On Stream Ciphers with Provable Beyond-the-Birthday-Bound Security against Time-Memory-Data Tradeoff Attacks

Matthias Hamann and Matthias Krause

University of Mannheim, Germany
{hamann,krause}@uni-mannheim.de
http://th.informatik.uni-mannheim.de/

Abstract. We propose and analyze the LIZARD-construction, a way to construct keystream generator (KSG) based stream ciphers with provable $\frac{2}{3}n$-security with respect to generic time-memory-data tradeoff attacks. Note that for the vast majority of known practical KSG-based stream ciphers such attacks reduce the effective key length to the birthday bound $n/2$, where n denotes the inner state length of the underlying KSG. This implies that practical stream ciphers have to have a comparatively large inner state length (e.g., $n = 288$ bit for Trivium [6] and $n = 160$ bit for Grain v1 [16]).
The LIZARD-construction proposes a state initialization algorithm for stream ciphers working in packet mode (like the GSM cipher A5/1 or the Bluetooth cipher E_0). The proposal is that for each packet i the packet initial state q^i_{init} is computed from the secret session key k and the packet initial value IV^i via $q^i_{init} = P(k \oplus IV^i) \oplus k$, where P denotes a state mixing algorithm. Note that the recently published cipher LIZARD (see [14]), a stream cipher having inner state length of only 121 bit, is a lightweight practical instantiation of our proposal, which is competitive w.r.t. the usual hardware and power consumption metrics.
The main technical contribution of this paper is to introduce a formal ideal primitive model (in the sense of [12]) for KSG-based stream ciphers and to show the sharp $\frac{2}{3}n$-bound for the security of the LIZARD-construction against generic time-memory-data tradeoff attacks.

1 Introduction

The vulnerability against generic time-memory-data (TMD) tradeoff attacks like those of *Babbage* [3], *Biryukov and Shamir* [4], and *Dunkelman and Keller* [9] represents an inherent weakness of keystream generator-based (for short: KSG-based) stream ciphers. This vulnerability implies that for KSG-based stream ciphers working in *one-stream mode*[1] the effective key length is bounded by $\frac{n}{2}$, where n denotes the inner state length of the underlying KSG. As a consequence,

[1] One-stream mode means that an initial state is computed only once and the corresponding keystream is used for the whole session.

modern practical stream ciphers have comparatively large inner state lengths (e.g., 288 bit for the eSTREAM portfolio member Trivium [6] or 160 bit for the eSTREAM portfolio member Grain v1 [16]).

In this paper, we show how to design KSG-based stream ciphers with a provable beyond-the-birthday-bound security of $\frac{2}{3}n$ against generic TMD tradeoff attacks.

Our construction refers to stream ciphers working in the so-called *packet mode*, like the E_0 cipher of the Bluetooth system or the A5/1 cipher in the GSM standard. Such ciphers produce a keystream which is divided into packets of moderate length, where for each keystream packet i, the initial state $q^i_{init} = q^i_{init}(k, IV^i)$ for this packet is computed from the symmetric secret session key k and a packet-specific initial value (IV) IV^i according to a *state initialization algorithm*.

As in many communication scenarios data streams are encrypted and transmitted packet-wise (Bluetooth, WLAN, cellular networks etc.), it seems natural to consider stream ciphers working in packet mode (see [14] for more practical examples of stream ciphers working in packet mode and more information about the practical relevance of such ciphers).

We focus on analyzing the influence of the state initialization algorithm on the security against generic session key recovery and packet prediction TMD tradeoff attacks.

Note that the state initialization algorithms of E_0 and A5/1, two prominent practical examples of stream ciphers working in packet mode, are of type

$$q^i_{init}(k, IV^i) = P\left(L(k) \oplus L'(IV^i)\right),$$

which provides only a security level of $\frac{n}{2}$ w.r.t. session key recovery attacks. Here, L, L' denote $GF(2)$-linear mappings, and $P : \{0,1\}^n \longrightarrow \{0,1\}^n$ denotes the state mixing algorithm of the cipher.[2]

The main contribution of this paper is to show that stream ciphers using a state initialization algorithm of type

$$q^i_{init}(k, IV^i) = P\left(k \oplus IV^i\right) \oplus k \tag{1}$$

reach a security level of $\frac{2}{3}n$ w.r.t. session key recovery attacks and even w.r.t. so-called *packet prediction attacks*. Note here that in a previous version of this paper, the algorithmic scheme (1) was called $FP(1)$-mode and as such it is referenced by the designers of Lizard in [14].

We prove our security bound by introducing, in the sense of *Gazi and Tessaro* [12], an ideal primitive model (IPM) for KSG-based stream ciphers working in packet mode and show a tight information-theoretic $\frac{2}{3}n$ security bound against

[2] The aim of the mixing algorithm is to provide enough diffusion, confusion and high algebraic degree in the dependencies of the initial state bits from the session key bits and IV bits. The easiest way to perform the mixing algorithm is by clocking the KSG a sufficiently large number of times without producing keystream, see e.g. Trivium.

key recovery and packet prediction attacks for ciphers which use a state initialization algorithm of type (1).

To the best of our knowledge, this is the first time that a formal model for the security of stream ciphers against generic time-memory-data tradeoff attacks is considered. So far, similar IPMs were used, e.g., for analyzing the security of operation modes of block ciphers, of key-alternating block cipher constructions (see the framework of iterated Even-Mansour ciphers), or of cryptographic hash functions, but not for stream ciphers.

Very recently, the specification of the lightweight stream cipher LIZARD [14] has been published. LIZARD works in packet mode with a packet length of $R \leq 2^{18}$ bit, has a state initialization algorithm of type (1), and an inner state length of 121 bit. The design features of LIZARD presented in [14] show that our design principle *packet mode + state initialization of type (1)* allows for lightweight practical instantiations which are competitive w.r.t. all relevant hardware and power consumption metrics.

Note that *Armknecht and Mikhalev* suggested with Sprout [2] another approach for obtaining KSG-based stream ciphers with beyond-the-birthday-bound security against generic TMD tradeoff attacks (see also [13], where another cipher named Fruit, also basing on this principle, has been presented). The idea here is that the session key is not only accessed during the state initialization but also continuously used as part of the state update function (see [14] for a discussion about the practical hardware and energy efficiency of this approach). It has to be mentioned here that, so far, security proofs showing a beyond-the-birthday-bound security against generic TMD tradeoff attacks for the Sprout-construction are missing.

In the remaining part of this introduction, we provide some basics on KSG-based stream ciphers (subsection 1.1), TMD tradeoff attacks (subsection 1.2), and motivate and describe our results in more detail (subsection 1.3).

1.1 Stream Ciphers

Stream ciphers are symmetric encryption algorithms intended for encrypting, in an online manner, plaintext bitstreams X which have to pass an insecure channel. The encryption is performed via bitwise addition of a keystream S to X, which is generated in dependence of a secret session key k and public initial values. The legal recipient, who also knows k, decrypts the encrypted bitstream $Y = X \oplus S$ by generating S and computing $X = Y \oplus S$. The secret session key k is typically generated in the first phase of a session by executing a key exchange protocol. This session key generation phase will not be considered in this paper.

We consider stream ciphers working in *packet mode*, which means that a session is divided into packet steps, and that the keystream S and plaintext X are generated and encrypted packet-wise. Let $X = X^1X^2X^3\cdots$ and $S = S^1S^2S^3\cdots$ denote the corresponding partition of the plaintext X and the keystream S into packets. It holds $|X^i| = |S^i| \leq R$ for all $i \geq 0$ and some parameter R called the packet length. In each packet step i, the keystream packet S^i is generated in dependence of k and an initial value IV^i, and X^i is encrypted via $X^i \oplus S^i$.

We consider stream ciphers which are defined by KSGs. KSGs are clock-controlled devices which can be formally specified by finite automata, defined by an inner state length n, the set of inner states $\{0,1\}^n$, a state update function $\pi : \{0,1\}^n \longrightarrow \{0,1\}^n$ and an output function $out : \{0,1\}^n \longrightarrow \{0,1\}^*$. Starting from an initial state q_1, in each clock cycle $t \geq 1$, the KSG produces a piece of keystream $z_t = out(q_t)$ and changes the inner state according to $q_{t+1} = \pi(q_t)$. The output bitstream $S(q_1)$ is defined by concatenating all the outputs $z_1 z_2 z_3 \cdots$.

