K} \times \mathcal{T} \times \{0,1\}^{wn}$. If T and T^{-1} are both (δ, δ')-blockwise universal, then T is called (δ, δ')-*super blockwise universal* ((δ, δ')-*SBU*).

Regularity. In our security proof, it will be essential to ensure that, when at most one of the w blocks of an input (resp. output) of the second keyed permutation layer is fixed to an arbitrary value[2], and the remaining blocks are chosen uniformly at random without replacement in some set, the distribution of the output (resp. input) is close enough to uniform. More specifically, we will only be interested in the probability that the w blocks of the output (resp. input) are pairwise distinct and belong to a specific set of authorized values, in order to avoid collisions with previously queried inputs/outputs to the public permutation. More formally, we define the regularity of a permutation as follows.

Definition 2. A permutation

$$P : \{0,1\}^{wn} \to \{0,1\}^{wn}$$

is called *regular* if for any $A, B \subset \{0,1\}^n$, the following three conditions are satisfied.

1. The number of elements $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x) \in (\{0,1\}^n \setminus B)^{*w}$ is at least
$$(2^n - |A|)_w \left(1 - \frac{w|B| + w(w-1)/2}{2^n - |A| - w + 1}\right).$$

2. For any $a \in A$ and $i \in \{1, \ldots, w\}$, the number of elements $x \in (\{0,1\}^n)^{*w}$ such that $x_i = a$, $x_j \notin A$ for $j \neq i$ and $P(x) \in (\{0,1\}^n \setminus B)^{*w}$ is at least
$$(2^n - |A|)_{w-1} \left(1 - \frac{w|B| + w(w-1)/2}{2^n - |A| - w + 2}\right).$$

3. For any $b \in B$ and $i \in \{1, \ldots, w\}$, the number of elements $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x) \in (\{0,1\}^n)^{*w}$, $P(x)_i = b$ and $P(x)_j \notin B$ for $j \neq i$ is at least
$$(2^n - |B|)_{w-1} \left(1 - \frac{w|A| + (w-1)w/2}{2^n - |B| - w + 2}\right).$$

A keyed tweakable permutation T will be called regular if and only if $T(k, t, \cdot)$ is regular for any $(k, t) \in \mathcal{K} \times \mathcal{T}$.

This technical definition is actually rather natural. If we consider the first condition, we want a lower bound on the number of tuples $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x) \in (\{0,1\}^n \setminus B)^{*w}$. There are exactly $(2^n - |A|)_w$ elements in $(\{0,1\}^n \setminus A)^{*w}$, while $P(x)$ should satisfy $w|B| + \frac{w(w-1)}{2}$ conditions since all w blocks of $P(x)$ should be distinct and outside B. Intuitively, the first point of the definition essentially requires that each of the conditions on $P(x)$ removes at most $(2^n - |A|)_{w-1}$ possibilities for x. Other lower bounds can be derived similarly. As we will see, there is a simple sufficient condition for an affine map to be regular.

Lemma 1. *Let $+, \times$ be two binary oparations such that $R = (\{0,1\}^n, +, \times)$ is a unitary ring of characteristic 2. Let $P : \{0,1\}^{wn} \to \{0,1\}^{wn}$ be an affine map where*

$$\begin{aligned} P : \{0,1\}^{wn} &\longrightarrow \{0,1\}^{wn} \\ x &\longmapsto Mx + a, \end{aligned}$$

for a $w \times w$ invertible matrix M over the ring R and $a \in \{0,1\}^{wn}$, identifying elements in $\{0,1\}^{wn}$ with w-dimensional column vectors over R. Then P is regular if M satisfies the following conditions.

1. Each row of M and M^{-1} contains at least two invertible entries.

[2]The remaining cases will be easy to rule out thanks to the previously defined BU property.

2. The sum of any two rows of M contains at least two invertible entries.

3. The sum of any two rows of M^{-1} contains at least two invertible entries.

Proof. To lower bound the number of elements $x = (x_1, \ldots, x_w)$ such that $x \in (\{0,1\}^n \setminus A)^{*w}$ and $P(x) \in (\{0,1\}^n \setminus B)^{*w}$, we first fix $i \in \{1, \ldots, w\}$ and $b \in B$. Suppose that the j-th entry of the i-th row of M is invertible. Then we select distinct $w-1$ values $x_1, \ldots, x_w$ except x_j, all from $\{0,1\}^n \setminus A$. The number of possible choices for these values is $(2^n - |A|)_{w-1}$. Since the equation $P(x)_i = b$ uniquely determines x_j, the number of $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x)_i \in B$ for some $i = 1, \ldots, w$ is at most $w|B|(2^n - |A|)_{w-1}$.

Next, we fix two different indices i_1, $i_2 \in \{1, \ldots, w\}$. Suppose that the j-th entry is invertible in the sum of the i_1-th row and the i_2-th row of M. We select distinct $w-1$ values $x_1, \ldots, x_w$ except x_j, all from $\{0,1\}^n \setminus A$. Then the equation $P(x)_{i_1} = P(x)_{i_2}$ will uniquely determine x_j. So the number of $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x)_{i_1} = P(x)_{i_2}$ for some $1 \le i_1 < i_2 \le w$ is at most $\binom{w}{2}(2^n - |A|)_{w-1}$.

Overall, the number of "bad choices" is at most $w|B|(2^n - |A|)_{w-1} + \binom{w}{2}(2^n - |A|)_{w-1}$, and hence the number of elements $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x) \in (\{0,1\}^n \setminus B)^{*w}$ is at least

$$(2^n - |A|)_w - w|B|(2^n - |A|)_{w-1} - \binom{w}{2}(2^n - |A|)_{w-1} \\ = (2^n - |A|)_w \left(1 - \frac{w|B| + w(w-1)/2}{2^n - |A| - w + 1}\right).$$

To prove the second condition of regularity, we will assume that $x_1 = a$ for some $a \in A$ (without loss of generality), and lower bound the number of element $x = (x_1, \ldots, x_w)$ such that $x \in (\{0,1\}^n)^{*w}$, $x_i \notin A$ for $i \ge 2$ and $P(x) \in (\{0,1\}^n \setminus B)^{*w}$. We first fix $i \in \{1, \ldots, w\}$ and $b \in B$. Then we can find an index $j \ge 2$ such that the j-th entry of the i-th row of M is invertible since each row of M contains at least two invertible entries. We select distinct $w-2$ values $x_2, \ldots, x_w$ except x_j, all from $\{0,1\}^n \setminus A$. The number of possible choices for these values is $(2^n - |A|)_{w-2}$. Since the equation $P(x)_i = b$ uniquely determines x_j, the number of elements $x \in (\{0,1\}^n)^{*w}$ such that $x_1 = a$, $x_j \notin A$ for $j \ge 2$ and $P(x)_i \in B$ for some $i = 1, \ldots, w$ is at most $w|B|(2^n - |A|)_{w-2}$.

Next, we fix two different indices i_1, $i_2 \in \{1, \ldots, w\}$. We can find an index $j \ge 2$ such that the j-th entry is invertible in the sum of the i_1-th row and the i_2-th row of M. We select distinct $w-2$ values $x_2, \ldots, x_w$ except x_j, all from $\{0,1\}^n \setminus A$. Then the equation $P(x)_{i_1} = P(x)_{i_2}$ will uniquely determine x_j. So the number of $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $x_1 = a$, $x_j \notin A$ for $j \ge 2$ and $P(x)_{i_1} = P(x)_{i_2}$ for some $1 \le i_1 < i_2 \le w$ is at most $\binom{w}{2}(2^n - |A|)_{w-2}$.

By discarding at most $w|B|(2^n - |A|)_{w-2} + \binom{w}{2}(2^n - |A|)_{w-2}$ elements, the number of elements $x \in (\{0,1\}^n)^{*w}$ such that $x_1 = a$, $x_j \notin A$ for $j \ge 2$ and $P(x) \in (\{0,1\}^n \setminus B)^{*w}$ is lower bounded by

$$(2^n - |A|)_{w-1} - w|B|(2^n - |A|)_{w-2} - \binom{w}{2}(2^n - |A|)_{w-2} \\ = (2^n - |A|)_{w-1} \left(1 - \frac{w|B| + w(w-1)/2}{2^n - |A| - w + 2}\right).$$

To prove the third condition, we fix $b \in B$ and $i \in \{1, \ldots, w\}$. Then the number of elements $x \in (\{0,1\}^n \setminus A)^{*w}$ such that $P(x) \in (\{0,1\}^n)^{*w}$, $P(x)_i = b$ and $P(x)_j \notin B$ for $j \ne i$ is the same as the number of elements $y \in (\{0,1\}^n)^{*w}$ such that $y_i = b$, $y_j \notin B$ for $j \ne i$ and $P^{-1}(y) \in (\{0,1\}^n \setminus A)^{*w}$. The linear part of P^{-1} is represented by M^{-1}, and in

the same way as we proved the second condition, we can prove that this number is lower bounded by

$$(2^n - |B|)_{w-1} \left(1 - \frac{w|A| + w(w-1)/2}{2^n - |B| - w + 2}\right). \qquad \square$$

2.2 An Efficient Regular SBU Tweakable Permutation

Halevi [Hal07] proposed an efficient xor-blockwise universal construction BPE, and it has been made tweakable by Cogliati et al. [CDK+18], where the tweakable variant has been dubbed TBPE. In this section, we will see that TBPE is not only super blockwise universal but also regular. We begin with the definition of TBPE.

For each $k \in \mathbb{F}$, define a $w \times w$ matrix over $\mathbb{F}$, $M_k =^{\text{def}} A_k \oplus I$, where I is the identity matrix and

$$A_k = \begin{bmatrix} k & k^2 & & k^w \\ k & k^2 & & k^w \\ & & \ddots & \\ k & k^2 & & k^w \end{bmatrix}. \tag{1}$$

Let z be a primitive element of $\mathbb{F}$, and let

$$\mathcal{K} = \left\{ k \in \mathbb{F} : \sum_{i=0}^{w} k^i \neq 0 \right\} \times \mathbb{F}$$

and $\mathcal{T} = \{0,1\}^n$ denote the key space and the tweak space, respectively. Then TBPE is defined as follows.

$$\begin{aligned} \mathsf{TBPE} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^{wn} &\longrightarrow \{0,1\}^{wn} \\ ((k,k'),t,x) &\longmapsto M_k(x \oplus b_t) \oplus a_{k'} \oplus b_t, \end{aligned}$$

where we identify $x \in \{0,1\}^{wn}$ with an element of $\mathbb{F}^w$, and

$$a_{k'} = \begin{bmatrix} k' \\ zk' \\ \vdots \\ z^{w-1}k' \end{bmatrix}, \qquad b_t = \begin{bmatrix} t \\ t \\ \vdots \\ t \end{bmatrix}.$$

It is easy to check that M_k is invertible if $\sum_{i=0}^{w} k^i \neq 0$; precisely,

$$M_k^{-1} = I \oplus \frac{A_k}{k^*},$$

where $k^* =^{\text{def}} \sum_{i=0}^{w} k^i$. Therefore, each pair of key $(k,k') \in \mathcal{K}$ and tweak $t \in \mathcal{T}$ defines a permutation $\mathsf{TBPE}_{k,k',t}$ on $\{0,1\}^{wn}$; let

$$\begin{aligned} (\mathsf{TBPE})^{-1} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^{wn} &\longrightarrow \{0,1\}^{wn} \\ (k,k',t,x) &\longmapsto (\mathsf{TBPE}_{k,k',t})^{-1}(x). \end{aligned}$$

Cogliati et al. [CDK+18] proved the following lemma.

Lemma 2. *Let* TBPE *be the keyed tweakable permutation as defined above, and let* TBPE^{-1} *be its inverse.*

1. *For all distinct* (t,x,i), $(t',x',i') \in \mathcal{T} \times \{0,1\}^{wn} \times \{1,\ldots,w\}$, *we have*

$$\mathsf{Pr}\left[(k,k') \xleftarrow{\$} \mathcal{K} : \mathsf{TBPE}_{k,k',t}(x)_i = \mathsf{TBPE}_{k,k',t'}(x')_{i'}\right] \leq \frac{w}{2^n - w}.$$

2. For all $(t, x, i, c) \in \mathcal{T} \times \{0,1\}^{wn} \times \{1, \ldots, w\} \times \{0,1\}^n$*, we have*

$$\mathsf{Pr}\left[(k, k') \xleftarrow{\$} \mathcal{K} : \mathsf{TBPE}_{k,k',t}(x)_i = c\right] \leq \frac{1}{2^n}.$$

3. For all distinct (t, x, i)*,* $(t', x', i') \in \mathcal{T} \times \{0,1\}^{wn} \times \{1, \ldots, w\}$*, we have*

$$\mathsf{Pr}\left[(k, k') \xleftarrow{\$} \mathcal{K} : \mathsf{TBPE}^{-1}_{k,k',t}(x)_i = \mathsf{TBPE}^{-1}_{k,k',t'}(x')_{i'}\right] \leq \frac{w}{2^n - w}.$$

4. For all $(t, x, i, c) \in \mathcal{T} \times \{0,1\}^{wn} \times \{1, \ldots, w\} \times \{0,1\}^n$*, we have*

$$\mathsf{Pr}\left[(k, k') \xleftarrow{\$} \mathcal{K} : \mathsf{TBPE}^{-1}_{k,k',t}(x)_i = c\right] \leq \frac{w+1}{2^n - w}.$$

In this work, we also prove the regularity of TBPE using Lemma 1.

Lemma 3. *If* $w \geq 3$*, then* $\mathsf{TBPE}_{k,k',t}$ *is regular for any* $(k, k', t) \in \mathcal{K} \times \mathcal{T}$*.*

Proof. For a fixed $(k, k', t) \in \mathcal{K} \times \mathcal{T}$, the linear part of TBPE is represented by $M_k = A_k \oplus I$, and $M_k^{-1} = I \oplus \frac{A_k}{k^*}$, where A_k is defined in (1). One can easily see that M_k and M_k^{-1} satisfy the three conditions of Lemma 1, and hence TBPE is regular when $w \geq 3$.[3] □

From Lemma 2 and Lemma 3, it follows that TBPE is $\left(\frac{w}{2^n - w}, \frac{w+1}{2^n - w}\right)$-super blockwise universal and regular (for any key and tweak).

2.3 Indistinguishability in the Multi-user Setting

Let $\mathsf{C}[S]$ be a keyed tweakable permutation on $\{0,1\}^{wn}$ with key space $\mathcal{K}$ and tweak space $\mathcal{T}$ using an n-bit *secret* S-box S as its inner primitive.

In the multi-user setting, let ℓ denote the number of users. In the *real* world, ℓ secret keys $\mathbf{k} = (\mathbf{k}_1, \ldots \mathbf{k}_\ell) \in \mathcal{K}$ are chosen independently at random. An ℓ-tuple of S-boxes $\mathbf{S} = (S_1, \ldots, S_\ell)$ is also randomly chosen from $\mathsf{Perm}(n)^\ell$. A distinguisher $\mathcal{D}$ is given oracle access to $(\mathsf{C}_{\mathbf{k}_1}[S_1], \ldots, \mathsf{C}_{\mathbf{k}_\ell}[S_\ell])$. In the *ideal* world, $\mathcal{D}$ is given a set of independent random tweakable permutations $\widetilde{\mathcal{P}} = (\widetilde{P}_1, \ldots, \widetilde{P}_\ell) \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell$ instead of $(\mathsf{C}_{\mathbf{k}_1}[S_1], \ldots, \mathsf{C}_{\mathbf{k}_\ell}[S_\ell])$.

The adversarial goal is to tell apart the two worlds $(\mathsf{C}_{\mathbf{k}_1}[S_1], \ldots, \mathsf{C}_{\mathbf{k}_\ell}[S_\ell])$ and $(\widetilde{P}_1, \ldots, \widetilde{P}_\ell)$ by adaptively making forward and backward queries to each of the constructions (without access to the S-boxes). Formally, $\mathcal{D}$'s distinguishing advantage is defined by

$$\begin{aligned}\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{C}}(\mathcal{D}) = \mathsf{Pr}\left[\widetilde{P}_1, \ldots, \widetilde{P}_\ell \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{T}, wn) : 1 \leftarrow \mathcal{D}^{\widetilde{P}_1, \ldots, \widetilde{P}_\ell}\right] \\ - \mathsf{Pr}\left[\mathbf{k} \xleftarrow{\$} \mathcal{K}^\ell, \mathbf{S} \xleftarrow{\$} \mathsf{Perm}(n)^\ell : 1 \leftarrow \mathcal{D}^{\mathsf{C}_{\mathbf{k}_1}[S_1], \ldots, \mathsf{C}_{\mathbf{k}_\ell}[S_\ell]}\right].\end{aligned}$$

For $q \geq 0$, we define

$$\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{C}}(q) = \max_{\mathcal{D}} \mathrm{Adv}^{\mathrm{mu}}_{\mathsf{C}}(\mathcal{D})$$

where the maximum is taken over all adversaries $\mathcal{D}$ making at most q queries to the tweakable permutations.

H-COEFFICIENT TECHNIQUE. Suppose that a distinguisher $\mathcal{D}$ makes total q queries to the construction oracles. The queries made to the λ-th construction oracle, denoted C_λ, are recorded in a query history

$$\mathcal{Q}_{C_\lambda} = (\lambda, t_{\lambda,i}, x_{\lambda,i}, y_{\lambda,i})_{1 \leq i \leq q_\lambda}$$

[3] When $w = 2$, we can make TBPE regular simply by discarding the square roots of 1 from $\mathcal{K}$.

for $\lambda = 1, \ldots, \ell$, where q_λ is the number of queries made to C_λ and $(\lambda, t_{\lambda,i}, x_{\lambda,i}, y_{\lambda,i})$ represents the evaluation obtained by the i-th query to C_λ.[4] So according to the instantiation, it implies either $\mathsf{C}_{\mathbf{k}_\lambda}[S_\lambda](t_{\lambda,i}, x_{\lambda,i}) = y_{\lambda,i}$ or $\widetilde{P}_\lambda(t_{\lambda,i}, x_{\lambda,i}) = y_{\lambda,i}$. Let

$$\mathcal{Q}_C = \mathcal{Q}_{C_1} \cup \cdots \cup \mathcal{Q}_{C_\ell}.$$

Then the query history $\mathcal{Q}_C$ will be called the *transcript* of the attack: it contains all the information that $\mathcal{D}$ has obtained at the end of the attack. In this work, we will only consider information theoretic distinguishers. Therefore we can assume that a distinguisher is deterministic without making any redundant query, and hence the output of $\mathcal{D}$ can be regarded as a function of $\mathcal{Q}_C$, denoted $\mathcal{D}(\mathcal{Q}_C)$.

Fix a transcript $\mathcal{Q}_C$, a key $\mathbf{k} \in \mathcal{K}$, a tweakable permutation $\widetilde{P} \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)$, an S-box $\mathbf{S} \in \mathsf{Perm}(n)$ and $\lambda \in \{1, \ldots, \ell\}$: if $\mathsf{C}_{\mathbf{k}}[\mathbf{S}](t_{\lambda,i}, x_{\lambda,i}) = y_{\lambda,i}$ (resp. $\widetilde{P}(t_{\lambda,i}, x_{\lambda,i}) = y_{\lambda,i}$) for every $i = 1, \ldots, q_\lambda$, then we will write $\mathsf{C}_{\mathbf{k}}[\mathbf{S}] \vdash \mathcal{Q}_{C_\lambda}$ (resp. $\widetilde{P} \vdash \mathcal{Q}_{C_\lambda}$).

Let $\mathbf{k}_1, \ldots, \mathbf{k}_\ell \in \mathcal{K}$, $S_1, \ldots, S_\ell \in \mathsf{Perm}(n)$ and $\widetilde{P}_1, \ldots \widetilde{P}_\ell \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)$. If $\mathsf{C}_{\mathbf{k}_\lambda}[S_\lambda] \vdash \mathcal{Q}_{C_\lambda}$ (resp. $\widetilde{P}_\lambda \vdash \mathcal{Q}_{C_\lambda}$) for every $\lambda = 1, \ldots, \ell$, then we will write $(\mathsf{C}_{\mathbf{k}_\lambda}[S_\lambda])_{\lambda=1,\ldots,\ell} \vdash \mathcal{Q}_C$ (resp. $(\widetilde{P}_\lambda)_{\lambda=1,\ldots,\ell} \vdash \mathcal{Q}_C$).

If there exist $\widetilde{\mathbf{P}} = (\widetilde{P}_1, \ldots, \widetilde{P}_\ell) \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell$ that output $\mathcal{Q}_C$ at the end of the interaction with $\mathcal{D}$, then we will call the transcript $\mathcal{Q}_C$ *attainable*. For an attainable transcript $\mathcal{Q}_C$, let

$$\mathsf{p}_1(\mathcal{Q}_C) = \mathsf{Pr}\left[\widetilde{\mathbf{P}} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell : \widetilde{\mathbf{P}} \vdash \mathcal{Q}_C\right],$$
$$\mathsf{p}_2(\mathcal{Q}_C) = \mathsf{Pr}\left[\mathbf{k}_1, \ldots, \mathbf{k}_\ell \xleftarrow{\$} \mathcal{K}, S_1, \ldots, S_\ell \xleftarrow{\$} \mathsf{Perm}(n) : (\mathsf{C}_{\mathbf{k}_\lambda}[S_\lambda])_\lambda \vdash \mathcal{Q}_C\right].$$

With these definitions, the following lemma, the core of the H-coefficients technique (without defining "bad" transcripts), will be also used in our security proof.

Lemma 4. *Let $\varepsilon > 0$. Suppose that for any attainable transcript $\mathcal{Q}_C$,*

$$\mathsf{p}_2(\mathcal{Q}_C) \geq (1 - \varepsilon)\mathsf{p}_1(\mathcal{Q}_C). \tag{2}$$

Then one has

$$\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{C}}(\mathcal{D}) \leq \varepsilon.$$

The lower bound (2) is called *ε-point-wise proximity* of the transcript $\mathcal{Q}_C$. The point-wise proximity of a transcript in the multi-user setting is guaranteed by the point-wise proximity of $(\mathcal{Q}_{C_\lambda})$ for each $\lambda = 1, \ldots, \ell$ in the single-user setting. The following lemma is a restatement of Lemma 3 in [HT16] in the secret permutation setting.

Lemma 5. *Let $\varepsilon : \mathbb{N} \times \mathbb{N} \to \mathbb{R}^{\geq 0}$ be a function such that $\varepsilon(y) + \varepsilon(z) \leq \varepsilon(y + z)$ for every y, $z \in \mathbb{N}$. Suppose that for any distinguisher $\mathcal{D}$ in the single-user setting that makes q construction queries, and for any attainable transcript $\mathcal{Q}_C$ obtained by $\mathcal{D}$, one has*

$$\mathsf{p}_2(\mathcal{Q}_C) \geq (1 - \varepsilon(q))\mathsf{p}_1(\mathcal{Q}_C).$$

Then for any distinguisher $\mathcal{D}$ in the multi-user setting that makes total q construction queries, and for any attainable transcript $\mathcal{Q}_C$ obtained by $\mathcal{D}$, one has

$$\mathsf{p}_2(\mathcal{Q}_C) \geq (1 - \varepsilon(q))\mathsf{p}_1(\mathcal{Q}_C).$$

[4] The index λ in a construction query can be dropped out in the single-user setting.

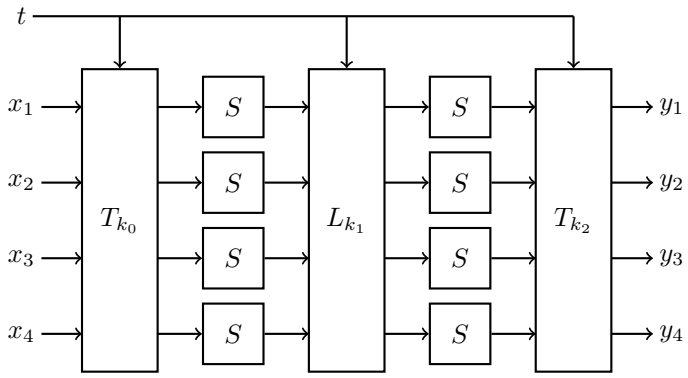

Figure 1: CTET^+ with $w = 4$. The input and output blocks of the SPN are represented as $x = x_1||x_2||x_3||x_4$ and $y = y_1||y_2||y_3||y_4$, respectively.

3 The CTET$^+$ Enciphering Scheme

Let J_w (resp. I_w) denote the $w \times w$ all-ones matrix (resp. identity matrix) over $\mathbb{F}$, and let z be a primitive element of $\mathbb{F}$. We define a keyed tweakable permutation L as follows.

$$\begin{aligned} L : \mathcal{K}' \times \mathcal{T} \times \{0,1\}^{wn} &\longrightarrow \{0,1\}^{wn} \\ (k,t,x) &\longmapsto (2J_w \oplus I_w)x \oplus a_k \oplus b_t \end{aligned}$$

where $\mathcal{K}' = \mathcal{T} = \{0,1\}^n$, a_k, b_t are defined as in Section 2.2, and 2 is a shorthand for the n-bit block $0\cdots010$ (similarly, 1 is a shorthand for the block $0\cdots01$). For any key k and tweak t, we have

$$L_{k,t}^{-1}(x) = \begin{cases} (2J_w \oplus I_w)(x \oplus a_k \oplus b_t) & \text{if } w \text{ is even,} \\ ((1 \oplus (2 \oplus 1)^{-1})J_w \oplus I_w)(x \oplus a_k \oplus b_t) & \text{if } w \text{ is odd.} \end{cases}$$

So the regularity of L and L^{-1} is immediate from Lemma 1.

The CTET^+ enciphering scheme based on an n-bit S-box S is defined as follows; for a key $\mathbf{k} = (k_0, k_1, k_2) \in \mathcal{K} \times \mathcal{K}' \times \mathcal{K}$, a tweak $t \in \mathcal{T}$ and a plaintext $x \in \{0,1\}^{wn}$,

$$\mathsf{CTET}^+[S]_{\mathbf{k}}(t,x) = T_{k_2}\left(t, S^{\|}\left(L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)\right)\right),$$

where T denotes TBPE (as defined in Section 2), and for $x = (x_1, \ldots, x_w)$, we write

$$S^{\|}(x) = S(x_1) \,\|\, S(x_2) \,\|\, \cdots \,\|\, S(x_w).$$

As we will see in the following section, the middle layer of our construction has to be regular, but does not need to be SBU (although it still has to satisfy a weaker universality constraint).

3.1 Security of CTET$^+$

In this section, we will prove the following theorem.

Theorem 1. *Let n, and w be positive integers such that $w \geq 2$ and let ℓ be the number of users. Then for any q such that $3w^2 + 16w^2q \leq 2^n$, one has*

$$\mathbf{Adv}^{\mathrm{mu}}_{\mathsf{CTET}^+}(q) \leq \frac{(4w^3 + 31w^2)q}{2^n} + \frac{32w^4q^2 + (4w^6 + 32w^5 + 128w^4)q^3}{2^{2n}} + \frac{12w^6q^4}{2^{3n}}.$$

3.2 Outline of the Proof of Theorem 1

The proof of Theorem 1 relies on the following Lemma (with $\delta \leq \frac{2w}{2^n}$), and on Lemma 4 and Lemma 5.

Lemma 6. *Let q be positive integers such that $3w^2 + 16w^2q \leq 2^n$, and let $\delta = \frac{w}{2^n - w}$.*[5] *Let also $\mathcal{D}$ be a distinguisher in the single-user setting that makes q construction queries. Then for any attainable transcript $\tau = \mathcal{Q}_C$, one has*

$$\frac{\mathsf{p}_2(\mathcal{Q}_C)}{\mathsf{p}_1(\mathcal{Q}_C)} \geq 1 - \frac{31w^2q}{2^n} - \frac{28w^4q^2 + 128w^4q^3}{2^{2n}} - \frac{12w^6q^4}{2^{3n}} - 2w^2q\delta - \frac{2w^3q^2\delta}{2^n} - w^4q^3\delta^2 - \frac{16w^4q^3\delta}{2^n}.$$

First note that, if $\frac{2w^2q}{2^n} + \frac{16w^4q^2+64w^4q^3}{2^{2n}} > 1$, then there is nothing to prove as the r.h.s. of the inequality becomes negative. Thus we are going to focus on the case where this inequality does not hold, as this condition will allow us to prove the positivity of several terms throughout our proof.