Note that in this paper, we consider only KSGs which produce one bit per clock cycle.

Packet mode for KSG-based stream ciphers means that each packet step $i \geq 0$ starts with computing an initial inner state $q^i_{init} = q^i_{init}(k, IV^i)$ from the secret session key k and an initial value IV^i. Then, the keystream packet S^i is generated as the prefix of length R of the keystream $S(q^i_{init})$.

The opposite of the packet mode would be the *one-stream mode*, in which only one initial state $q_{init} = q_{init}(k, IV)$ per session is generated and where the keystream $S = S(q_{init})$ is used for the whole session. Trivium [6] and Grain [16] can be considered examples of stream ciphers designed for one-stream mode due to their extremely large limits (e.g., 2^{64} bits for Trivium) on the amount of keystream generated under a single key-IV pair.[3]

Besides the KSG, the second main component of a stream cipher is the *state initialization algorithm*, which defines how the initial state $q^i_{init} = q^i_{init}(k, IV^i)$ for the i-th keystream packet is computed from k and the initial value IV^i.

The state initialization algorithm is typically performed by the KSG and divided into the following three phases:

(1) The **loading phase** defines how k and IV^i are loaded into the inner state registers and results in a loading state $q^i_{load} = q^i_{load}(k, IV^i)$.
(2) The **mixing phase** runs an appropriate KSG-based mixing algorithm on q^i_{load} and results in a mixing state $q^i_{mixed} = q^i_{mixed}(q^i_{load})$.
(3) The **hardening phase**, which computes q^i_{init} from q^i_{mixed} and, possibly, k and IV^i.

The aim of the mixing phase (2) is to generate a sufficient amount of diffusion, confusion, high algebraic degree etc. in the dependencies of the initial state bits from the session key bits. Concerning (3), note that in many previous cases we had $q^i_{init} = q^i_{mixed}$.

We formalize the process of state initialization and keystream generation of KSG-based stream ciphers by identifying the following primitives $P, \tilde{F} : \{0,1\}^n \longrightarrow \{0,1\}^n$, where n denotes the inner state length of the underlying keystream generator.

For all $y \in \{0,1\}^n$, the function value $\tilde{F}(y) \in \{0,1\}^n$ is defined as the sequence of the first n keystream bits generated on the inner state y. Clearly, $\tilde{F}$ should be *preimage resistant* in the sense that it is infeasible to compute, for

[3] Clearly, Trivium and Grain could also be used in packet mode but, in contrast to, e.g., LIZARD [14], their design is not specifically optimized for such scenarios.

given $z \in \{0,1\}^n$, a value $y \in \{0,1\}^n$ fulfilling $\tilde{F}(y) = z$. Otherwise, for instance, it would be feasible to predict, on the basis of the first n keystream bits of a packet, all remaining keystream bits of this packet.

Note that the n-block of bits r to $r+n-1$ of the keystream packet S^i can be expressed as

$$(S^i_r, \cdots, S^i_{r+n-1}) = \tilde{F}\left(\pi^r(q^i_{init})\right). \tag{2}$$

We use further the primitive $P : \{0,1\}^n \longrightarrow \{0,1\}^n$ for modeling the mixing phase, i.e., for all $u \in \{0,1\}^n$, the value $P(u)$ denotes q^i_{mixed} if $u = q^i_{load}$. Standard efficiency and security assumptions on KSGs imply that P should be an efficiently computable function which behaves like a random function with respect to several combinatorial properties.

Let us describe the state initialization algorithm of some relevant stream ciphers and express them by our formalism:

Trivium: The stream cipher Trivium has an inner state of length 288 bit, distributed over three nonlinear feedback shift registers (NFSRs) of lengths 93 bit, 84 bit, and 111 bit. The state update function consists of the corresponding three feedback functions, which in each case are quadratic and take their inputs from two of the three NFSRs. The linear output function XORs six inner state bits, two from each NFSR. The loading state $q_{load}(IV, CONST, k)$ is defined to be the concatenation of the 80-bit session key k, the 80-bit IV IV and a predefined 128-bit constant $CONST$. In the mixing phase, the KSG is clocked $4 \cdot 288$ times without producing output (see [6] for more details). Consequently,

$$q_{init} = q_{mixed} = P(IV||CONST||k). \tag{3}$$

Grain v1: The stream cipher Grain v1 has an inner state of length 160 bit, distributed over one NFSR and one linear feedback shift register (LFSR), both of length 80 bit. The state update function consists of the corresponding two feedback functions, where the NFSR feedback function depends also on one of the LFSR bits. The output function produces one keystream bit per clock cycle and depends nonlinearly on five LFSR bits and one NFSR bit and linearly on further seven NFSR bits. The loading state $q_{load}(IV, CONST, k)$ is defined to be the concatenation of the 80-bit session key k, a 64-bit IV IV and a predefined 16-bit constant $CONST$. In the mixing phase, the Grain-KSG is clocked 160 times, where, in each clock cycle, the corresponding output keystream bit is XORed to the result of each of the two feedback functions (see [16] for more details). Consequently, we have again

$$q_{init} = q_{mixed} = P(IV||CONST||k). \tag{4}$$

Bluetooth-E_0: E_0 works in packet mode with a packet length $R \leq 2745$ bit.[4] The inner state length is 132 bit, distributed over four LFSRs of overall length 128 bit and an extra finite state machine of inner state length four bit. The state

[4] More exactly, if the so-called *basic rate* is used, Bluetooth data packets contain at most 2745 bits of payload, which are encrypted using the E_0 cipher.

update function updates all LFSRs separately. The state transition of the 4-bit finite state machine additionally depends on four bits from the LFSRs. The output function XORs the output bits of the LFSRs with the nonlinear output of the finite state machine.
For each packet step i, the initial value IV^i is composed of the 48-bit Bluetooth address of the master device, 26 bits of the master's clock (to which both devices are synchronized) at the time of the first transmission slot of the packet i and two 3-bit constants. The E_0 cipher loads k and IV^i stepwise to the register cells of the KSG, resulting in the inner state $q^i_{load} = L(k) \oplus \tilde{L}(IV^i)$, where $L, \tilde{L}$ denote linear functions defined by the four linear feedback shift registers of the E_0-KSG. Subsequently, the generator is clocked 56 times and the output is discarded. Based on the resulting inner state of the E_0-KSG, 128 keystream bits are then computed without outputting them. Instead, they are copied into the LFSR register cells, overwriting the old inner state (see [19] for more details). Consequently, the state initialization algorithm of E_0 can be modeled as

$$q^i_{init} = q^i_{mixed} = P\left(L\left(k\right) \oplus \tilde{L}\left(IV^i\right)\right). \tag{5}$$

LIZARD: The definition of LIZARD is highly inspired by the Grain family [15] of stream ciphers. In opposite to Grain, LIZARD is designed for working in packet mode with a packet length of up to 2^{18} bit. It has an inner state length of 121 bit, distributed over two NFSRs of lengths 90 bit and 31 bit, and a nonlinear output function (see [14] for more details). The prominent innovation of LIZARD is that the state initialization algorithm is designed according to the scheme (1) mentioned above with some minor adaptions (see section 3.5 in [14] for a detailed discussion of how LIZARD implements the generic construction presented here).

1.2 Attacks against Stream Ciphers

During the last decades, many KSGs for practical use have been suggested and many different techniques for cryptanalyzing stream ciphers have been developed (correlation attacks, fast correlation attacks, guess-and-verify attacks, BDD attacks, cube attacks etc.).

Attacks on stream ciphers typically suppose that the attacker knows a piece S' of keystream. Typical goals of attacks are to distinguish S' from a truly random bitstream, to recover inner states responsible for S', to predict a new keystream packet on the basis of S', or to recover the secret session key.

In this paper, we concentrate on analyzing the security of stream ciphers running in packet mode with respect to generic TMD tradeoff attacks which try to recover the secret session key k or to predict a new packet on the basis of black-box access to the primitives $\tilde{F}$ and P, and on the basis of a set of keystream packets generated w.r.t. to k and publicly known initial values.