We fix a distinguisher $\mathcal{D}$ as described in Lemma 6 and fix an attainable transcript $\tau = \mathcal{Q}_C$ obtained by $\mathcal{D}$. Let us also denote q_t the number of queries done using tweak $t \in \mathcal{T}$, and $q = \sum_{t\in\mathcal{T}} q_t$ the total number of queries.

We will first define what we mean by an extension of the transcript τ. Then we will define bad extensions and upper bound their number in Lemma 7, and then show that the probability to obtain any good extension in the real world is sufficiently close to the probability to obtain τ in the ideal world in Lemma 8. We will then show how Lemma 6 is derived from Lemmas 7 and 8. For space reasons, the proof of Lemma 8 will be given in subsection 3.3.

Extension of a transcript. We will extend τ as follows. Let us choose any pair of keys $(k_0, k_2) \in \mathcal{K}^2$. Once these keys have been chosen, some construction queries will become involved in collisions. A *first-order colliding query* is a construction query $(t, x, y) \in \mathcal{Q}_C$ such that one of the following conditions holds:

1. there exist a construction query $(t', x', y') \in \mathcal{Q}_C$ and two integers $i, j \in \{1, \ldots, w\}$ such that $(t, x, i) \neq (t', x', j)$ and $T_{k_0}(t, x)_i = T_{k_0}(t', x')_j$;
2. there exist a construction query $(t', x', y') \in \mathcal{Q}_C$ and two integers $i, j \in \{1, \ldots, w\}$ such that $(t, y, i) \neq (t', y', j)$ and $T^{-1}_{k_2}(t, y)_i = T^{-1}_{k_2}(t', y')_j$.

A first-order colliding query will be said *forward* (resp. *backward*) if it satisfies condition 1 (resp. condition 2) above. As we will see later, no first-order colliding query will be both backward and forward with overwhelming probability. Let us denote FColl^+ (resp. FColl^-) the set of all forward (resp. backward) first-order colliding queries and $\mathrm{FColl} = \mathrm{FColl}^+ \cup \mathrm{FColl}^-$.

We are now going to build a new set $\mathcal{Q}_S$ that will play the role of an extension of transcript. For each *forward* (resp. *backward*) *first-order colliding* query $(t, x, y) \in \mathcal{Q}_C$, we will add a tuple $(T_{k_0}(t, x)_i, v')_{1\leq i\leq w}$ (resp. $(u', T^{-1}_{k_2}(t, y)_i)_{1\leq i\leq w}$) to $\mathcal{Q}_S$, by lazily sampling a uniformly random (dummy) permutation. In more details, using an arbitrary ordering of the queries, for every first-order forward (resp. backward) colliding query (t, x, y) and every $i = 1, \ldots, w$, if $T_{k_0}(t, x)_i$ (resp. $T^{-1}_{k_2}(t, y)_i$) does not appear in $\mathcal{Q}_S$, we draw uniformly at random a block v' (resp. u') in $\{0, 1\}^n$ that is different from the values that already appear in the second (resp. first) coordinate of a tuple from $\mathcal{Q}_S$. We finally choose a key k_1.

[5] The security proof requires only the blockwise universality of TBPE, not the uniformity. So δ' does not appear in our bound.

An extended transcript τ' will then be a tuple $\tau' = (\mathcal{Q}_C, \mathcal{Q}_S, \mathbf{k})$ where $\mathbf{k} = (k_0, k_1, k_2)$. These added values will prove useful in the description of bad extended queries transcript. Indeed, for each first-order colliding query, we will now have complete information about the evaluation of one round of the SPN, which will allow us to define a condition on the draw of the last key k_1. Note that the addition of a pair $(T_{k_0}(t,x)_i, v')$ or $(u', T_{k_2}^{-1}(t,y)_i)$ could create a new colliding query. Such colliding queries will be referred to as *second-order colliding* queries. As we will see later, this type of collision will only occur with negligible probability as the values u' and v' are chosen uniformly randomly in the set of authorized values. We will denote SColl the set of second-order colliding queries.

Definition and Number of Bad Transcript Extensions. Let

$$U = \{u \in \{0,1\}^n : (u,v) \in \mathcal{Q}_S\}, \qquad V = \{v \in \{0,1\}^n : (u,v) \in \mathcal{Q}_S\}$$

denote the domain and range of $\mathcal{Q}_S$.

Definition 3. We say that an extended transcript τ' is *bad* if at least one of the following conditions is fulfilled:

(C-1) $\mathrm{FColl}^- \bigcap \mathrm{FColl}^+ \neq \emptyset$;

(C-2) $\mathrm{SColl} \neq \emptyset$

(C-3) there exists $(t,x,y) \in \mathrm{FColl}^+$, $i \in \{1,\ldots,w\}$ such that

$$L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)_i \in U;$$

(C-4) there exists $(t,x,y) \in \mathrm{FColl}^+$, $(t',x',y') \in \mathcal{Q}_C$, $i,j \in \{1,\ldots,w\}$ such that

$$L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)_i = T_{k_0}(t',x')_j;$$

(C-5) there exists $(t,x,y),(t',x',y') \in \mathrm{FColl}^+$, $i,j \in \{1,\ldots,w\}$ with $(t,x,i) \neq (t',x',j)$ such that

$$L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)_i = L_{k_1}\left(t', S^{\|}\left(T_{k_0}(t',x')\right)\right)_j;$$

(C-6) there exists $(t,x,y) \in \mathrm{FColl}^-$, $i \in \{1,\ldots,w\}$ such that

$$L_{k_1}^{-1}\left(t, (S^{-1})^{\|}\left(T_{k_2}^{-1}(t,y)\right)\right)_i \in V;$$

(C-7) there exists $(t,x,y) \in \mathrm{FColl}^-$, $(t',x',y') \in \mathcal{Q}_C$, $i,j \in \{1,\ldots,w\}$ such that

$$L_{k_1}^{-1}\left(t, (S^{-1})^{\|}\left(T_{k_2}^{-1}(t,y)\right)\right)_i = T_{k_2}^{-1}(t',y')_j;$$

(C-8) there exists $(t,x,y),(t',x',y') \in \mathrm{FColl}^-$, $i,j \in \{1,\ldots,w\}$ with $(t,y,i) \neq (t',y',j)$ such that

$$L_{k_1}^{-1}(t, (S^{-1})^{\|}(T_{k_2}^{-1}(t,y)))_i = L_{k_1}^{-1}(t', (S^{-1})^{\|}(T_{k_2}^{-1}(t',y')))_j.$$

Otherwise we say that τ' is good. We denote Θ_{good}, resp. Θ_{bad} the set of good, resp. bad extended transcripts and Θ' the set of all extended transcripts. $\Diamond$

We are also going to define a probability distribution on the set Θ' as follows. First, the keys k_0, k_2 are chosen independently and uniformly at random in $\mathcal{K}$, then the evaluation $\mathcal{Q}_S$ (based on collisions) is chosen uniformly at random (meaning that each possible u' and v' is chosen uniformly at random in the set of its authorized values, beginning by forward first-order colliding queries and choosing an arbitrary ordering of the queries), and finally the key k_1 is chosen uniformly at random from $\{0,1\}^n$, independently from everything else. Thus the exact probability of observing an extended transcript τ' is $1/2^n|\mathcal{K}|^2(2^n)_{|\mathcal{Q}_S|}$. We start by upper bounding the probability to get a bad extended transcript with this probability distribution.

Lemma 7. *One has*

$$\Pr\left[\tau' \in \Theta_{\text{bad}}\right] \leq 2w^2q\delta + \frac{2w^3q^2\delta}{2^n} + w^4q^3\delta^2 + \frac{16w^4q^3\delta}{2^n}.$$

Proof. Let us fix any construction query $(t,x,y) \in \mathcal{Q}_C$. By the blockwise universality of T,

$$\Pr\left[k_0 \leftarrow_{\$} \mathcal{K} : (t,x,y) \in \text{FColl}^+\right] \leq w^2q\delta, \tag{3}$$

and similarly,

$$\Pr\left[k_2 \leftarrow_{\$} \mathcal{K} : (t,x,y) \in \text{FColl}^-\right] \leq w^2q\delta. \tag{4}$$

Also let us define auxiliary events,

- $\mathsf{aux}_1 \Leftrightarrow$ there exists $(t,x,y) \in \mathcal{Q}_C$, $(i,j) \in \{1,\ldots,w\}^{*2}$ such that $T_{k_0}(t,x)_i = T_{k_0}(t,x)_j$.
- $\mathsf{aux}_2 \Leftrightarrow$ there exists $(t,x,y) \in \mathcal{Q}_C, (i,j) \in \{1,\ldots,w\}^{*2}$ such that $T_{k_2}^{-1}(t,y)_i = T_{k_2}^{-1}(t,y)_j$.
- $\mathsf{aux}_3 \Leftrightarrow$ there exists distinct $(t,x,y),(t',x',y') \in \mathcal{Q}_C$, and $a,b,c \in \{1,\ldots,w\}$ such that $b \neq c$, $T_{k_0}(t,x)_a = T_{k_0}(t',x')_a$, and $T_{k_0}(t,x)_b = T_{k_0}(t',x')_c$.
- $\mathsf{aux}_4 \Leftrightarrow$ there exists distinct $(t,x,y),(t,x,y) \in \mathcal{Q}_C$, and $a,b,c \in \{1,\ldots,w\}$ such that $b \neq c$, $T_{k_2}^{-1}(t,y)_a = T_{k_2}^{-1}(t',y')_a$, and $T_{k_2}^{-1}(t,y)_b = T_{k_2}^{-1}(t',y')_c$.

One can easily derive $\Pr[\mathsf{aux}_1] \leq w^2q\delta$ and $\Pr[\mathsf{aux}_3] \leq w^3q^2\delta 2^{-n}$. Since aux_2 and aux_4 are symmetric events of aux_1 and aux_3, respectively, we have

$$\Pr[\mathsf{aux}_1 \vee \mathsf{aux}_2 \vee \mathsf{aux}_3 \vee \mathsf{aux}_4] \leq 2w^2q\delta + 2w^3q^2\delta 2^{-n}.$$

We now upper bound the probabilities of the eight conditions in turn. We denote Θ_i the set of attainable transcripts fulfilling condition (C-i).

Condition (C-1). Consider condition (C-1). One has

$$\Pr\left[\tau' \in \Theta_1\right] \leq \sum_{(t,x,y)\in\mathcal{Q}_C} \Pr\left[(t,x,y) \in \text{FColl}^+ \cap \text{FColl}^-\right].$$

Since the random draw of k_0 and k_2 are independent, (3) and (4) give

$$\Pr\left[\tau' \in \Theta_1\right] \leq w^4q^3\delta^2.$$

Condition (C-2). Consider condition (C-2). A second-order collision could be created in the following two ways:

- the completion of the information about a query $(t, x, y) \in \mathrm{FColl}^+$ triggers a collision, i.e. there exists $1 \leq i \leq w$ such that we added the pair $(T_{k_0}(t, x)_i, v')$ where $v' = T_{k_2}^{-1}(t', y')_j$ for some query $(t', x', y') \in \mathcal{Q}_C$ and some $j \in \{1, \ldots, w\}$.
- the completion of the information about a query $(t, x, y) \in \mathrm{FColl}^-$ triggers a collision, i.e. there exists $1 \leq i \leq w$ such that we added the pair $(u', T_{k_2}^{-1}(t, y)_i)$ where $u' = T_{k_0}(t', x')_j$ for some query $(t', x', y') \in \mathcal{Q}_C$ and some $j \in \{1, \ldots, w\}$.

Since the values u' and v' are randomly chosen in a set of size at least $2^n - wq$, one has

$$\Pr[\tau' \in \Theta_2] \leq \frac{2w^4q^3\delta}{2^n - wq}.$$

Condition (C-3), (C-4), (C-6), and (C-7). Denoted $h = h_1 \| \cdots \| h_w$,

$$\Pr[L_{k_1}(t, h)_i = c \wedge \neg \mathsf{aux}_1] \leq \frac{1}{2^n - wq}$$

since the coefficient of h_1 cannot be 0 and the number of such choices for h_1 is always larger than $2^n - wq$. Thus, by summing over the number of queries that can make each event, we get

$$\Pr[\tau' \in \Theta_3 \wedge \neg \mathsf{aux}_1] \leq \frac{w^4q^3\delta}{2^n - wq}, \qquad \Pr[\tau' \in \Theta_4 \wedge \neg \mathsf{aux}_1] \leq \frac{w^4q^3\delta}{2^n - wq}.$$

Similarly, we get

$$\Pr[\tau' \in \Theta_6 \wedge \neg \mathsf{aux}_3] \leq \frac{w^4q^3\delta}{2^n - wq}, \qquad \Pr[\tau' \in \Theta_7 \wedge \neg \mathsf{aux}_3] \leq \frac{w^4q^3\delta}{2^n - wq}.$$

Condition (C-5), (C-8) Let us fix queries $(t, x, y), (t', x', y') \in \mathrm{FColl}^+$ and assume $\neg(\mathsf{aux}_1 \vee \mathsf{aux}_2 \vee \mathsf{aux}_3 \vee \mathsf{aux}_4)$. Denoted $S^{\|}(T_{k_0}(t, x)) = h = h_1 \| \cdots \| h_w$ and $S^{\|}(T_{k_0}(t', x')) = h' = h'_1 \| \cdots \| h'_w$, the condition (C-5) holds (by given two queries) when there exists i, j such that $(t, x, y, i) \neq (t', x', y', j)$ and

$$2\sum_{r=1}^{w}(h_r \oplus h'_r) \oplus h_i \oplus h'_j = (z^i \oplus z^j)k_1 \oplus t \oplus t'.$$

(a) If $i \neq j$, the equation holds with probabilty at most 2^{-n} by the randomness of k_1.

(b) If $i = j$ and $t \neq t'$, the equation holds with probability at most $1/(2^n - wq)$ since the number of choices for $S(\cdot)$ is always larger than $2^n - wq$.

(c) If $(t, i) = (t', j)$ and $h_i \neq h'_i$. Then the equation holds with probability at most $1/(2^n - wq)$ since the coefficient of h_i cannot be 0.

(d) If $(t, i, h_i) = (t', j, h'_j)$, we have $x \neq x'$ and $h \neq h'$ so there exists $a \in \{1, \ldots, w\}$ such that $h_a \neq h'_a$ since otherwise we have aux_1 or aux_3. Then, h_a is unique in h and h' so for the same reason above, the equation holds with probability at most $1/(2^n - wq)$.

Overall, the probability that C-5 occurs is smaller than

$$\Pr[\mathsf{aux}_1 \vee \mathsf{aux}_3] + \frac{w^4q^3\delta}{2^n - wq}.$$

Similarly, the probability that C-8 occurs is smaller than

$$\Pr\left[\mathsf{aux}_2 \vee \mathsf{aux}_4\right] + \frac{w^4q^3\delta}{2^n - wq}.$$

The result follows by $wq \leq 2^{n-1}$ and an union bound over all conditions. □

From Attainable Transcripts to Extended Transcripts. Let us fix any extended transcript $\tau' = (\mathcal{Q}_C, \mathcal{Q}_S, \mathbf{k})$ and let

$$\mathsf{p}_{\mathrm{re}}(\tau') = \frac{1}{2^n|\mathcal{K}|^2} \Pr\left[(S \vdash \mathcal{Q}_S) \wedge (\mathsf{CTET}^+[S]_{\mathbf{k}} \vdash \mathcal{Q}_C)\right],$$
$$\mathsf{p}(\tau') = \Pr\left[\mathsf{CTET}^+[S]_{\mathbf{k}} \vdash \mathcal{Q}_C | S \vdash \mathcal{Q}_S\right].$$

Note that one has

$$\mathsf{p}_2(\mathcal{Q}_C) \geq \sum_{\tau' \in \Theta_{\mathrm{good}}} \mathsf{p}_{\mathrm{re}}(\tau') = \sum_{\tau' \in \Theta_{\mathrm{good}}} \frac{1}{2^n|\mathcal{K}|^2(2^n)_{|\mathcal{Q}_S|}} \mathsf{p}(\tau'),$$

and

$$\mathsf{p}_1(\mathcal{Q}_C) = \frac{1}{\prod_{t \in \mathcal{T}} (2^{wn})_{q_t}}.$$

Thus one has

$$\frac{\mathsf{p}_2(\mathcal{Q}_C)}{\mathsf{p}_1(\mathcal{Q}_C)} \geq \sum_{\tau' \in \Theta_{\mathrm{good}}} \frac{\prod_{t \in \mathcal{T}} (2^{wn})_{q_t}}{2^n|\mathcal{K}|^2(2^n)_{|\mathcal{Q}_S|}} \mathsf{p}(\tau') \geq \Pr\left[\tau \in \Theta_{\mathrm{good}}\right] \left(\min_{\tau' \in \Theta_{\mathrm{good}}} \mathsf{p}(\tau') \prod_{t \in \mathcal{T}} (2^{wn})_{q_t} \right), \tag{5}$$

where the last line comes from the fact that the exact probability to obtain an extended transcript τ is $\frac{1}{2^n|\mathcal{K}|^2(2^n)_{|\mathcal{Q}_S|}}$.

Thus, our next step is the study of good extended transcripts.

Lemma 8. *For any good extended transcript τ', one has*

$$\mathsf{p}(\tau') \prod_{t \in \mathcal{T}} (2^{wn})_{q_t} \geq 1 - \frac{31w^2q}{2^n} - \frac{28w^4q^2 + 128w^4q^3}{2^{2n}} - \frac{12w^6q^4}{2^{3n}}.$$

The proof of this Lemma can be found in Section 3.3.

Concluding the proof of Lemma 6. We get Lemma 6 by combining Lemmas 7 and 8 with Equation (5).

3.3 Proof of Lemma 8

Fix any good extended transcript $\tau' = (\mathcal{Q}_C, \mathcal{Q}_S, (k_0, k_1, k_2))$ and let $p = |\mathcal{Q}_S|$. Recall that U and V denote respectively the domain and the range of $\mathcal{Q}_S$, which means that $|U| = |V| = p$.

We define two quantities characterizing an extended transcript τ', namely

$$\alpha_1 \stackrel{\mathrm{def}}{=} |\{(t, x, y) \in \mathcal{Q}_C : T_{k_0}(t, x)_i \in U \text{ for some } i \in \{1, \ldots, w\}\}|,$$
$$\alpha_2 \stackrel{\mathrm{def}}{=} |\{(t, x, y) \in \mathcal{Q}_C : T^{-1}_{k_2}(t, y)_i \in V \text{ for some } i \in \{1, \ldots, w\}\}|.$$

In words, α_1 (resp. α_2) is the number of queries $(t,x,y) \in \mathcal{Q}_C$ which "collide" with a query $(u,v) \in \mathcal{Q}_S$ in the extended transcript. This corresponds exactly to the number of queries $(t,x,y) \in \mathcal{Q}_C$ which collide with a query $(t',x',y') \in \mathcal{Q}_C$ at the input of S (resp. at the output of S), once the choice of (k_0,k_2) has been made. Indeed, since τ' is a good extended transcript, there are no second-order collisions. Thus $\alpha_1 = |\mathrm{FColl}^+|$ and $\alpha_2 = |\mathrm{FColl}^-|$.

Our goal is then to prove that $\mathsf{p}(\tau')$ is close enough to $1/\prod_{t\in\mathcal{T}}(2^{wn})_{q_t}$. In order to do so, we are going to successively consider queries belonging to FColl^+, FColl^- and $\mathcal{Q}_0 = \mathcal{Q}_C \setminus \left(\mathrm{FColl}^+ \cup \mathrm{FColl}^-\right)$.

Note that, thanks to the additional information from the extended transcript, and since there are no second-order collisions in a good extended transcript, for every query $(t,x,y) \in \mathcal{Q}_C$, there is an equivalence between the events $T_{k_0}(t,x)_i \in U$ for each $i = 1,\ldots,w$ and there exists $i \in \{1,\ldots,w\}$ such that $T_{k_0}(t,x)_i \in U$. Also note that these three sets of queries form a partition of $\mathcal{Q}_C$:

- $\mathcal{Q}_0 \bigcap \mathrm{FColl}^+ = \emptyset$ by definition;
- $\mathcal{Q}_0 \bigcap \mathrm{FColl}^- = \emptyset$ by definition;
- $\mathrm{FColl}^+ \bigcap \mathrm{FColl}^- = \emptyset$ since otherwise τ' would satisfy (C-1).

If E_+, E_- and E_0 denote the events $\mathsf{CTET}^+[S]_{\mathbf{k}} \vdash \mathrm{FColl}^+$, $\mathsf{CTET}^+[S]_{\mathbf{k}} \vdash \mathrm{FColl}^-$ and $\mathsf{CTET}^+[S]_{\mathbf{k}} \vdash \mathcal{Q}_0$, respectively, then the event $\mathsf{CTET}^+[S]_{\mathbf{k}} \vdash \mathcal{Q}_C$ is equivalent to $E_+ \wedge E_- \wedge E_0$. Note that, by definition of FColl^+, each $(t,x,y) \in \mathrm{FColl}^+$ is such that $T_{k_0}(t,x)_i \in U$ for each $i = 1,\ldots,w$; this means that the output of S is already fixed by $\mathcal{Q}_S$. A similar reasoning can be made for E_-. Thus we have

$$\begin{aligned}\mathsf{p}(\tau') &= \Pr\left[E_+ \wedge E_- \wedge E_0 | S \vdash \mathcal{Q}_S\right] \\ &= \Pr\left[E_+ \wedge E_- | S \vdash \mathcal{Q}_S\right] \cdot \Pr\left[E_0 | E_+ \wedge E_- \wedge S \vdash \mathcal{Q}_S\right]. \end{aligned} \tag{6}$$

Evaluation of $\mathbf{Pr}\left[\boldsymbol{E_+ \wedge E_- | S \vdash \mathcal{Q}_S}\right]$. First note that, since we condition on the event $S \vdash \mathcal{Q}_S$, S is already fixed on p values. Second, remark that this event is actually equivalent to the following equations.

$$\begin{aligned} &S\left(L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)_i\right) = T_{k_2}^{-1}(t,y)_i && \text{for every } (t,x,y,i) \in \mathrm{FColl}^+ \times [w], \\ &S\left(T_{k_0}(t,x)_i\right) = L_{k_1}^{-1}\left(t, (S^{-1})^{\|}\left(T_{k_2}^{-1}(t,y)\right)\right)_i && \text{for every } (t,x,y,i) \in \mathrm{FColl}^- \times [w]. \end{aligned}$$

For the first set of equations, note that the values $L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)_i$ are pairwise distinct otherwise τ' would satisfy (C-5). These values are also outside U otherwise τ' would satisfy (C-3). The values $T_{k_2}^{-1}(t,y)_i$ are pairwise distinct (otherwise τ' would satisfy (C-1)) and outside V since otherwise τ' would satisfy (C-1) or (C-2).

Similarly, for the second set of equations,the values $T_{k_0}(t,x)_i$ are all pairwise distinct and outside U, otherwise τ' would satisfy (C-1) or (C-2). The values $L_{k_1}^{-1}\left(t, (S^{-1})^{\|}\left(T_{k_2}^{-1}(t,y)\right)\right)_i$ are also pairwise distinct and outside V or τ' would satisfy (C-6) or (C-8).

Moreover, the values $L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t,x)\right)\right)_i$ for every $(t,x,y,i) \in \mathrm{FColl}^+ \times [w]$ are distinct from the values $T_{k_0}(t,x)_i$ for every $(t,x,y,i) \in \mathrm{FColl}^- \times [w]$ since otherwise τ' would satisfy (C-4). Similarly the values $T_{k_2}^{-1}(t,y)_i$ for every $(t,x,y,i) \in \mathrm{FColl}^+ \times [w]$ are pairwise distinct from the values

$$L_{k_1}^{-1}\left(t, (S^{-1})^{\|}\left(T_{k_2}^{-1}(t,y)\right)\right)_i$$

for every $(t,x,y,i) \in \mathrm{FColl}^- \times [w]$.

Hence the event $E_+ \wedge E_-$ is actually equivalent to $w\alpha_1 + w\alpha_2$ new and distinct equations on S, so that

$$\Pr\left[E_+ \wedge E_- | S \vdash \mathcal{Q}_S\right] = \frac{1}{(2^n - p)_{w\alpha_1 + w\alpha_2}}. \tag{7}$$

Lower bounding $\mathbf{Pr}\left[\boldsymbol{E_0} | \boldsymbol{E_+} \wedge \boldsymbol{E_-} \wedge \boldsymbol{S} \vdash \boldsymbol{\mathcal{Q}_S}\right]$. Conditioned on $E_+ \wedge E_- \wedge S \vdash \mathcal{Q}_S$, S is fixed on exactly $p + w\alpha_1 + w\alpha_2$ values. Let U' be the set of values on which S is already fixed and $V' = \{S(u) : u \in U'\}$. For the sake of clarity, we denote

$$\mathcal{Q}_0 = \{(t_0, x_0, y_0), \ldots, (t_{q_0-1}, x_{q_0-1}, y_{q_0-1})\},$$

using an arbitrary ordering of the queries, and $q_0 = |\mathcal{Q}_0| (= q - \alpha_1 - \alpha_2)$.

First note that the values $T_{k_0}(t, x)_i$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ are pairwise distinct by definition of $\mathcal{Q}_0$. On the other hand, we note that U' consists of two different types of values:

- values of the form $T_{k_0}(t', x')_{i'}$ that were either added in U' during the completion of a forward colliding query, or that came from a condition that was introduced by event E_-,
- values of the form $L_{k_1}\left(t', S^{\|}\left(T_{k_0}(t', x')\right)\right)_{i'}$ that were either added during the completion of a backward colliding query, or that came from a condition that was introduced by event E_+.

Therefore, the values $T_{k_0}(t, x)_i$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ are outside U' by definition of $\mathcal{Q}_0$ and since otherwise τ' would satisfy either (C-2) or (C-4). Similarly, the values $T_{k_2}^{-1}(t, y)_i$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ are pairwise distinct and outside V'. Let us denote U'' the set of all values $T_{k_0}(t, x)_i$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ and V'' the set of all values $T_{k_2}^{-1}(t, y)_i$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$. Note that $U' \cup U''$ (resp. $V' \cup V''$) contains all the values $T_{k_0}(t, x)_i$ for each $(t, x, y) \in \mathcal{Q}_C, i \in \{1, \ldots, w\}$ (resp. $T_{k_2}^{-1}(t, y)_i$ for each $(t, x, y) \in \mathcal{Q}_C, i \in \{1, \ldots, w\}$), since the conditions from the queries in FColl were integrated in U' and V'.

In order to lower bound $\Pr\left[E_0 | E_+ \wedge E_- \wedge S \vdash \mathcal{Q}_S\right]$, we are going to lower bound the number of possible "intermediate" values for $S\left(T_{k_0}(t, x)_i\right)$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ such that no new collision will be created. The explicit requirements that should be met are the following ones:

- the values $S\left(T_{k_0}(t, x)_i\right)$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ are pairwise distinct and outside V',
- the values $L_{k_1}\left(t, S^{\|}\left(T_{k_0}(t, x)\right)\right)_i$ for each $(t, x, y) \in \mathcal{Q}_0, i \in \{1, \ldots, w\}$ are pairwise distinct and outside U'.

Let N_0 be the number of tuples of distinct values $(v_{i,j})_{(i,j) \in [q_0] \times [w]}$ in $\{0,1\}^n \setminus V'$ such that the values $L_{k_1}\left(t_i, v_{i,1} \| \ldots \| v_{i,w}\right))$ are pairwise distinct and outside U'. Simply lower bounding N_0 will not be sufficient to accurately lower bound $\Pr\left[E_0 | E_+ \wedge E_- \wedge S \vdash \mathcal{Q}_S\right]$. Indeed, if we choose one of these N_0 tuples and condition on S satisfying $S\left(T_{k_0}(t_i, x_i)_j\right) = v_{i,j}$ for each $(i, j) \in [q_0] \times [w]$, the event E_0 will then be equivalent to a number of new equations on S that will depend on the number of collisions between values $\left(L_{k_1}\left(t_i, v_{i,1} \| \ldots \| v_{i,w}\right)\right)_j$ and $T_{k_0}(t_{i'}, x_{i'})_{j'}$. Thus we will have to be mindful of the occurence of such collisions. The simplest way to do so would be to only consider the tuples of values that do not create such collisions. However, such a strategy could only lead to a security bound up to the birthday bound. Instead, we are going to fix in advance a small number of collisions and then lower bound the number of tuples of values that will exactly satisfy these collisions. The result will follow by summing over every possible choice of collisions.