For illustration purposes, let us shortly demonstrate how the idea of the TMD tradeoff attack of *Babbage* [3] can be applied to stream ciphers working

in packet mode. Suppose that the attacker knows a collection $\mathcal{S}$ of pieces of keystream which can have their origin in different packets of one session and which contain s different subsequences of n consecutive keystream bits. Then the attacker generates a set T of pairs $(y, \tilde{F}(y))$ for randomly chosen inner states $y \in \{0,1\}^n$. If $s \cdot |T| \approx 2^n$, then, with high probability, there is some pair $(y, \tilde{F}(y)) \in T$ such that $\tilde{F}(y)$ occurs as a subsequence of length n in one of the keystream pieces contained in $\mathcal{S}$. With high probability, y is responsible for this piece of keystream. As the state transition function π is usually efficiently invertible, this allows to efficiently compute the secret initial state q^i_{init} of the corresponding packet. Hence, one gets a TMD tradeoff attack of $\tilde{O}(2^{n/2})$ for computing the initial state of one packet.

If we were in the one-stream mode, the attacker would be done, as, with the knowledge of the only initial state q_{init}, the whole remaining bitstream of this session could be computed. Note here that the state initialization algorithms of Trivium and Grain v1 are designed in such a way that the secret session key k can be efficiently computed from q_{init}.

However, in the packet mode, the knowledge about the initial state for one packet does not suffice for predicting future packets of this session. For reaching this goal, it would be sufficient to recover the secret session key k.

Consequently, to achieve beyond-the-birthday-bound security against generic TMD tradeoff attacks, the state initialization algorithm has to ensure that the session key cannot be efficiently derived from the packets' initial states.

1.3 Our Results

Our results are based on introducing, in the sense of [12], an *ideal primitive model (IPM)* for KSG-based stream ciphers, which allows to prove information theoretic security lower bounds w.r.t. to generic chosen-IV attackers who have black-box access to the primitives, i.e. the components of the cipher. Note that all types of generic TMD tradeoff attacks against stream ciphers which are known from the literature can be formulated as attacks in this IPM in a straightforward way. As mentioned above, the relevant components, which will be modeled as ideal primitives, are the function $\tilde{F} : \{0,1\}^n \longrightarrow \{0,1\}^n$, assigning to each inner state the block of the next n keystream bits, and the permutation $P : \{0,1\}^n \longrightarrow \{0,1\}^n$ corresponding to the mixing algorithm. In our IPM, we define P to be a random permutation over $\{0,1\}^n$ and $\tilde{F}$ to be a random π-iterative function, where π-iterativeness means that for all inputs $y \in \{0,1\}^n$, the suffix of $\tilde{F}(y)$ of length $n-1$ equals the prefix of $\tilde{F}(\pi(y))$ of length $n-1$. This reflects exactly the output behavior of a KSG which produces always one keystream bit per clock cycle. Again, π denotes the state transition function, which is not counted as an ideal primitive but given as a global parameter fulfilling certain combinatorial properties.

Our security analysis will consist in analyzing the success probability of an attacker Eve to win a certain *packet prediction game* against an honest player Alice. This game is defined in a way which is common standard in the context of formal IP-models. Alice chooses a random session key $k \in \{0,1\}^n$, a random

permutation P and a random π-iterative function $\tilde{F}$. Eve is allowed to pose component queries, i.e., oracle queries to a P-, a P^{-1}-, and an $\tilde{F}$-oracle[5]. Moreover, Eve is allowed to pose construction queries with inputs $x \in \{0,1\}^n$, which are answered by Alice with the keystream packet $E(x)$ corresponding to session key k and initial value x. The aim of Eve is to submit a pair $(x^*, E(x^*))$ for an initial value x^* which did not occur as input of a construction query posed before.

Our main results is to derive a sharp bound on the security of the LIZARD-variant of the packet prediction game (for short, the LIZARD-PPG), which means that construction queries are answered in accordance with the LIZARD-construction (see relation (1)).

Upper Bounds w.r.t. key recovery attacks: We show that Eve can win the LIZARD-PPG with success probability 1/2 with $O(2^{(2/3)n})$ oracle queries. The corresponding attack combines a randomized algorithm for constructing a sufficiently large number of pairs $(x, y) \in \{0,1\}^n \times \{0,1\}^n$ for which $E(x)$ has prefix $\tilde{F}(y)$ with the Slidex-attack of *Dunkelman, Keller, Shamir* [10] against the Even-Mansour cipher (see [11]).

Upper Bounds w.r.t. distinguishing attacks: It is important to note that for a packet length of $R > n$, the security of KSG-based stream ciphers working in packet mode w.r.t. *distinguishing TMD tradeoff attacks* is bounded by only $O(2^{n/2})$. We sketch a corresponding attack. It is possible to compute with TMD-cost $O(2^{n/2})$ a pair $(x, y) \in \{0,1\}^n \times \{0,1\}^n$ for which $E(x)$ has prefix $\tilde{F}(y)$. In the pseudorandom case, w.h.p. bit $n+1$ of $E(x)$ equals the last bit of $\tilde{F}(\pi(y))$. But in the random case, in which construction queries are answered according to a truly random function $E : \{0,1\}^n \longrightarrow \{0,1\}^R$, the probability for this event is exactly 1/2. In the appendix section A, we describe a formal model for the security of stream cipher constructions w.r.t. distinguishing attacks and formulate the $O(2^{n/2})$-attack for packet length $R > n$ in terms of this model.

Lower Bounds w.r.t. key recovery and packet prediction attacks: Our main technical contribution consists in the proof of a matching security lower bound implying that for all constants $\alpha < 2/3$, the success probability of Eve to win the LIZARD-PPG with $O(2^{\alpha \cdot n})$ oracle queries is bounded by $2^{-\epsilon \cdot n}$ for some constant $\epsilon > 0$.

The way our lower bound proof is organized is inspired by the typical structure of similar proofs which occur in the context of the security analysis of iterated Even-Mansour ciphers (see, e.g., [11], [5], [1], [8], [7], [17]). Note here that at several places, our proof uses a very nontrivial combinatorial argument, the so-called Sum-Capture Theorem, which was developed in [7] for proving matching security lower bounds for minimized Even-Mansour ciphers of iteration depth two.

A main difference lies in the fact that our lower bound concerns attackers who have the aim to recover the secret session key or to predict a new package, while the lower bounds for Even-Mansour ciphers typically refer to distinguishing attackers. This implies that well-established proof techniques like *Patarin's H*-coefficient [18] technique can not be directly applied in our scenario. The rough

[5] Note that the absence of an $\tilde{F}^{-1}$-oracle reflects the preimage resistency of $\tilde{F}$.

idea of our proof is to show that if the number of oracle queries is bounded by $O(2^{\alpha \cdot n})$, then, from Eve's point of view, the entropy of the secret session key is still larger than $n/2$, which implies only an exponentially small success probability for recovering the session key or predicting a correct packet.

The paper is organized as follows. In section 2, we introduce our ideal primitive model for stream ciphers including the packet prediction game. Section 3 is devoted to the $O(2^{(2/3)n})$-attack against the LIZARD-construction, while section 4 contains the lower bound results. Section 5 concludes the paper by summarizing our results and showing some directions of further research. Due to space restrictions, some parts of the lower bound proofs had to be shifted into the appendix.

2 Formal Description of Stream Ciphers and a Security Model for the LIZARD-Construction

In this section, we introduce a formal ideal primitive model (IPM) for KSG-based stream ciphers and define a prediction game between a secret-holder Alice and an adversary Eve which models generic TMD tradeoff attacks against the LIZARD-construction.