Let $\theta \in \{0, \ldots, \lfloor q_0/2 \rfloor\}$. We are going to choose θ pairs of queries that are not involved in a first-order collision, and to force a collision of the type $S(T_{k_0}(t,x)_i) = T_{k_2}^{-1}(t',y')_{i'}$ for each pair of queries. In order to simplify the computations, no query should appear in more than one pair. Note that, in that case, there are exactly $w^{2\theta}(q_0)_{2\theta}/\theta!$ possible sets of θ pairs of the form $((t,x,y,i),(t',x',y',i'))$ where $(t,x,y),(t',x',y') \in \mathcal{Q}_0$ and $i,j \in [w]$. Let us fix one of these sets A. We are going to lower bound the number N_θ of possible intermediate values $(v_{i,1}, \ldots, v_{i,w})_{i \in [q_0]} \in (\{0,1\}^n)^{wq_0}$ such that:

- these values are pairwise distinct and outside V';
- the values $L_{k_1}(t_i, v_{i,1} \| \ldots \| v_{i,w})_j$ for $i \in [q_0]$, $j \in [w]$ are pairwise distinct and outside U';
- for every pair of queries $((t_i,x_i,y_i,j),(t_{i'},x_{i'},y_{i'},j')) \in A$, $v_{i,j} = T_{k_2}^{-1}(t_{i'},y_{i'})_{j'}$ and $L_{k_1}(t_{i'}, v_{i',1} \| \ldots \| v_{i',w})_{j'} = T_{k_0}(t_i,x_i)_j$;
- every other value $v_{i,j}$ for $i \in [q_0]$, $j \in [w]$ should be outside V'' and every other value $L_{k_1}(t_i, v_{i,1} \| \ldots \| v_{i,w})_j$ for $i \in [q_0]$, $j \in [w]$ should be outside U''.

One has the following lower bound, whose proof can be found in Section 3.4.

Lemma 9. *One has*

$$N_\theta \geq (2^n - p - wq)_{wq_0 - 2\theta} \prod_{i=0}^{q_0 - 2\theta - 1} \left(1 - \frac{w(p + wq + wi) + w(w-1)/2}{2^n - p - wq - w(i+1) + 1}\right) \times \prod_{j=0}^{\theta - 1} \left(1 - \frac{2wp + 4w^2 q + 4jw^2 + (2w+1)(w-1)}{2^n - p - 4wq - 2w}\right).$$

Note that, if we fix such intermediate values, the probability that E_0 is satisfied along with the equations $S(T_{k_0}(t_i,x_i)_j) = v_{i,j}$ for each $(i,j) \in [q_0] \times [w]$ is exactly $1/(2^n - p - w\alpha_1 - w\alpha_2)_{2wq_0 - \theta}$. Indeed, if $\theta = 0$, then no collision occurs and each query in $\mathcal{Q}_0$ adds $2w$ new conditions on S. If $\theta > 0$, then, for each one of the θ pairs of queries in A, the condition $S(T_{k_0}(t,x)_i) = T_{k_2}^{-1}(t',y')_{i'}$ appears twice, thus adding only $4w-1$ new conditions for these two queries. Hence

$$\Pr\left[E_0 | E_+ \wedge E_- \wedge S \vdash \mathcal{Q}_S\right] \geq \sum_{\theta=0}^{\lfloor q_0/2 \rfloor} \frac{w^{2\theta}(q_0)_{2\theta} N_\theta}{\theta!(2^n - p - w\alpha_1 - w\alpha_2)_{2wq_0 - \theta}}. \tag{8}$$

Combining (8) with (6) and (7) yields

$$\mathsf{p}(\tau') \geq \sum_{\theta=0}^{\lfloor q_0/2 \rfloor} \frac{w^{2\theta}(q_0)_{2\theta} N_\theta}{\theta!(2^n - p)_{wq + wq_0 - \theta}}$$

since $q_0 + \alpha_1 + \alpha_2 = q$. We will appeal to a trick used in [CLL+14] and introduce the hypergeometric probability mass function[6] $\mathrm{Hyp}_{2^n - p - w\alpha_1 - w\alpha_2, wq_0, wq_0}$ in the previous sum, where, for $0 \leq \theta \leq wq_0$,

$$\mathrm{Hyp}_{2^n - p - w\alpha_1 - w\alpha_2, wq_0, wq_0}(\theta) = \frac{(wq_0)_\theta (wq_0)_\theta (2^n - p - wq)_{wq_0 - \theta}}{\theta!(2^n - p - w\alpha_1 - w\alpha_2)_{wq_0}}.$$

[6] The random variable $\mathrm{Hyp}_{N,a,b}$, parameterized by N, a, and b, counts the number of elements selected from a certain subset of b elements when a elements are selected from the universe of N elements without replacement.

Hence, one has

$$\begin{aligned}\mathsf{p}(\tau')\prod_{t\in\mathcal{T}}(2^{wn})_{q_t} &\geq \sum_{\theta=0}^{\lfloor q_0/2\rfloor}\frac{w^{2\theta}(q_0)_{2\theta}N_\theta\prod_{t\in\mathcal{T}}(2^{wn})_{q_t}}{\theta!(2^n-p)_{wq+wq_0-\theta}}\\ &\geq \sum_{\theta=0}^{\lfloor q_0/2\rfloor}\frac{w^{2\theta}(q_0)_{2\theta}N_\theta(2^{wn})_q}{\theta!(2^n-p)_{wq+wq_0-\theta}}\\ &\geq \sum_{\theta=0}^{\lfloor q_0/2\rfloor}\mathrm{Hyp}_{2^n-p-w\alpha_1-w\alpha_2,wq_0,wq_0}(\theta)A_\theta B_\theta \qquad (9)\end{aligned}$$

where

$$\begin{aligned}A_\theta &= \frac{w^{2\theta}(q_0)_{2\theta}}{(wq_0)_\theta(wq_0)_\theta},\\ B_\theta &= \frac{N_\theta(2^n-p-w\alpha_1-w\alpha_2)_{wq_0}(2^{wn})_q}{(2^n-p)_{wq+wq_0-\theta}(2^n-p-wq)_{wq_0-\theta}}.\end{aligned}$$

We will lower bound A_θ and B_θ in turn. Since $\theta\leq q_0/2$ and $w>1$, one has

$$\begin{aligned}A_\theta &= \prod_{i=0}^{\theta-1}\frac{w^2(q_0-i)(q_0-\theta-i)}{(wq_0-i)^2}\\ &= \prod_{i=0}^{\theta-1}\left(1-\frac{q_0(w^2\theta+2w^2i-2iw)-i(w^2\theta+w^2i-i)}{(wq_0-i)^2}\right)\\ &\geq 1-\sum_{i=0}^{\theta-1}\frac{q_0(w^2\theta+2w^2i-2iw)-i(w^2\theta+w^2i-i)}{(wq_0-i)^2}\\ &\geq 1-\sum_{i=0}^{\theta-1}\frac{3w^2q_0\theta}{(wq_0-i)^2}\geq 1-\sum_{i=0}^{\theta-1}\frac{12\theta}{q_0}=1-\frac{12\theta^2}{q_0}. \qquad (10)\end{aligned}$$

Using Lemma 9, one has

$$\begin{aligned}B_\theta &= \frac{N_\theta(2^n-p-w\alpha_1-w\alpha_2)_{wq_0}(2^{wn})_q}{(2^n-p)_{wq+wq_0-\theta}(2^n-p-wq)_{wq_0-\theta}}\\ &\geq \frac{N_\theta 2^{wnq}}{(2^n-p)_{w\alpha_1+w\alpha_2}\left((2^n-p-wq)_{wq_0-\theta}\right)^2}\left(1-\frac{q^2}{2^{wn+1}}\right)\\ &\geq \frac{N_\theta 2^{wnq_0}}{(2^n-p-wq)_{wq_0-\theta}(2^n-p-wq)_{wq_0-\theta}}\left(1-\frac{q^2}{2^{wn+1}}\right)\\ &\geq \frac{N_\theta 2^{n(wq_0-2\theta)}}{(2^n-p-wq)_{wq_0-2\theta}(2^n-p-wq)_{wq_0-2\theta}}\left(1-\frac{q^2}{2^{wn+1}}\right)\\ &\geq \frac{2^{n(wq_0-2\theta)}}{(2^n-p-wq)_{wq_0-2\theta}}\prod_{i=0}^{q_0-2\theta-1}\left(1-\frac{w(p+wq_+wi)+w(w-1)/2}{2^n-p-wq-w(i+1)+1}\right)\\ &\times\left(1-\frac{q^2}{2^{wn+1}}\right)\prod_{j=0}^{\theta-1}\left(1-\frac{2wp+4w^2q+4jw^2+(2w+1)(w-1)}{2^n-p-4wq-2w}\right). \qquad (11)\end{aligned}$$

Finally, one has

$$\begin{aligned}
&\frac{2^{n(wq_0-2\theta)}}{(2^n-p-wq)_{wq_0-2\theta}}\prod_{i=0}^{q_0-2\theta-1}\left(1-\frac{w(p+wq+wi)+w(w-1)/2}{2^n-p-wq-w(i+1)+1}\right)\\
&\geq \frac{2^{wn(q_0-2\theta)}}{(2^n-p-wq)_{wq_0-2w\theta}}\prod_{i=0}^{q_0-2\theta-1}\left(1-\frac{w(p+wq+wi)+w(w-1)/2}{2^n-p-wq-w(i+1)+1}\right)\\
&\geq \prod_{i=0}^{q_0-2\theta-1}\left(1-\frac{w(p+wq+wi)+w(w-1)/2}{2^n-p-wq-w(i+1)+1}\right)\left(1+\frac{p+wq+wi}{2^n-p-wq-wi}\right)^w\\
&\geq \prod_{i=0}^{q_0-2\theta-1}\left(1-\frac{w(p+wq+wi)+w(w-1)/2}{2^n-p-wq-w(i+1)+1}\right)\left(1+\frac{wp+w^2q+w^2i}{2^n-p-wq-wi}\right)\\
&\geq \prod_{i=0}^{q_0-2\theta-1}\left(1-\frac{\frac{w^2}{2}(2^n+(w+1)p+(w+w^2)(q+i))+(wp+w^2q+w^2i)^2}{(2^n-p-wq-w(i+1)+1)(2^n-p-wq-wi)}\right)\\
&\geq 1-\frac{2w^2q}{2^n}-\frac{4w^3q\times 4wq+4q(4w^2q)^2}{2^{2n}}. \qquad (12)
\end{aligned}$$

since $p \leq 2wq$ by definition and we assumed $3w^2 + 16w^2q \leq 2^n$. Hence, by combining (10), (11) and (12), one has

$$\begin{aligned}
A_\theta B_\theta \geq &\left(1-\frac{12\theta^2}{q_0}\right)\left(1-\frac{q^2}{2^{wn+1}}\right)\\
&\times\prod_{j=0}^{\theta-1}\left(1-\frac{2wp+4w^2q+4jw^2+(2w+1)(w-1)}{2^n-p-4wq-2w}\right)\\
&\times\left(1-\frac{2w^2q}{2^n}-\frac{16w^4q^2+64w^4q^3}{2^{2n}}\right). \qquad (13)
\end{aligned}$$

Thanks to our assumptions on q, each term in the previous product, except the first one, is between 0 and 1. Since both A_θ and B_θ are positive, the previous bound holds whether $q_0 \leq 12\theta^2$ or not. Combining (9) and (13) with Weierstrass product inequality applied, and using $p \leq 2wq$, one has

$$\begin{aligned}
\mathsf{p}(\tau')\prod_{t\in\mathcal{T}}(2^{wn})_{q_t} &\geq \sum_{\theta=0}^{\lfloor q_0/2\rfloor}\mathrm{Hyp}_{2^n-p-w\alpha_1-w\alpha_2,wq_0,wq_0}(\theta)(1-f(\theta))\\
&= \sum_{\theta=0}^{\lfloor q_0/2\rfloor}\mathrm{Hyp}_{2^n-p-w\alpha_1-w\alpha_2,wq_0,wq_0}(\theta)-\mathbb{E}[f(\theta)]\\
&\geq 1-\sum_{\theta>\lfloor q_0/2\rfloor}\mathrm{Hyp}_{2^n-p-w\alpha_1-w\alpha_2,wq_0,wq_0}(\theta)-\mathbb{E}[f(\theta)], \qquad (14)
\end{aligned}$$

where

$$\begin{aligned}
f(\theta) = &\frac{12\theta^2}{q_0}+\frac{q^2}{2^{wn+1}}+\frac{2w\theta p+4w^2\theta q+\theta^2(2w^2+1)+2(2w+1)(w-1)\theta}{2^n}\\
&+\frac{2w^2q}{2^n}+\frac{16w^4q^2+64w^4q^3}{2^{2n}}
\end{aligned}$$

and the expectation $\mathbb{E}[f(\theta)]$ is taken over the random variable θ which follows the probability

distribution $\mathrm{Hyp}_{2^n-p-w\alpha_1-w\alpha_2,wq_0,wq_0}$. Note that

$$\mathbb{E}[\theta] = \frac{w^2q_0^2}{2^n-p-w\alpha_1-w\alpha_2} \leq \frac{2w^2q_0^2}{2^n},$$
$$\mathbb{E}[\theta^2] \leq \frac{4w^4q_0^4}{2^{2n}} + \frac{2w^2q_0^2}{2^n}.$$

Hence, using Markov's inequality, one has

$$\sum_{\theta>q_0/2} \mathrm{Hyp}_{2^n-p-w\alpha_1-w\alpha_2,wq_0,wq_0}(\theta) \leq \frac{2\mathbb{E}[\theta]}{q_0} \leq \frac{4w^2q_0}{2^n} \leq \frac{4w^2q}{2^n}. \tag{15}$$

Moreover, one has

$$\begin{aligned}\mathbb{E}[f(\theta)] &\leq \frac{26w^2q}{2^n} + \frac{q^2}{2^{wn+1}} + \frac{20w^4q^2+128w^4q^3}{2^{2n}} \\ &\quad + \frac{2q^2w^2\left(2(2w+1)(w-1)+1\right)}{2^{2n}} + \frac{12w^6q^4}{2^{3n}} \\ &\leq \frac{27w^2q}{2^n} + \frac{28w^4q^2+128w^4q^3}{2^{2n}} + \frac{12w^6q^4}{2^{3n}}. \end{aligned} \tag{16}$$

Combining (14), (15) and (16) yields the result.