Definition 1. *A stream cipher construction is an* 8*-tuple*

$$(n, KL, IVL, R, \pi, P, F, \hat{E}),$$

where

- *parameter* n *corresponds to the inner state length of an underlying KSG,*
- KL*,* IVL *and* R *correspond to the session key length, the initial value length, and the packet length, respectively.*
- π *denotes a bijective function* $\pi : \{0,1\}^n \longrightarrow \{0,1\}^n$ *corresponding to the state transition function.*
- $P : \{0,1\}^n \longrightarrow \{0,1\}^n$ *denotes the function corresponding to the mixing algorithm of the cipher as described in subsection 1.1.*
- $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ *denotes the function assigning to each inner state* $y \in \{0,1\}^n$ *the* n*-bit keystream block* $F(y)$ *generated on* y *as described in subsection 1.1.*
- $\hat{E} : \{0,1\}^{KL} \times \{0,1\}^{IVL} \longrightarrow \{0,1\}^R$ *denotes the function assigning to each pair* (k, IV) *the keystream packet generated on session key* k *and packet initial value* IV*.*

Definition 2. *The* LIZARD*-construction is defined to be a stream cipher construction which additionally fulfills the following four conditions.*

(L1) It holds $n = KL = IVL$ *and* $R \geq n$*.*

(L2) The function F *is* π*-iterative in the sense that for all* $y \in \{0,1\}^n$ *it holds that the suffix of length* $n-1$ *of* $F(y)$ *equals the prefix of length* $n-1$ *of* $F(\pi(y))$*.*

(L3) For all $k, x \in \{0,1\}^n$ *it holds that*

$$\hat{E}(k,x) = (z_0, z_1, \cdots, z_{R-1})$$

where for all r, $0 \leq r \leq R-n$, *it holds*

$$(z_r, z_{r+1}, \cdots, z_{r+n-1}) = F(\pi^r(P(x \oplus k) \oplus k)).$$

(L4) For all inner states $y \in \{0,1\}^n$ *the period of the sequence* $(\pi^r(y))_{r \geq 0}$ *is larger than* R.

Note here that the stream cipher LIZARD, as defined in [14], differs from the design features of the LIZARD-construction in some minor points, which do not harm our security bounds. For instance, in contrast to condition (L1), the IV length of LIZARD is smaller than the inner state length. Observe that in our situation a smaller IV length lowers the power of a chosen-IV attacker.

We assign to each stream cipher construction an IPM by considering the functions P and F as ideal primitives, which can be evaluated by a possible attacker via black-box access. Note that the function $\hat{E}$ depends on P and F and describes how these components play together in computing, for given session key k and packet initial value IV, the corresponding keystream packet. Conditions (L2) and (L3) reflect the fact that exactly one keystream bit per clock cycle is generated.

In particular, we define the ideal primitive P to be a random permutation over $\{0,1\}^n$, and we allow the attacker Eve to have black-box access to a P- and to a P^{-1}-oracle.

Moreover, we define the ideal primitive F to be a random π-iterative function. The preimage resistance of F is reflected by the fact that Eve does not have access to an F^{-1}-oracle.

Note that random, uniformly distributed π-iterative function can be generated as follows:

Generating a random π-iterative function F:

Note that, as π is bijective, the connected components of the undirected graph $G_\pi = (\{0,1\}^n, E_\pi)$, where $E_\pi = \{(v, \pi(v)); v \in \{0,1\}^n\}$, are simple circuits $C^1, \cdots, C^s$ of sizes $d_1, \cdots, d_s$, which we call π-circuits.

For each π-circuit C^j, $1 \leq j \leq s$, fix a starting point $x_0^j \in C^j$.

Note that $C^j = \{x_0^j, \cdots, x_{d_j-1}^j\}$, where for all i, $1 \leq i \leq d_j - 1$ it holds $x_i^j = \pi^i(x_0^j)$,

A uniformly distributed π-iterative function F can be defined by choosing for all j, $1 \leq j \leq s$, randomly and independently a uniformly distributed bitstring

$$b^j = (b_0^j, \cdots, b_{d_j-1}^j) \in \{0,1\}^{d_j}$$

and defining $F(x_i^j)$ for all i, $0 \leq i \leq d_j - 1$, by

$$F(x_i^j) = (b_i^j, b_{i+1 \mod d_j}^j \cdots, b_{i+n-1 \mod d_j}^j).$$

We model the security of the LIZARD-construction against generic TMD tradeoff attacks by the adversary Eve's success probability to win the following *packet prediction game* with a limited number of oracle queries against Alice. Informally, we consider an adversary Eve who has black-box access to the ideal components P and F and is allowed to ask for keystream packets generated w.r.t. a secret session key k and IVs x of Eve's choice. Eve wins the game if, after asking a certain number of oracle queries, she is able to predict a new keystream packet w.r.t. to a new IV, which has not been asked before.

Definition 3. *(i) The game depends on the global parameters π, M, n, R, where π denotes a fixed bijective state transition function $\pi : \{0,1\}^n \longrightarrow \{0,1\}^n$, M, n, R denote natural numbers, and n, R, π fulfill the conditions [A1, A2]. The game is divided into a query phase and a prediction phase.*

(ii) At the beginning, Alice chooses randomly and w.r.t. the uniform distribution a secret triple $\omega = (k_\omega, P_\omega, F_\omega)$, where

- *$k_\omega \in \{0,1\}^n$ denotes the secret session key,*
- *$P_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ denotes a random permutation,*
- *$F_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ denotes a random π-iterative function.*

We denote by Ω the corresponding probability space of all such triples together with the uniform distribution.

(iii) The adversary Eve is supposed to be a randomized oracle algorithm of potentially unbounded computational power, who is allowed to pose component oracle queries of type $P(u) =?$, or $P^{-1}(v) =?$, or $F(y) =?$ for inputs $u, v \in \{0,1\}^n$ and $y \in \{0,1\}^n$, which are correctly answered by Alice by $P_\omega(u)$, $(P_\omega)^{-1}(v)$, or $F_\omega(y)$, respectively.

(iv) Moreover, Eve poses construction queries of the form $E(x) =?$, where $x \in \{0,1\}^n$, which will be answered by Alice with the keystream packet $E_\omega(x)$ corresponding to the initial state $y := P_\omega(x \oplus k_\omega) \oplus k_\omega$ induced by the session key k_ω and the initial value x. Note that this keystream packet $E_\omega(x)$ is the concatenation of R/n F-values. In particular,

$$E_\omega(x) = F_\omega(y)||F_\omega(\pi^n(y))||F_\omega(\pi^{2n}(y))||\cdots||F_\omega(\pi^{(R/n-1)n}(y)).$$

(v) In the query phase, Eve poses exactly M oracle queries. In the prediction phase, Eve has to submit a pair $(x, z) \in \{0,1\}^n \times \{0,1\}^n$, where x does not occur as input of an E-query in the query phase. Eve wins if $z = F_\omega(P_\omega(x \oplus k_\omega) \oplus k_\omega)$, i.e., if z equals the block of the first n bits of the keystream packet $E_\omega(x)$ corresponding to the initial state $P_\omega(x \oplus k_\omega) \oplus k_\omega$, i.e., the keystream packet corresponding to session key k_ω and initial value x.

(vi) Besides the running time and the number M of oracle queries, the essential cost parameter is the winning probability of Eve, which is measured with respect to the uniform distribution on Ω and the internal randomization of Eve.

3 Upper Bounds

Theorem 1. *Eve can win the packet prediction game, described in Definition 3, with winning probability* $1/2$ *with* $M = \mathcal{O}(2^{2/3 \cdot n})$ *oracle queries in running time* $\mathcal{O}(2^{2/3 \cdot n})$.

Proof (Theorem 1). We sketch a key-recovery attack for the case that $R = n$. This attack can be easily applied also for greater packet lengths by considering only the first n bits of the packets generated during the attack.

According to Definition 3 we suppose that Alice chooses a random elementary event $\omega = (k_\omega, P_\omega, F_\omega) \in \Omega$. Remember that $k_\omega \in \{0,1\}^n$, $P_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ is a random permutation, and $F_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ is a random π-iterative function.

Note that, with the knowledge of the secret session key k_ω, Eve can choose some random $y \in \{0,1\}^n$, compute $z = F_\omega(y)$ and $x = P_\omega^{-1}(y \oplus k_\omega) \oplus k_\omega$ by one further F- and a further P^{-1}-query. Eve wins in the prediction phase with (x, z) with high probability.

Let $E_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ denote the construction function corresponding to ω, which is, as $R = n$, for all $x \in \{0,1\}^n$ defined by

$$E_\omega(x) = F_\omega(P_\omega(x \oplus k_\omega) \oplus k_\omega).$$

Let us further denote by $EM_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ the function which, to each IV x, assigns the corresponding packet initial state, i.e.,

$$EM_\omega(x) = P_\omega(x \oplus k_\omega) \oplus k_\omega.$$

Note that EM_ω corresponds to the one-key variant of the Even-Mansour cipher of iteration depth 1 (see, e.g., [11]). Our attack uses the Slidex attack of *Dunkelman, Keller, and Shamir* [10] against this Even-Mansour cipher as a subroutine.

In a first phase, Eve uses $\mathcal{O}(2^{2/3 \cdot n})$ E- and F-queries oracle queries to construct a set of pairs $\{(x, EM_\omega(x)); x \in X^*\}$ for a set $X^* \subseteq \{0,1\}^n$ of size $\Theta(2^{1/3 \cdot n})$.

She does this by generating a sufficiently large set $Coll = \{(x, y); x \in X^*, y \in \{0,1\}^n\}$ of so-called *EF-collisions*, where $|X^*| = \Omega(2^{1/3 \cdot n})$. Here, a pair (x, y) is called EF-collision if $E_\omega(x) = F_\omega(y)$. It can be shown quite straightforwardly that for any EF-collision (x, y), it holds that $EM_\omega(x) = y$ with high probability.

In particular, Eve first generates a set of pairs $\{(x, E_\omega(x)); x \in X\}$ for a set $X \subseteq \{0,1\}^n$ of size $\Theta(2^{2/3 \cdot n})$. Then, Eve generates pairs $(y, F_\omega(y))$ for randomly chosen elements $y \in \{0,1\}^n$ and puts (x, y) to $Coll$ if $E_\omega(x) = F_\omega(y)$ for some x in X. Note that the probability for this event is $|X|/2^n$. Consequently, after $\Theta(2^{2/3 \cdot n})$ rounds of choosing values y, the set $Coll$ has the desired size $\Omega(2^{1/3 \cdot n})$ with high probability.

In a second phase, Eve chooses random elements $u \in \{0,1\}^n$ and asks Alice for $P_\omega(u)$. Eve stops with u if

$$x \oplus u = P_\omega(u) \oplus EM_\omega(x) \tag{6}$$

for some $x \in X^*$ and publishes the hypothesis $k_\omega = u \oplus k$.

Note that this hypothesis is correct if the choice of u generates a so-called *sudden death pair* (u, x) where $x \in X^*$ and $u \oplus x = k_\omega$. This implies, by definition,

$$x \oplus u = k_\omega = P_\omega(x \oplus k_\omega) \oplus EM_\omega(x) = P_\omega(u) \oplus EM_\omega(x).$$

Consequently, Eve is successful after choosing an element $u \in X^* \oplus k_\omega$, which happens after

$$\frac{2^n}{|X^*|} = \Theta\left(2^{\frac{2}{3}n}\right)$$

rounds of choosing elements u with high probability. □

4 The Security Lower Bound Proof

4.1 Preliminaries

In this section, we show the main result of this paper, a sharp security lower bound for the LIZARD-construction. At several places, our lower bound proof uses a combinatorial result proved by *Chen, Lampe, Lee, Seurin, Steinberger* in [7], namely Theorem 1 in section 3, which is known as *Sum Capture Theorem*.

For motivating the use of this result note first that, from Eve's point of view, it is desirable to generate a sufficiently large set of triples (u, x, y) for which $x \oplus u = P_\omega(u) \oplus y$, as such triples give nontrivial information about the secret session key k_ω.

In particular, if $F_\omega(y)$ is not equal to the prefix of $E_\omega(x)$ of length n, then $x \oplus u \neq k_\omega$. If $F_\omega(y)$ equals to the prefix of $E_\omega(x)$ of length n then, with high probability, (u, x) forms a sudden death pair in the sense of the proof of Theorem 1, and $u \oplus k$ is a good hypothesis for k_ω.

Let us recall the Sum-Capture Theorem from [7] in a slightly modified form.

Theorem 2. *Let P denote a uniformly random permutation over $\{0,1\}^n$, let $N = 2^n$ and fix an arbitrary number M, $9n \leq M \leq N/2$. Suppose that Eve (who is supposed to be a probabilistic algorithm) poses a sequence $U = \{u_1, \cdots, u_M\}$ of M P-queries. For any subsets $X, Y \subseteq \{0,1\}^n$ let*

$$\mu(P, U, X, Y) = |\{(u, x, y) \in U \times X \times Y; x \oplus u = y \oplus P(u)\}|.$$

Then the probability for the event that there are subsets $X, Y \subseteq \{0,1\}^n$ such that

$$\mu(P, U, X, Y) \geq \frac{M \cdot |X| \cdot |Y|}{N} + \frac{2M^2 \cdot \sqrt{|X| \cdot |Y|}}{N} + 3\sqrt{n \cdot M \cdot |X| \cdot |Y|} \quad (7)$$

is at most $\frac{2}{N}$, where the probability is taken over the random choice of P and the internal randomization of Eve. □

In the following definition, we will state some technical relations between the parameters M, Δ, R, and n, which form the set of assumptions under which our security bound holds. These technical terms will become transparent during the course of our proof. Δ denotes some balancedness parameter, which will be needed in the proof for identifying computational transcripts, which have some critical combinatorial properties.

Definition 4. *(1)* $M \cdot R \leq 2^{(2/3)n}$.
(2) It holds that

$$B(M,R,n) + 2 \cdot \Delta \cdot M + \frac{(R+n) \cdot M^2}{\Delta} \leq \frac{2^n}{\sqrt{2}},$$

where for all j, $1 \leq j \leq M$, $B(j,R,n)$ *is defined as*

$$B(j,R,n) = 2^{-n} \cdot j^3 \cdot \left(R+n-1+2\sqrt{R+n-1}\right) + 3 \cdot \sqrt{n \cdot j^3 \cdot (R+n-1)}.$$

(3) It holds that

$$22 \cdot 2^{-(n-1)} \cdot R \cdot M^2 + \sqrt{\frac{n \cdot M}{2}} \leq \frac{\Delta - (R+n-1)}{R+n-1}.$$

(4) It holds that

$$\Delta \cdot ((n+R+2) \cdot M + \Delta) \leq \ln 2 \cdot 2^{-(n-2)}.$$

4.2 The Formulation of the Main Theorem

Theorem 3. *Suppose that the parameters* M, n, R *satisfy all rules in Definition 4 for some number* Δ. *Then Eve's success probability to win the packet prediction game with parameters* ρ, π, R, n *with* M *oracle queries is bounded by*

$$34 \cdot 2^{-n} + M \cdot e^{-n} + M \cdot (\Delta+1) \cdot 2^{-(n-1)} + 11 \cdot (R+4n) \cdot M \cdot 2^{-(n-1)}. \quad (8)$$

Corollary 1. *Suppose that* $M \leq 2^{(\frac{2}{3}-\epsilon)n}$ *for some constant* $\epsilon > 0$, *and let* $\Delta = \lfloor 2^{\frac{1}{3}n} \rfloor$. *Then there are positive constants* c_1 *and* c_2 *such that for* $M \cdot R \leq \frac{1}{c_1 \cdot n} \cdot 2^{\frac{2}{3}n}$ *it holds that* M, R, n, Δ *satisfy all rules in Definition 4 if* n *is large enough and that Eve's success probability to win the packet prediction game with parameters* π, R, n *with* M *oracle queries is bounded by* $c_2 \cdot 2^{-\epsilon \cdot n}$ *if* n *is large enough.* □

4.3 The Friendly Alice, Structural Collisions, and Sudden Death

We will prove our security bound for a modified game, in which Alice is friendly to Eve in the sense that in certain situations Alice gives some additional information to Eve, and that Alice directly gives up in certain other situation. In particular, Alice informs Eve if Eve managed to discover a so-called *structural collision*, and she follows a *sudden death rule*, which has to do with structural collisions.

Definition 5. – *A pair (x, y), where $x, y \in \{0,1\}^n$ is called a structural EF-collision w.r.t. to an elementary event $\omega = (k_\omega, P_\omega, F_\omega)$, if*

$$y = \pi^r(P_\omega(x \oplus k_\omega) \oplus k_\omega)),$$

for some r, $-(n-1) \leq r \leq R-1$. Note that this implies that the n-bit block $F_\omega(y)$ is a subblock of packet $E_\omega(x)$ or has at least a nonempty intersection with packet $E_\omega(x)$.

– *If (x, y) is a structural EF-collision w.r.t. ω, then the point $\bar{y} = P_\omega(x \oplus k_\omega) \oplus k_\omega$ is called the reference point of this collision.*

– *A pair (x, x'), where $x \neq x' \in \{0,1\}^n$, is called a structural EE-collision w.r.t. to ω if the packets $E_\omega(x)$ and $E_\omega(x')$ have a nonempty intersection, i.e., there is some number r, $1 \leq r \leq R-1$, such that*

$$\pi^r(P_\omega(x \oplus k_\omega) \oplus k_\omega) = P_\omega(x' \oplus k_\omega) \oplus k_\omega.$$

Note that this implies that the suffix of packet $E_\omega(x)$ starting at position r equals the prefix of packet $E_\omega(x')$.