3.4 Proof of Lemma 9

Let us fix one sets of pairs of queries A. Recall that we are going to lower bound the number N_θ of possible intermediate values $(v_{i,1},\ldots,v_{i,w})_{i\in[q_0]} \in (\{0,1\}^n)^{wq_0}$ such that:

(C-i) these values are pairwise distinct and outside V';

(C-ii) the values $L_{k_1}\left(t_i, v_{i,1}\|\ldots\|v_{i,w}\right)_j$ for $i \in [q_0]$, $j \in [w]$ are pairwise distinct and outside U';

(C-iii) for every pair of queries $((t_i,x_i,y_i,j),(t_{i'},x_{i'},y_{i'},j')) \in A$, $v_{i,j} = T_{k_2}^{-1}(t_{i'},y_{i'})_{j'}$ and $L_{k_1}\left(t_{i'}, v_{i',1}\|\ldots\|v_{i',w}\right)_{j'} = T_{k_0}(t_i,x_i)_j$;

(C-iv) every other value $v_{i,j}$ for $i \in [q_0]$, $j \in [w]$ should be outside V'' and every other value $L_{k_1}\left(t_i, v_{i,1}\|\ldots\|v_{i,w}\right)_j$ for $i \in [q_0]$, $j \in [w]$ should be outside U''.

In order to do so, we are going to rely on the regularity of L. We are first going to reorder the queries from $\mathcal{Q}_0$ so that the queries appearing in A are last, and both queries of a pair are consecutive. We are going to lower bound the number of possible intermediate values for these queries iteratively as follows.

THE $q_0 - 2\theta$ SINGLE QUERIES. These queries are not involved in any collision. Let $i \in \{0,\ldots,q_0-2\theta-1\}$ and let us assume that $v_{j,1},\ldots,v_{j,w}$ for $0 \leq j < i$ are already chosen according to the conditions (C-i) to (C-iv). The values $v_{i,1},\ldots,v_{i,w}$ should be pairwise distinct, outside of $V' \cup V''$[7], and distinct from $v_{j,1},\ldots,v_{j,w}$ for $j < i$[8]. This excludes a set of values of size exactly $p+wq+wi$. Similarly, the values $L_{k_1}\left(t_i, v_{i,1}\|\ldots\|v_{i,w}\right)_j$ for $j \in [w]$ should be pairwise distinct, outside of $U' \cup U''$ and different from the values $L_{k_1}\left(t_j, v_{j,1}\|\ldots\|v_{j,w}\right)_{j'}$ for $j < i$, $j' \in [w]$. This excludes a set of exactly $p+wq+wi$ values.

[7]Note that $|U' \cup U''| = |V' \cup V''| = p + w\alpha_1 + w\alpha_2 + wq_0 = p + wq$ since τ' is a good extended transcript.

[8]These values are pairwise distinct and outside of $V' \cup V''$ by construction.

Using the regularity of L, the number of possibilities for $v_{i,1}, \ldots, v_{i,w}$ is greater than

$$(2^n - p - wq - wi)_w \left(1 - \frac{w(p + wq + wi) + w(w-1)/2}{2^n - p - wq - w(i+1) + 1}\right).$$

Overall, the number of possible intermediate values for the first $q_0 - 2\theta$ intermediate values is greater than

$$(2^n - p - wq)_{w(q_0-2\theta)} \prod_{i=0}^{q_0-2\theta-1} \left(1 - \frac{w(p + wq + wi) + w(w-1)/2}{2^n - p - wq - w(i+1) + 1}\right). \tag{17}$$

where this value is non-negative since we assume $3w^2 + 16w^2q \leq 2^n$.

Let us fix one of these sequences of intermediate values. Let us also denote V''' (resp. U''') the set of all values $v_{i,j}$ (resp. $L_{k_1}\left(t_i, v_{i,1} \| \ldots \| v_{i,w}\right)_j$) for $i = 0, \ldots, q_0 - 2\theta - 1$, $j = 1, \ldots, w$. Note that, by construction, $V''' \cap (V' \cup V'') = \emptyset$, $U''' \cap (U' \cup U'') = \emptyset$ and $|U'''| = |V'''| = w(q_0 - 2\theta)$. We now have to handle the remaining 2θ queries. Let

$$\mathcal{Q}'_0 = \{(t_0, x_0, y_0), \ldots, (t_{2\theta-1}, x_{2\theta-1}, y_{2\theta-1})\}$$

be the set of the remaining queries appearing in A.

The last $\boldsymbol{\theta}$ pairs of queries. Let $((t_0, x_0, y_0, i_0), (t_1, x_1, y_1, i_1))$ be the first pair of queries. Let us consider the first query. We want to fix $v_{0,i_0} = T_{k_2}^{-1}(t_1, y_1)_{i_1}$. Moreover, we want $v_{0,i}$ for $i \neq i_0$ to be pairwise distinct and outside of $V' \cup V'' \cup V'''$, and the values $L_{k_1}\left(t_0, v_{0,1} \| \ldots \| v_{0,w}\right)_j$ for $j \in [w]$ to be pairwise distinct and outside of $U' \cup U'' \cup U'''$. Using the regularity of L, there are at least

$$\begin{aligned}(2^n - p - w(q + q_0 - 2\theta))_{w-1} &\left(1 - \frac{w(p + w(q + q_0 - 2\theta)) + w(w-1)/2}{2^n - p - w(q + q_0 - 2\theta) - w + 2}\right) \\ &\geq (2^n - p - w(q + q_0 - 2\theta))_{w-1} \left(1 - \frac{wp + 2w^2q + w(w-1)/2}{2^n - p - 2wq - 2w}\right)\end{aligned}$$

possibilities for $v_{0,1}, \ldots, v_{0,w}$.

Similarly, for the second query, we want $v_{1,i}$ for $i \in [w]$ to be pairwise distinct, outside of $V' \cup V'' \cup V'''$ and different from the values $v_{0,i}$ for $i \neq i_0$, which excludes exactly $p' + w(q + q_0 - 2\theta) + w - 1$ values. Note that the value v_{0,i_0} is automatically excluded since it appears in V''. We also want the values $L_{k_1}\left(t_1, v_{1,1} \| \ldots \| v_{1,w}\right)_i$ for $i \neq i_1$ to be pairwise distinct, outside of $U' \cup U'' \cup U'''$ and different from the values $L_{k_1}\left(t_0, v_{0,1} \| \ldots \| v_{0,w}\right)_j$ for $j \in [w]$. This excludes exactly $p + w(q + q_0 - 2\theta) + w$ values. Finally, we fix $L_{k_1}\left(t_1, v_{1,1} \| \ldots \| v_{1,w}\right)_{i_1} = T_{k_0}(t_0, y_0)_{i_0}$. Using the regularity of L, the number of possibilities for $v_{1,1}, \ldots, v_{1,w}$ is lower bounded by

$$\begin{aligned}&(2^n - p - w(q + q_0 - 2\theta) - w)_{w-1} \\ &\times \left(1 - \frac{w(p + w(q + q_0 - 2\theta) + w - 1) + w(w-1)/2}{2^n - p - w(q + q_0 - 2\theta) - 2w + 2}\right) \\ &\geq (2^n - p - w(q + q_0 - 2\theta) - w + 1)_{w-1} \left(1 - \frac{w - 1}{2^n - p - w(q + q_0 - 2\theta + 2)}\right) \\ &\times \left(1 - \frac{w(p + w(q + q_0 - 2\theta)) + 3w(w-1)/2}{2^n - p - w(q + q_0 - 2\theta) - 2w + 2}\right) \\ &\geq (2^n - p - w(q + q_0 - 2\theta) - w + 1)_{w-1} \left(1 - \frac{wp + 2w^2q + (3w+2)(w-1)/2}{2^n - p - 2wq - 2w}\right).\end{aligned}$$

Overall, the number of possible intermediate values for this pair of queries is at least

$$(2^n - p - w(q + q_0 - 2\theta))_{2w-2} \left(1 - \frac{2wp + 4w^2q + (2w+1)(w-1)}{2^n - p - 2wq - 2w}\right) \geq 0.$$

Let $1 \leq j \leq \theta - 1$, and let

$$((t_{2j}, x_{2j}, y_{2j}, i_{2j}), (t_{2j+1}, x_{2j+1}, y_{2j+1}, i_{2j+1}))$$

be the $(j+1)$-th pair of queries. Let us consider the first query. We want to fix $v_{2j,i_{2j}} = T_{k_2}^{-1}(t_{2j+1}, y_{2j+1})_{i_{2j+1}}$. Moreover, we want $v_{2j,j'}$ for $j' \neq i_{2j}$ to be pairwise distinct and outside of $V' \cup V'' \cup V'''$, and distinct from the $j(2w-1)$ values $v_{2j',j''}$ and $v_{2j'+1,j'''}$ for $j' < j$, $j'' \neq i_{2j'}$ and $j''' \in [w]$. Similarly, we want the values $L_{k_1}(t_{2j}, v_{2j,1} \| \dots \| v_{2j,w})_{j'}$ for $j' \in [w]$ to be pairwise distinct and outside of $U' \cup U'' \cup U'''$, and distinct from the $j(2w-1)$ values that were previously fixed for the j previous pairs of queries. Using the regularity of L, the number of possibilities for $v_{2j,1}, \dots, v_{2j,w}$ is lower bounded by

$$\begin{aligned}
&(2^n - p - w(q + q_0 - 2\theta) - j(2w-1))_{w-1} \\
&\qquad \times \left(1 - \frac{w(p + w(q + q_0 - 2\theta) + j(2w-1)) + w(w-1)/2}{2^n - p - w(q + q_0 - 2\theta) - j(2w-1) - w + 2}\right) \\
&\qquad\qquad \geq (2^n - p - w(q + q_0 - 2\theta) - j(2w-1))_{w-1} \\
&\qquad\qquad\qquad \times \left(1 - \frac{wp + 2w^2q + jw(2w-1)) + w(w-1)/2}{2^n - p - 2wq - j(2w-1) - 2w}\right).
\end{aligned}$$

Similarly, for the second query, we want $v_{2j+1,j'}$ for $j' \in [w]$ to be pairwise distinct, outside of $V' \cup V'' \cup V'''$ and different from the values $v_{j',j''}$ for $j' \leq 2j$ and $j'' \neq i_{j'}$ if j' is even, which excludes exactly $p + w(q + q_0 - 2\theta) + j(2w-1) + w - 1$ values. Note that the values $v_{2j',i_{2j'}}$ are automatically excluded since they appear in V''. We also want the values $L_{k_1}(t_{2j+1}, v_{2j+1,1} \| \dots \| v_{2j+1,w})_{j'}$ for $j' \neq i_{2j+1}$ to be pairwise distinct, outside of $U' \cup U'' \cup U'''$ and different from the values $L_{k_1}(t_{j'}, v_{j',1} \| \dots \| v_{j',w})_{j''}$ for $j' \leq 2j$, and $j'' \neq i_{j'}$ if j' is odd. This excludes exactly $p + w(q + q_0 - 2\theta) + j(2w-1) + w$ values. Finally, we fix $L_{k_1}(t_{2j+1}, v_{2j+1,1} \| \dots \| v_{2j+1,w})_{i_{2j+1}} = T_{k_0}(t_{2j}, y_{2j})_{i_{2j}}$. Using the regularity of L, the number of possibilities for $v_{2j+1,1}, \dots, v_{2j+1,w}$ is lower bounded by

$$\begin{aligned}
&(2^n - p - w(q + q_0 - 2\theta) - j(2w-1) - w)_{w-1} \\
&\times \left(1 - \frac{w(p + w(q + q_0 - 2\theta) + j(2w-1) + w - 1) + w(w-1)/2}{2^n - p - w(q + q_0 - 2\theta) - j(2w-1) - 2w + 2}\right) \\
&\geq (2^n - p - w(q + q_0 - 2\theta) - j(2w-1) - w + 1)_{w-1} \\
&\times \left(1 - \frac{w - 1}{2^n - p - w(q + q_0 - 2\theta + 2w) - j(2w-1)}\right) \\
&\times \left(1 - \frac{w(p + w(q + q_0 - 2\theta) + j(2w-1)) + 3w(w-1)/2}{2^n - p - w(q + q_0 - 2\theta + 2) - j(2w-1)}\right) \\
&\geq (2^n - p - w(q + q_0 - 2\theta) - j(2w-1) - w + 1)_{w-1} \\
&\times \left(1 - \frac{wp + 2w^2q + jw(2w-1) + (3w+2)(w-1)/2}{2^n - p - 2wq - j(2w-1) - 2w}\right).
\end{aligned}$$

Overall, the number of possible intermediate values for this pair of queries is at least

$$\begin{aligned}(2^n - p - w(q + q_0 - 2\theta) - j(2w-1))_{2w-2} \\ \times \left(1 - \frac{2wp + 4w^2q + 4jw^2 + (2w+1)(w-1)}{2^n - p - 2wq - j(2w-1) - 2w}\right) \\ \geq (2^n - p - w(q + q_0 - 2\theta) - j(2w-2))_{2w-2} \\ \times \left(1 - \frac{2wp + 4w^2q + 4jw^2 + (2w+1)(w-1)}{2^n - p - 4wq - 2w}\right) \geq 0.\end{aligned}$$

Hence, the number of possible intermediate values for the last θ pairs of queries is lower bounded by

$$\begin{aligned}&(2^n - p - w(q + q_0 - 2\theta))_{\theta(2w-2)} \\ &\times \prod_{j=0}^{\theta-1} \left(1 - \frac{2wp + 4w^2q + 4jw^2 + (2w+1)(w-1)}{2^n - p - 4wq - 2w}\right) \geq 0. \end{aligned} \tag{18}$$

Combining (17) and (18) yields the result.

4 Concrete Instance

The first option to instantiate the CTET^+ construction consists in using a (full-round) block cipher, supposed to have the ideal behavior we are looking for, in each of the w boxes of each round. In our case, the natural candidate is the 10-round AES-128 since its good software performance would fit the applications we have in mind.