Note here that structural EF-collisions are exactly those collisions which are exploited in the classical TMD tradeoff attacks against stream ciphers. Note further that there may occur collisions which are non-structural but caused by internal collisions of F_ω.

Suppose that Alice holds the elementary event $\omega = (k_\omega, P_\omega, F_\omega)$ and communicates with Eve. The friendly Alice does the following.

Definition 6. – *Whenever Eve poses an F-query with some input $y \in \{0,1\}^n$ which forms a structural EF-collision (x, y) w.r.t. ω for some $x \in \{0,1\}^n$ which already occurred as input of an E-query posed before, then, besides publishing $F_\omega(y)$, Alice confirms a structural collision, publishes a pointer to the input x and publishes the reference point $P_\omega(x \oplus k_\omega) \oplus k_\omega$ of this collision.*

– *Whenever Eve poses an E-query with some input $x \in \{0,1\}^n$ which forms a structural EF-collision (x, y) w.r.t. ω for some y which already occurred as input of an F-query posed before, then, besides publishing $E_\omega(x)$, Alice confirms a structural collision, publishes a pointer to y and publishes the reference point $P_\omega(x \oplus k_\omega) \oplus k_\omega$ of this collision.*

– *Suppose that Eve poses an E-query with some input $x \in \{0,1\}^n$ which forms a structural EE-collision (x, x') or (x', x) w.r.t. ω for some x' which already occurred as input of another E-query posed before. Suppose w.l.o.g. that $\pi^r(P_\omega(x \oplus k_\omega) \oplus k_\omega) = P_\omega(x' \oplus k_\omega) \oplus k_\omega$ for some r, $1 \leq r \leq R-1$. Then, besides publishing $E_\omega(x)$, Alice confirms a structural EE-collision and publishes a pointer to x'. Moreover, Alice publishes the value $y = \pi^r(P_\omega(x \oplus k_\omega) \oplus k_\omega)) = P_\omega(x' \oplus k_\omega) \oplus k_\omega)$, the value $F_\omega(y)$, and the reference points $\bar{y} = P_\omega(x \oplus k_\omega) \oplus k_\omega$ and y of the resulting structural EF-collisions (x, y) and (x', y).*

Next we formulate the *sudden death rule*.

Definition 7. *Suppose that Alice holds an elementary event $\omega = (k_\omega, P_\omega, F_\omega)$ and consider a situation in which Eve already posed a number of queries. A pair (x, u), where $x, u \in \{0,1\}^n$ is called a sudden death pair w.r.t. ω if the following conditions are fulfilled*

- *Eve has already asked an E-query with input x and a P-query with input u or a P^{-1}-query with output u.*
- *There is a structural EF-collision (x, y) discovered already by Eve.*
- *It holds $x \oplus u = k_\omega$.*

Whenever Eve asks a query which causes a sudden death pair w.r.t. to the secert ω holded by Alice, then Alice immediately gives up, the game stops and Eve wins.

Note that the friendliness of Alice increases Eve's chances to win the prediction game. Consequently, it is sufficient to show the security lower bound of Theorem 3 for an adversary Eve who plays the packet prediction game with a friendly Alice.

Note further that the definition of a sudden death pair in Definition 7 equals the corresponding definition in the description of the key recovery attack in the proof of Theorem 1.

4.4 Transcripts and Deterministic versus Randomized Adversaries

First note the well-known fact, proved, e.g., in [7] and many other papers, that it is sufficient to prove our security lower bound for deterministic adversaries. For showing this suppose that Eve is randomized and that the randomization is organized by a number B of random bits. Then Eve' success probability can be written as

$$Pr[Eve\ successfull] = \sum_{b \in \{0,1\}^B} 2^{-B} Pr[Eve\ successfull|b], \tag{9}$$

where $Pr[Eve\ successfull|b]$ denotes the success probability of the deterministic algorithm obtained by assigning b to Eve's random bits.

Consequently, if we show an upper bound on the success probability of all deterministic adversaries then, by (9), this bound holds also for randomized adversaries.

Therefore, we assume from now on that Eve is deterministic.

During each computation, Eve poses at most M oracle queries, where she either wins via sudden death of Alice or she stops after M queries with the publication of a challenge-response pair from $\{0,1\}^n \times \{0,1\}^n$ as final output.

We identify computations of Eve with transcripts of the form τ, which are defined to be a sequences of at most M query-triples $(type_j, input_j, output_j)$ corresponding to the oracle queries posed during the computation. If τ has length M then $(chall(\tau), res(\tau)) \in \{0,1\}^n \times \{0,1\}^n$ denotes the challenge-response pair published after τ in dependence of τ.

We define $type_j \in \{F, P^{-1}, P, E\}$ and $input_j$ and $output_j$ to denote the type, the input and the output of the j-th oracle query, $j = 1, \cdots, M$. Note that the output of an oracle query can, besides function values of P_ω, P_ω^{-1}, F_ω, E_ω, contain additional information about structural collisions discovered by this query (see Definition 6).

Note that each elementary event $\omega \in \Omega$ defines a unique computation of Eve on ω which can be written as a pair

$$(\tau_\omega, next(\tau_\omega, \omega)),$$

where τ_ω is the transcript corresponding to the sequence of all queries posed by Eve on ω.

For all transcripts τ of a length $j \leq M$ and all elementary events ω, for which the transcript of the first j queries along τ_ω equals τ, $next(\tau_\omega, \omega))$ is defined to be

- *sudden death* if τ has less than M queries and the uniquely defined next query after τ causes a sudden death pair w.r.t. ω, or
- $(chall(\tau_\omega), res(\tau)_\omega)$, if τ consists of M queries, or
- the query-triple corresponding to the uniquely defined next query after τ and the answer corresponding to ω, if τ consists less than M queries and the next query does not causes a sudden death pair w.r.t. ω.

Note that the computation corresponding to $(\tau_\omega, next(\tau_\omega, \omega))$ is successful (from Eve's point of view) if and only if

$$next(\tau_\omega, \omega) = sudden\ death$$

or the first n bits of the packet corresponding to $chall(\tau_\omega)$ via ω coincide with $res(\tau_\omega)$, i.e., if

$$F_\omega\left(P_\omega\left(chall(\tau_\omega) \oplus k_\omega\right) \oplus k_\omega\right) = res(\tau_\omega).$$

Let us denote with $\Omega^{succ} \subseteq \Omega$ the set

$$\Omega^{succ} = \{\omega; (\tau_\omega, next(\tau_\omega, \omega)) \text{ is successful}\}$$

of elementary events leading to a successful computation.

The set Ω^{succ} contains the subset $\Omega^{s.death}$ consisting of all elementary events ω for which $result(\tau_\omega, \omega) = sudden\ death$.

Note that $\Omega^{s.death}$ can be written as

$$\Omega^{s.death} = \bigcup_{j=2}^{M-1} \Omega_j^{s.death},$$

where for all j, $2 \leq j \leq M-1$, $\Omega_j^{s.death}$ contains all elementary events for which the $j+1$-th query generates a sudden death pair.

Observe that for all j, $2 \leq j \leq M-1$, and $\Omega_j^{s.death}$ it holds that τ_ω consists of j query-triples.

For all j, $1 \leq j \leq M$, let us call an elementary events ω to be j-alive if τ_ω contains at least j query-triples, i.e., if $\omega \notin \Omega_J^{s.death}$ for all J, $1 \leq J \leq j-1$.

Note

Lemma 1. *For all j, $2 \leq j \leq M-1$, it holds that $\omega \in \Omega_j^{s.death}$ if and only if ω is j-alive but not $j+1$-alive.* □

For all j, $1 \leq j \leq M$, we denote by $\mathcal{T}^j$ the set of all transcripts (i.e. sequences of query-triples) of length j for which there is some $\omega \in \Omega$ such that τ is the prefix of length j of τ_ω.

Moreover, for all J, $1 \leq J \leq j$, we denote $\tau^{\leq J}$ the subsequence of the first J queries along τ.