Nonetheless, we hope for even better performances and we thus develop here the idea of reducing the number of rounds in each box, in a prove-then-prune manner [HKR15]. A simple solution to reduce the number of AES rounds in the final cipher would be to opt for a round-reduced version that has a security level at least equal to the bound we are aiming for, that is $\frac{2n}{3} \approx 85$ bits of security. In view of the existing distinguishers for 6 rounds (see Table 2) it would mean opting for at least 7 rounds of AES.

Table 2: Secret-key Distinguishers on 6 rounds of AES-128 (ACC = adaptive chosen ciphertexts, CP = chosen plaintexts).

Type	**Time**	**Data**	**Data Type**	**Ref.**
Exchange attack	2^{83} Encryptions	2^{83}	CP and ACC	[Bar19]
Truncated Differential	$2^{96.5}$ Memory Accesses	$2^{89.4}$	CP	[BGL20]
Impossible Yoyo	$2^{121.8}$ XORs	$2^{122.8}$	ACC	[RBH17]

Our hope is to reduce further this number so we decide to move away from a direct use of the proved security to see if cryptanalysis arguments can show that CTET^+ instantiated with 6-round AES reaches the required security goal.

In this case, Theorem 1 cannot be used to provide a concrete security bound anymore. Instead, it justifies the fact that the generic structure of AES_6-CTET^+ is sound, and will resist generic attacks with high probability. Our security claims will then be justified by the extensive and dedicated cryptanalysis presented in Section 5.

Specification of the Concrete Instance

AES_6-CTET^+ is the instance of CTET^+ where $n = 128$ and for which the S-box corresponds to the first 6 rounds of AES-128 using a secret key.

For a fixed value of w, AES$_6$-CTET$^+$ uses a 5×128-bit key $\mathbf{k} = ((k_0, k'_0), k_1, (k_2, k'_2))$ for the 3 affine layers, a tweak t of 128 bits, and an additional 128-bit key L used as parameter of the S-box. It modifies a plaintext x of $w \times 128$ bits by applying in this order the following operations:

- TBPE $T_{(k_0,k'_0)}$ as defined in Section 2.2, with $z = 2$;
- 6 rounds of AES-128 with a secret key L to each 128-bit block of the internal state. We later call these 6 rounds an *AES-box* as it stands for the S-boxes of the scheme and recall the definition of AES-128 in Supplementary Material A. Note that we still omit the last MixColumns here.
- L_{k_1} as defined in Section 3;
- AES-box on each 128-bit of the internal state, with the same secret key L;
- TBPE $T_{(k_2,k'_2)}$ with $z = 2$;

Security Claim. In view of the previous proof, we make an initial claim of 85 bits of security in the single key scenario, for instances with fixed $w > 1$. Since in the considered use cases we have w that is at most equal to 256, we believe that it is reasonable to set an upper bound for w, with $w \leq 1024$.

5 Security Analysis of the Concrete Instance

To justify the security of our proposal, we first show that it would be hard to extend the properties of the AES-boxes to the full cipher and second show that structural attacks are not a concern either.

5.1 Security Arguments for Attacks based on the AES

In this section, we start by recalling some properties of 6-round AES as it already provides some guarantees against differential and linear attacks. Then, we show that extending an attack on AES to our instance is very hard. As a starting point, we provide in Table 3 the best attacks published so far on AES-128 in the single-key scenario.

Table 3: Best attacks on AES-128 in the single key setting (we only report the fastest one for each type).

Rounds	Type	Time	Data	Ref.
6	Square	2^{71}	2^{32}	[DKR97]
6	Partial Sums	2^{48}	2^{32}	[FKL$^+$01]
7	Herd	2^{120}	2^{128}	[FKL$^+$01]
7	Collision	2^{128}	2^{32}	[GM00]
7	Impossible Differential	$2^{110.9}$	$2^{104.9}$	[LP20]
7	MITM	2^{99}	2^{97}	[DFJ13]

Differential and Linear Properties. AES was designed to provide strong arguments against differential and linear attacks, and as few as 4 rounds already provide a reasonable security against these two basic attack vectors in the single-key setting: regarding differentials, Keliher and Sui [KS07] were able to prove an upper bound equal to 1.881×2^{-114}. In the linear case, [PSLL03] reports that the maximum linear hull

probability for 4 rounds of AES is bounded by 1.075×2^{-106}. These bounds prevent an attacker from using differential or linear techniques that rely on fixed input and output differences over one (or more) AES-box(es).

Algebraic Resistance. According to [HLLT20], the algebraic degree of 4 rounds of AES is at least 116 and thus 6 rounds are expected to provide resistance against an algebraic attacker with power 2^{85}. Note that the property we are looking for here is not to reach the full degree (which is known as impossible for ASASA [BKP16]) but to be sure that exploiting the non-optimal degree is not possible given our claim.

Extending the AES Distinguishers. A first idea to attack AES_6-CTET^+ is to adapt one of the existing distinguishers (or attacks) on round-reduced AES-128 to obtain a property on one of the AES-box that is then extended to the full construction. The basic linear and differential distinguishers are out of reach, but techniques like the ones in Table 2 and Table 3 might return good results. As we are going to discuss in the following subsection, a first difficulty in doing so is that the first (or last if we work with decryption queries) affine layer makes difficult to control the input values or differences of the AES-boxes. If we want to include a key recovery part to cover some of the 6 rounds of an AES-box – copying the usual attacks on AES – it would require to know the value entering it (the usual plaintext), and then already requires a guess on k'_0 before further processing.

Another possibility would be to position the distinguisher at the start of the AES-box, without a key-recovery opening[9]. According to the state of the art, a maximum of 6 rounds of AES-128 are distinguishable. Extending these properties over the L_{k_1} layer and some rounds of the subsequent AES-box is not trivial. Thus, it seems very unlikely that the full second-round AES-box is covered.

All in all, it seems difficult to use those techniques to attack the full version of AES_6-CTET^+.

5.2 Structural Attacks

The capabilities of the previous techniques being rather limited, we move here to structural attacks.We start our analysis with remarks on the first and last affine layers.

Going through the First or Last Affine Layer. In addition to the resistance coming from the AES-box, the first and last affine layers play an important role in the strength of the final construction. The use of two keys in each T layer makes it hard to fix the value of one of the 128-bit block that enters an AES-box, but it also renders it difficult to set a specific difference.

Values. If we focus on one 128-bit block, the description of $a_{k'_0}$ implies that to determine s input bits entering a specific AES-box an attacker requires an s-bit guess of k'_0 (in addition to guesses on k_0). Since the same 128-bit value is used for each 128-bit AES-box, a guess for one specific AES-box input gives information for other boxes too, but the position of the known bits is different given that we add $2^{i-1}k'_0$ to the i-th 128-bit block.

Differences. Recall that the expression of the first affine layer is $T_{k_0,k'_0}(t,x) = (I \oplus A_{k_0})(x \oplus b_t) \oplus a_{k'_0} \oplus b_t$. Considering the case where a difference is set in both the tweak t and the input x and in which the aimed difference at the input of the first AES-boxes is d,

[9]Starting with a distinguisher might allow to only require to control input differences instead of differences and values for instance. As we detail in the following subsection some differences can be set at the input of the AES-boxes with no cost under the condition to consider related tweaks.

the equation that needs to be solved is:

$$\begin{aligned} & T_{k_0,k_0'}(t,x) \oplus T_{k_0,k_0'}(t',x') = d \\ \Leftrightarrow \quad & (I \oplus A_{k_0})(x \oplus x' \oplus b_t \oplus b_t') \oplus b_t \oplus b_t' = d \\ \Leftrightarrow \quad & (x \oplus x') = d \oplus (\tfrac{A_{k_0}}{k_0^*})(d \oplus b_t \oplus b_t') \end{aligned}$$

In case there is no tweak difference ($b_t = b_t'$), d can only be obtained by guessing the correct 128-bit key k_0. If there are differences both in the message and in the tweak a guess of k_0 is also required, except if $d = b_t \oplus b_t'$. However, this last case is very restricted as it corresponds to a difference pattern where each of the 128-bit difference entering the AES-boxes is the same and is equal to $t \oplus t'$. Obtaining difference patterns that are easy to propagate (like for instance one or several 128-bit zero differences) requires a key guess.

Yoyo Distinguisher. As explained in [RBH17], the yoyo technique allows to distinguish two generic SP rounds with only one pair of messages and one pair of (adaptive) ciphertexts. We discuss here the possibility of using this technique to distinguish or attack AES$_6$-CTET$^+$. First, the yoyo distinguisher can directly be applied to the 3 middle rounds of AES$_6$-CTET$^+$ (that is, the S-layer made by the w AES-boxes of the first round, the middle affine layer L_{k_1} and the second S-layer of w AES-boxes).

Assume that we manage to build a pair of messages (P_0, P_1) so that only one of the w AES-boxes of the first round is active (see Figure 2). Supposing that the last affine layer is absent, we can play the yoyo game, that is ask for the decryption of two modified ciphertexts $\tilde{C}_0, \tilde{C}_1$ constructed by swapping some (arbitrary) 128-bit words in the ciphertexts of P_0 and P_1.

With probability one the obtained plaintexts $\tilde{P}_0, \tilde{P}_1$ have the same activity pattern as P_0 and P_1 at the input of the first S-layer. Even without knowing the value of the secret key

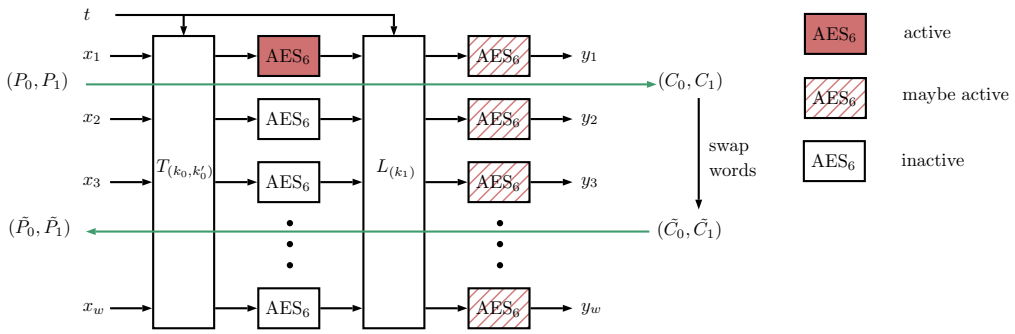

Figure 2: Yoyo game on the CTET$^+$ construction missing the last affine layer.

used in the first affine layer, an attacker can detect that the yoyo returned properly. Indeed, if $\tilde{P}_0$ and $\tilde{P}_1$ are such that (say) only the first AES-box is active, it means that their values can be written as $T_{(k_0,k_0')}(t, \tilde{P}_0) = (u_1, u_2, \ldots, u_w)$ and $T_{(k_0,k_0')}(t, \tilde{P}_1) = (u_1 \oplus \delta, u_2, \ldots, u_w)$. An expression of the difference between $\tilde{P}_0$ and $\tilde{P}_1$ is thus: $(c \oplus \delta, c, \ldots, c)$ where $c = \frac{k_0}{k_0^*} \times \delta$. The probability of observing such a pattern (equality of the differences of the last $w-1$ word) in the random case is equal to $2^{-128\times(w-2)}$ (we thus consider $w > 2$).

Cost of Building a pair of messages that differ in only one 128-bit block. The previous distinguisher relies on the assumption that an attacker can build a pair of messages that differ in only one (or a limited number) of the 128-bit word(s) after the first affine layer.

This matter is not trivial given that $T_{k_0,k_0'}$ depends on secret keys. Without lost of generality, the relation that $P_0 = (x_1, x_2, \ldots, x_w)$ and $P_1 = (x_1', x_2', \ldots, x_w')$ has to fulfill so that only the top AES input is active is:

$$P_0 \oplus P_1 = (I + \frac{A_k}{k^*}) \times (\Delta, 0, \ldots, 0)^T$$

where Δ is any non-zero value. It can be rewritten as:

$$\begin{cases} (x_1 \oplus x_1') = \Delta \oplus \Delta \times \frac{k_0}{k_0^*} \\ (x_2 \oplus x_2') = \Delta \times \frac{k_0}{k_0^*} \\ \ldots \\ (x_w \oplus x_w') = \Delta \times \frac{k_0}{k_0^*} \end{cases}$$

Solving this system requires to make a guess on the 128-bit value of k_0 (we possibly iterates on a little less than 2^{128} possibilities here given the condition that $k_0^* \neq 0$). For each guess of k_0 the attacker makes 3 queries, (the encryption of P_1, and the decryption of $\tilde{C}_0$ and $\tilde{C}_1$, while P_0 is common to all the input pairs) while as explained previously she directly spots that a guess is correct by noticing an equality of the difference of the last $(w-1)$ 128-bit words that indicates that the yoyo returned.

While this is the most promising attack so far, it already requires more queries than what we announced in our security claim.

Taking the last Affine Layer into Account. To fully adapt the yoyo technique to AES_6-CTET^+, the second difficulty comes from the necessity to do the swapping operation through $T_{(k_2,k_2')}$.

Denote $C_0 = (y_1, y_2, \ldots, y_w)$, $C_1 = (y_1', y_2', \ldots, y_w')$, $T^{-1}_{(k_2,k_2')}(t, C_0) = (z_1, z_2, \ldots, z_w)$ and $T^{-1}_{(k_2,k_2')}(t, C_1) = (z_1', z_2', \ldots, z_w')$. The objective is to build two new ciphertexts $\tilde{C}_0$ and $\tilde{C}_1$ by swapping some of the 128-bit words of $T^{-1}_{(k_2,k_2')}(t, C_0)$ and $T^{-1}_{(k_2,k_2')}(t, C_1)$. Without loss of generality, we consider that we are aiming for $T^{-1}_{(k_2,k_2')}(t, \tilde{C}_0) = (z_1', z_2', \ldots, z_w)$ and $T^{-1}_{(k_2,k_2')}(t, \tilde{C}_1) = (z_1, z_2, \ldots, z_w')$ that is swapping the first two 128-bit words.