Note that fore all j, $1 \leq j \leq M$, Ω defines a probability distribution on $\mathcal{T}^j$. For all $\tau \in \mathcal{T}^j$ it holds

$$Pr_\Omega[\tau] = \frac{|\Omega(\tau)|}{|\Omega|},$$

where $\Omega(\tau) = \{\omega \in \Omega; \tau_\omega^{\leq j} = \tau\}$.

A Visualization of the Computational Behavior of Eve: Note that the computational behavior of Eve can be visualized by a leaf-directed tree of depth M and two additional sinks labeled with *succ* and *unsucc*, which is defined as follows.

- For all j, $1 \leq j \leq M$, the tree-nodes of depth $j-1$ correspond to the j-th query made by Eve and are labeled by the type and the input of the corresponding query. Corresponding to this, the source of the tree is labeled by the type and the input of the first query posed by Eve.
- The tree-nodes of depth M are labeled by challenge-response pairs.
- The edges leaving a tree-nodes of depth $j-1$, where $1 \leq j \leq M-1$, correspond to and are labeled with the possible answers of the corresponding query the node is labeled with. They point to the node in depth j which corresponds to the uniquely determined next query. Moreover, there is one edge leaving this node which points to the *succ*-sink and which corresponds to the sudden death event.
- The edges leaving a tree-node of depth $M-1$ correspond also to and are also labeled with the possible answers of the corresponding query the node is labeled with. They point to the node in depth M which corresponds to the uniquely determined challenge-response pair published after this query.
- All tree-nodes of depth M are left by two edges, one pointing to the *succ*-sink and one pointing to the *unsucc*-sink.

Note for all j, $1 \leq j \leq M$, each node of depth j correspond exactly to one transcripts τ in $\mathcal{T}^j$ (and vice versa), where the nodes and edges at the unique path from the source to this node correspond to the queries of τ.

Note further that each elementary event ω defines a unique path through the tree which starts at the source, follows the transcript τ_ω and reaches either the *succ*-sink or the *unsucc*-sink in dependence of ω is in Ω^{succ} or not.

4.5 Basic Definitions for Transcripts

For each j, $1 \leq j \leq M$, and each transcript $\tau \in \mathcal{T}^j$ we define the following sets corresponding to the queries along τ.

- $X(\tau) = \{x \in \{0,1\}^n ;\ \tau$ contains an E-query with input $x\}$,
- $Y(\tau) = \{y \in \{0,1\}^n ;\ \tau$ contains an F-query with input $y\}$, [6]
- $U(\tau) = \{u \in \{0,1\}^n ;\ \tau$ contains a P-query with input u, or a P^{-1}-query with output $u\}$,
- $V(\tau) = \{v \in \{0,1\}^n ;\ \tau$ contains a P-query with output v, or a P^{-1}-query with input $v\}$,
- $X^*(\tau) = \{x \in X(\tau);\ x$ occurs at the left-hand side of some structural EF-collision in $Coll(\tau)\}$,
- $\bar{Y}^*(\tau) = \{\bar{y} \in \{0,1\}^n ;\ \bar{y}$ is reference point of some structural EF-collision in $Coll(\tau)\}$,
- $Coll(\tau) = \{(x, \bar{y})$; where $x \in X^*(\tau)$, and $\bar{y} \in Y^*(\tau)$ is the reference point of a structural EF-collision (x, y) of $\tau\}$,
- $\bar{Y}^{(r)}(\tau) = \{\bar{y} \in \{0,1\}^n ;\ \pi^r(\bar{y}) \in Y(\tau)\}$
- $\bar{Y}(\tau) = \bigcup_{r=-(n-1)}^{R-1} \bar{Y}^{(r)}(\tau)$

Remember that we suppose Alice to be friendly in the sense of Definition 6. This implies that the oracle answers of Alice along τ yield the complete knowledge about $Coll(\tau)$ and $\bar{Y}^*(\tau)$ and $X^*(\tau)$.

Note further that $Coll(\tau)$ also yields all information about structural EE-collisions discovered during τ. This is because, due to Definition 6, a pair (x, x') is a structural EE-collisions discovered during τ if and only if there is some $y \in Y(\tau)$ for which $(x, y) \in Coll(\tau)$ and $(x', y) \in Coll(\tau)$.

Moreover, $Coll(\tau)$ defines a one-to-one correspondence between $X^*(\tau)$ and $\bar{Y}^*(\tau)$ which is established by the bijection $P_\omega(x \oplus k_\omega) \oplus k_\omega$ for an $\omega \in \Omega(\tau)$. (Note that, by definition, this bijection is the same for all $\omega \in \Omega(\tau)$.)

Definition 8. *A transcript ω is called τ-consistent, if $\tau_\omega^{\leq j} = \tau$, i.e., if $\omega \in \Omega(\tau)$.*

A key $k \in \{0,1\}^n$ is called τ-consistent if there is some τ-consistent elementary event ω with $k_\omega = k$.

Let $K(\tau)$ denote the set of all τ-consistent keys.

Let us take a look on the situation of Eve after posing j queries and let τ denote the corresponding transcript. The knowledge of Eve about the secret ω chosen by Alice is that $\omega \in \Omega(\tau)$ and, particularly, that $k_\omega \in K(\tau)$. From Eve's point of view, all transcripts in $\Omega(\tau)$ are equally likely to be the secret.

Note that $\Omega(\tau)$ defines a probability distribution on $K(\tau)$, where for all $k \in K(\tau)$

$$Pr_{\Omega(\tau)}[k] = Pr_{\omega \in \Omega(\tau)}[k_\omega = k].$$

The analysis of this distribution will be an important part of the proof of Theorem 3.

[6] We put also those y to $Y(\tau)$, which occur at the right side of a structural EF-collision, which was disclosed by Alice as additional information to an EE-collision, see Definition 6).

4.6 Critical Keys and Critical Points and the Characterization of τ-Consistency

Definition 9. *A key k is called to be τ-critical, if there is some $u \in U(\tau)$ such that $u \oplus k \in X(\tau)$ and $P_\tau(u) \oplus k \in \bar{Y}(\tau)$.*

Here, $P_\tau(u)$ denotes the output of the P-query on input u along τ, resp. the input of the P^{-1}-query with output v.

Definition 10. *Let $k \in \{0,1\}^n$. A point $u \in U(\tau)$ is called (τ, k)-critical if at least one of the following conditions is fulfilled.*

C1: $u \oplus k \in X(\tau) \setminus X^*(\tau)$ and $P_\tau(u) \oplus k \in \bar{Y}(\tau) \setminus \bar{Y}^*(\tau)$.
C2: $u \oplus k \in X^*(\tau)$ or $P_\tau(u) \oplus k \in \bar{Y}^*(\tau)$.

The notion of (τ, k)-critical points allows to characterize τ-consistency.

Lemma 2. *A key $k \in \{0,1\}^n$ is not τ-consistent if and only if there is a (τ, k)-critical point $u \in U(\tau)$.*

Proof: We prove first the if-direction.

Let $k \in \{0,1\}^n$ and suppose that there is some $u \in U(\tau)$ which is (τ, k)-critical.

For deriving a contradiction we assume that $k \in K(\tau)$, i.e., that there is some $\omega \in \Omega(\tau)$ with $k_\omega = k$.

Suppose first that u is (τ, k)-critical via condition C1 of Definition 10.

By definition, $P_\tau(u) \oplus k = P_\omega(u) \oplus k_\omega \in \bar{Y}(\tau)$ which implies the existence of some r, $-(n-1) \leq r \leq R-1$ such that $\pi^r(P_\omega(u) \oplus_{k_\omega}) \in Y(\tau)$. This implies, that $(u \oplus k_\omega, \pi^r(P_\omega(u) \oplus k_\omega))$ has to be classified as structural collision with reference point $P_\omega(u) \oplus k_\omega$ along τ. But this can not be true, as, by Definition 7, $(u \oplus k, u)$ would form a sudden death pair w.r.t. ω, which implies that $\omega \notin \Omega(\tau)$.

Suppose now that u is (τ, k)-critical via condition C2 of Definition 10. If $u \oplus k = u \oplus k_\omega \in X^*(\tau)$ then (u, x) is again a sudden death pair w.r.t. ω which implies that $\omega \notin \Omega(\tau)$.