The difficulty comes from the fact that the z_i and z_i' cannot be easily computed without the knowledge of k_2 and k_2'. One way to avoid guessing the two keys is to only focus on differences: by guessing k_2 we are able to compute $T^{-1}_{(k_2,k_2')}(t, C_0) \oplus T^{-1}_{(k_2,k_2')}(t, C_1) = (z_1 \oplus z_1', z_2 \oplus z_2', \ldots, z_w \oplus z_w')$ and thus we can easily deduce $\tilde{C}_0 = C_0 \oplus (I \oplus A_{k_2})(z_1 \oplus z_1', z_2 \oplus z_2', 0 \cdots 0)$ and $\tilde{C}_1 = C_1 \oplus (I \oplus A_{k_2})(z_1 \oplus z_1', z_2 \oplus z_2', 0 \cdots 0)$.

It appears to us that doing the required swap without guessing the 128-bit key k_2 is impossible, and thus that the yoyo technique is hard to apply in our setting.

Truncated Distinguisher. The previous discussion shows a key recovery requiring around 2^{128} operations to recover the key k_0 on a version of our proposal that misses the last affine layer. While this seems to be the best we can do with a yoyo technique, one can distinguish the same reduced version with a simple truncated technique. Assuming an attacker can control the input value of the first AES-box layer, she simply queries $x = (x_1, x_1, x_3, \ldots, x_w)$ and $x' = (x_1 \oplus \delta, x_1 \oplus \delta, x_3, \ldots, x_w)$. Since all the AES-box are equal the difference at the input of L_{k_1} is equal to $(\Delta, \Delta, 0 \cdots, 0)$ for some Δ. Given the description of L_{k_1} only the first 2 AES-boxes are active at the input of $T_{(k_2,k_2')}$, an event that result in the last $w-2$ output differences to be equal (so we set w according to the advantage we want). If the attacker can only control the input difference, the same output pattern can be obtained with probability 2^{-127} (assuming the worst case scenario where the AES-box is APN). Extending this over the first affine layer without exceeding the claim does not seem possible.

On the ASASA structure of CTET$^+$. At ASIACRYPT14, Biryukov et al. [BBK14] proposed to study the properties of a generic 5-layered SP-network alternating affine and Sbox layers, denoted ASASA. The A layers are (possibly different) affine transformations while the S layers consist in small (again possibly different) Sboxes applied in parallel. Among other scenario, they studied the security of the secret-key ASASA for which an attacker is given a black-box access to the cipher and has to recover the specification of each layer. The authors concluded that their 128-bit block instance using 8-bit Sboxes has a security of 128 bits.

This scenario is clearly very close to the one we are looking at with CTET$^+$: We have the same number and the same ordering of affine and non-linear layers, and the goal and possibilities of an attacker are similar. She can do encryption and decryption queries, and her objective is to recover the secret keys, which can be seen as hidding the definition of the various layers. One of the main difference between CTET$^+$ and the secret-key ASASA of [BBK14] lies in the security claim that respectively corresponds to the size of only one S-box and to the block size.

We thus make a small review of the existing attacks on the ASASA schemes to see if they apply to our construction.

- In the original paper [BBK14], Biryukov et al. gave a security analysis of a concrete instance of the Black-Box ASASA scheme that has 128-bit blocks and 8-bit Sboxes. Their analysis points out two properties: first, the algebraic degree of the cipher is smaller than for a random permutation, giving the possibility to distinguish it, without leading to an attack. Second, an integral property holding on the SASA construction might be extended to ASASA, but with a very low probability of 2^{-960}. They consequently claimed a security level equal to the block size, i.e. of 128 bits.

- [MDFK15] proposes several attacks on the ASASA construction for various of its application scenarios, with in particular one algebraic attack on the Black-Box ASASA. It starts by peeling off the last affine layer by using the observation that the maximum degree of the product of two bits at the output of the last S-layer is different if the two bits belong to the same Sbox or not. The final time complexity given by the authors is $N^2 2^{(M-1)^2}$ where M represents the Sbox size and N is the block size, which gives an attack in 2^{63} encryptions in the case of [BBK14] but clearly has an exorbitant complexity exceeding 2^{128} in the case of CTET$^+$ as we have $M = 128$ and $N = w \cdot 128$.

- Finally, [DDKL15] proposes three attacks. The first one is an integral attack which first step consists in summing over subspaces that span all the possible inputs of a specific Sbox, with a final complexity equal to $N \cdot 2^{3N/2}$. Since the claimed security of CTET$^+$ is $2^{N/w}$, this technique does not threaten it. The two other attack vectors use boomerang and differential techniques. In the first case the attack relies on a boomerang distinguisher of probability 2^{-2M+2}, resulting in a time complexity of roughtly $2^{3N/2+3M/2}$. This does not lead to an attack on CTET$^+$. Similarly the differential technique has a too high complexity as it starts by doing 2^{2N} queries.

In view of this discussion, the techniques used to analyze the ASASA proposal of [BBK14] do not threaten CTET$^+$.

From our security analysis it seems safe to propose an *agressive* claim which says that the keys of AES$_6$-CTET$^+$ cannot be recovered with a time complexity under 2^{127} encryption-equivalents[10].

[10] We do not claim 128-bit security since k_0 and k_2 have less than 128-bit entropy.

6 Conclusion

In this work, we have built upon the results on tweakable SPNs with independent round keys and permutations from [CDK+18] by constructing a 2-round tweakable SPN, based on a single secret permutation, that uses a significantly more efficient middle linear layer, while still offering the same level of beyond-birthday-bound security. Besides, we have proposed an actual instantiation of our scheme using a reduced round AES, and provided extensive cryptanalysis of the resulting tweakable block cipher, dubbed $\mathsf{AES}_6\text{-}\mathsf{CTET}^+$. We conclude by listing several open problems for future research:

1. can the amount of key material of CTET^+ be reduced?
2. can we find a more efficient SBU linear layer?
3. is Theorem 1 tight?

Acknowledgments

We would like to thank the anonymous reviewers for their valuable suggestions that helped improving the paper. This work was carried out in the framework of the French-German-Center for Cybersecurity, a collaboration of CISPA and LORIA and was partly supported by the french PIA project "Lorraine Université d'Excellence", reference ANR-15-IDEX-04-LUE. Jooyoung was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No.2019-0-01343, Regional strategic industry convergence security core talent training business). Part of this work was written while Benoît Cogliati was employed by the University of Luxembourg.

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), FIPS PUB 197, U.S. Department of Commerce, November 2001.

[BAK98] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A new block cipher proposal. In Serge Vaudenay, editor, *FSE'98*, volume 1372 of *LNCS*, pages 222–238. Springer, Heidelberg, March 1998.

[Bar19] Navid Ghaedi Bardeh. A key-independent distinguisher for 6-round AES in an adaptive setting. *IACR Cryptol. ePrint Arch.*, 2019:945, 2019.

[BBK14] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key (extended abstract). In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 63–84. Springer, Heidelberg, December 2014.

[BGL20] Zhenzhen Bao, Jian Guo, and Eik List. Extended truncated-differential distinguishers on round-reduced AES. *IACR Trans. Symmetric Cryptol.*, 2020(3):197–261, 2020.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid

Verbauwhede, editors, *CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, Heidelberg, September 2007.

[BKP16] Alex Biryukov, Dmitry Khovratovich, and Léo Perrin. Multiset-algebraic cryptanalysis of reduced Kuznyechik, Khazad, and secret SPNs. *IACR Trans. Symm. Cryptol.*, 2016(2):226–247, 2016. http://tosc.iacr.org/index.php/ToSC/article/view/572.

[CDK$^+$18] Benoît Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John P. Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - Proceedings, Part 1*, volume 10991 of *LNCS*, pages 722–753. Springer, 2018.

[CLL$^+$14] Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the Two-Round Even-Mansour Cipher. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 (Proceedings, Part I)*, volume 8616 of *LNCS*, pages 39–56. Springer, 2014. Full version available at http://eprint.iacr.org/2014/443.

[CS06a] Debrup Chakraborty and Palash Sarka. HCH: A New Tweakable Enciphering Scheme Using the Hash-Encrypt-Hash Approach. In Rana Barua and Tanja Lange, editors, *Progress in Cryptology - INDOCRYPT 2006*, volume 4329 of *LNCS*, pages 287–302. Springer, 2006.

[CS06b] Debrup Chakraborty and Palash Sarkar. A New Mode of Encryption Providing a Tweakable Strong Pseudo-random Permutation. In Matthew Robshaw, editor, *Fast Software Encryption - FSE 2006*, volume 4047 of *LNCS*, pages 293–309. Springer, 2006.

[CS14] Shan Chen and John Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version available at http://eprint.iacr.org/2013/222.

[DDKL15] Itai Dinur, Orr Dunkelman, Thorsten Kranz, and Gregor Leander. Decomposing the ASASA block cipher construction. Cryptology ePrint Archive, Report 2015/507, 2015. http://eprint.iacr.org/2015/507.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 371–387. Springer, Heidelberg, May 2013.

[DG08] Jeffrey Dean and Sanjay Ghemawat. MapReduce: Simplified Data Processing on Large Clusters. *Commun. ACM*, 51(1):107–113, January 2008.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 149–165. Springer, Heidelberg, January 1997.

[DKS$^+$17] Yevgeniy Dodis, Jonathan Katz, John P. Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable security of substitution-permutation networks. *IACR Cryptology ePrint Archive*, 2017:16, 2017.

[Dwo10] Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. *NIST SP 800-38E*, 2010.

[EM97] Shimon Even and Yishay Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. *J. Cryptology*, 10(3):151–162, 1997.

[FKL+01] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230. Springer, Heidelberg, April 2001.

[FM07] Scott R. Fluhrer and David A. McGrew. The Security of the Extended Codebook (XCB) Mode of Operation. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *SAC 2007: Selected Areas in Cryptography*, volume 4876 of *LNCS*, pages 311–327. Springer, 2007.

[GM00] Henri Gilbert and Marine Minier. A collision attack on 7 rounds of Rijndael. In *The Third Advanced Encryption Standard Candidate Conference, April 13-14, 2000, New York, New York, USA*, pages 230–241. National Institute of Standards and Technology,, 2000.

[GSWG18] Chun Guo, Yaobin Shen, Lei Wang, and Dawu Gu. Beyond-birthday secure domain-preserving PRFs from a single permutation. *Designs, Codes and Cryptography*, Aug 2018.

[Hal04] Shai Halevi. EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 315–327. Springer, 2004.

[Hal07] Shai Halevi. Invertible Universal Hashing and the TET Encryption Mode. In Alfred Menezes, editor, *Advances in Cryptology - Crypto 2007*, volume 4622 of *LNCS*, pages 412–429. Springer, 2007.

[HKR15] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 15–44. Springer, Heidelberg, April 2015.

[HLLT20] Phil Hebborn, Baptiste Lambin, Gregor Leander, and Yosuke Todo. Lower bounds on the degree of block ciphers. In *ASIACRYPT 2020, Part I*, LNCS, pages 537–566. Springer, Heidelberg, December 2020.

[HR03] Shai Halevi and Phillip Rogaway. A Tweakable Enciphering Mode. In Dan Boneh, editor, *Advances in Cryptology - Crypto 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, 2003.

[HR04] Shai Halevi and Phillip Rogaway. A Parallelizable Enciphering Mode. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, 2004.

[HT16] 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, *Advances in Cryptology - CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 3–32. Springer, 2016.

[IEE08] IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. *IEEE Std 1619-2007*, pages 17–30, April 2008.

[IK00] Tetsu Iwata and Kaoru Kurosawa. On the Pseudorandomness of the AES Finalists - RC6 and Serpent. In Bruce Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *LNCS*, pages 231–243. Springer, 2000.

[KS07] Liam Keliher and Jiayuan Sui. Exact maximum expected differential and linear probability for two-round advanced encryption standard. *IET Inf. Secur.*, 1(2):53–57, 2007.

[LP20] Gaëtan Leurent and Clara Pernot. New representations of the AES key schedule. *IACR Cryptol. ePrint Arch.*, 2020:1253, 2020.

[MDFK15] Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman. Key-recovery attacks on ASASA. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 3–27. Springer, Heidelberg, November / December 2015.

[MV15] Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. *J. ACM*, 62(6):46:1–46:29, December 2015.

[Pat08] Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.

[PSLL03] Sangwoo Park, Soo Hak Sung, Sangjin Lee, and Jongin Lim. Improving the upper bound on the maximum differential and the maximum linear Hull probability for SPN structures and AES. In Thomas Johansson, editor, *FSE 2003*, volume 2887 of *LNCS*, pages 247–260. Springer, Heidelberg, February 2003.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 217–243. Springer, Heidelberg, December 2017.

[RGR18] David Reinsel, John Gantz, and John Rydning. The Digitization of the World: From Edge to Core. *IDC White Paper*, 2018.

[WFW05] Peng Wang, Dengguo Feng, and Wenling Wu. The Security of the Extended Codebook (XCB) Mode of Operation. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *CISC 2005: Information Security and Cryptology*, volume 3822 of *LNCS*, pages 175–188. Springer, 2005.

A Description of the AES

The AES [AES01] takes as input a 128-bit state represented as a 4×4 matrix of bytes, numbered as shown in Figure 3. AES-128 uses a 128-bit key that goes through a key schedule producing 11 round keys denoted $K_0, \cdots K_{10}$. The 9 first rounds iterate 4 operations, described as follow:

AddRoundKey adds the 128-bit round key to the internal state,

SubBytes takes each of the 16 bytes of the internal state and modifies it with a 8×8 Sbox,

ShiftRows changes the position of the bytes inside of the internal state: the i-th row (where i varies from 0 to 3) is shifted by i bytes to the left,

MixColumns multiplies each column of the internal state by the circulant matrix $M = circ(02, 03, 01, 01)$

while the last round has no final MixColumns operation but an additional round key addition.

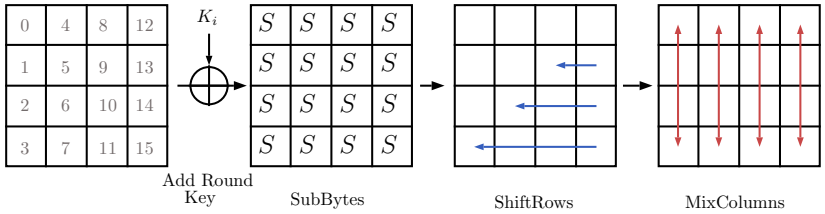

Figure 3: Round function of the Advanced Encryption Standard.