If $P_\tau(u) \oplus k \in \bar{Y}^*(\tau)$ then $(u \oplus k, P_\tau(u) \oplus k) \in Coll$ which again implies that $u \oplus k = u \oplus k_\omega \in X^*(\tau)$ and $\omega \notin \Omega(\tau)$.

Let us now show the only-if direction of Lemma 2.

We fix some j, $1 \leq j \leq M$, some transcript $\tau \in \mathcal{T}^j$ with $Pr_\Omega[\tau] > 0$ and some key $k \in \{0,1\}^n$ for which there do not exist (τ, k)-critical points $u \in U(\tau)$ in the sense of Definition 10.

We have to show that k is τ-consistent.

We do this by constructing a permutation P' over $\{0,1\}^n$ and a π-iterative function $F' : \{0,1\}^n \longrightarrow \{0,1\}^n$ such that $\omega' = (k, P', F') \in \Omega(\tau)$.

For all inputs $x \in X(\tau)$, $u \in U(\tau)$, $v \in V(\tau)$, $y \in Y(\tau)$ of oracle queries posed during τ we denote by $E_\tau(x)$, $P_\tau(u)$, $P_\tau^{-1}(v)$, and $F_\tau(y)$, resp., the corresponding oracle answers given by Alice during τ.

First observe that P' and F' have to satisfy the condition that $P'(u) = P_\tau(u)$ and $F'(y) = F_\tau(u)$ for all $u \in U(\tau)$ and $y \in Y(\tau)$, respectively.

We have now to define P' ands F' outside of $U(\tau)$ and $Y(\tau)$, respectively, in such a way that ω' is τ-consistent.

We do this by defining P' and F' along the (k, P')-paths, where the (k, P')-path through an input $u \in \{0,1\}^n$ is defined to be the triple $(u \oplus k, u, P'(u) \oplus k)$.

We do this by going with u through $\{0,1\}^n$ in a certain order.

We dynamically maintain a set $Target(P')$, which is initially set to $\{0,1\}^n \setminus V(\tau)$. Whenever we define $P'(u)$ for a *new* u, we delete $P'(u)$ from $Target(P')$.

- **Phase 1:** Here we consider all $u \in \{0,1\}^n$ for which $u \oplus k \in X^*(\tau)$.
  Then it holds $u \notin U(\tau)$ as otherwise u would be (τ, k)-critical via condition C2 of Definition 10.
  We define $P'(u) = \bar{y} \oplus k$, where $\bar{y}$ denotes the unique point in $\bar{Y}^*(\tau)$ for which $(u \oplus k, \bar{y}) \in Coll(\tau)$. Note that this point $\bar{y} \oplus k$ does not belong to $V(\tau)$. Otherwise, if $\bar{y} \oplus k$ would equal $P_\tau(u')$ for some $u' \neq u \in U(\tau)$ then u' would be (τ, k)-critical.
  In both cases, we define F' on the set $\{\pi^r(P'(u) \oplus k); r = -(n-1), \cdots, R-1\}$ according to the packet $E_\tau(u \oplus k)$. Note hereby that if $-(n-1) \leq r < 0$ then $E_\tau(u \oplus k)$ determines only a suffix of $F'(\pi^r(P'(u) \oplus k))$, and that if $R - n - 1 < r < R - 1$ then $E_\tau(u \oplus k)$ determines only a prefix of $F'(\pi^r(P'(u) \oplus k))$.
- **Phase 2** concerns the (k, P')-paths through those $u \in U(\tau)$ for which $u \oplus k \in X(\tau) \setminus X^*(\tau)$. Note that for these $u \in U(\tau)$, as they are not (τ, k)-critical, it holds $\bar{y} := P_\tau(u) \oplus k \notin \bar{Y}(\tau)$.
  This implies that for all r, $-(n-1) \leq r \leq R-1$, it holds that $\pi^r(\bar{y})$ is not in $Y(\tau)$, which allows us to define $F'(\bar{y})$ according to the packet $E_\tau(u \oplus k)$.
- **Phase 3** considers all $u \notin U(\tau)$ for which $u \oplus k \in X(\tau) \setminus X^*(\tau)$.
  Here, $P'(u)$ has to be chosen in such a way that $P'(u) \oplus k \notin \bar{Y}(\tau)$. Otherwise, as $u \oplus k$ does not occur as left hand side of a EF-collision, u would be (τ, k)-critical.
  Corresponding to this, we define a set

$$Forbidden(u) = \{v \in \{0,1\}^n ; v \oplus k \in \bar{Y}(\tau)\},$$

  and choose

$$P'(u) \in Target(P') \setminus Forbidden(u).$$

Note that for all remaining $u \in \{0,1\}^n$ the values of $P'(u)$ can be freely chosen in $Target(P')$. For all remaining $y \in \{0,1\}^n$, the values of $F'(y)$ can also be freely chosen $\{0,1\}^n$ in such a way that the π-iterativeness of F' is maintained. □

4.7 Assigning Colors to Elementary Events, Transcripts and Keys

We will now assign the colors red, black, blue and green to transcripts, elementary events, and keys. There will be three colors, namely black, red, and blue, which have to be considered as bad in the sense, that if ω has a bad color then τ_ω yields some nontrivial information which helps Eve to win the game.

Let us start with the definition of black elementary events, which is partly based on considering the following equivalence relation $\equiv_P$, induced by a permutation P over $\{0,1\}^n$.

Definition 11. *Let P denote a permutation of $\{0,1\}^n$ and let U be an arbitrary subset of $\{0,1\}^n$.*

- *For all $u, u' \in U$ let $u \equiv_P u'$ if and only if $u \oplus P(u) = u' \oplus P(u')$.*
- *Let $Max(P,U)$ denote the maximal size of an equivalence class w.r.t. $\equiv_P$ in U.*

Definition 12. – *For all j, $1 \leq j \leq M$, we call a transcript $\tau \in \mathcal{T}^j$ to be black if the number of τ-critical keys (see Definition 9) exceeds*

$$B(j,R,n) = 2^{-n} \cdot j^3 \cdot \left(R+n-1+2\sqrt{R+n-1}\right) + 3\sqrt{n \cdot j^3 \cdot (R+n-1)}$$

or if

$$Max(P_\tau, U(\tau)) > 5,$$

where $P_\tau : U(\tau) \longrightarrow \{0,1\}^n$ denotes the injective mapping corresponding to the P- and P^{-1}-queries in τ.

- *For all j, $1 \leq j \leq M$, an elementary event ω is called j-black, if ω is j-alive and the transcript $\tau_\omega^{\leq j}$, corresponding to the first j queries along τ_ω, is black.*
- *Let Ω^j_{black} denote the set of all j-black elementary events and by $\mathcal{T}^j_{black}$ the set of all black transcripts $\tau \in \mathcal{T}^j$.*
- *Let $\Omega^{black} = \bigcup_{j=1}^M \Omega^j_{black}$.*

Let us next define red transcripts.

Definition 13. – *For all j, $1 \leq j \leq M$, we call a transcript $\tau \in \mathcal{T}^j$ to be red if it is not black but it holds $|X^*(\tau)| > \Delta$.*

- *An elementary event ω is called j-red, if ω is j-alive and the transcript $\tau_\omega^{\leq j}$ is red.*
- *Let Ω^j_{red} denote the set of all j-red elementary events and by $\mathcal{T}^j_{red}$ the set of all red transcripts $\tau \in \mathcal{T}^j$.*
- *Let $\Omega^{red} = \bigcup_{j=1}^M \Omega^j_{red}$.*

Note that one strategy of Eve could be to pose queries in a first phase in such a way that for the resulting transcript τ it holds that the set $K(\tau)$ of τ-consistent keys is small, and then to try each key in $K(\tau)$ if it fits. Redness and blackness of transcripts τ cover exactly the case in which this strategy could be successful:

Lemma 3. *For all j, $1 \leq j \leq M$, and $\tau \in \mathcal{T}^j$ it holds the following. If τ is neither red nor black then*

$$|K(\tau)| \geq 2^n - B(j,R,n) - 2 \cdot \Delta \cdot j.$$

Proof: From Definition 10 and Lemma 2 we know that $k \in \{0,1\}^n \setminus K(\tau)$ if and only if there is some $u \in U(\tau)$ such that u is k-critical via condition C1 or via condition C2. Condition C1 implies that k is τ-critical in the sense of Definition 10. As τ is not black, the number of such keys is bounded by $B(j,R,n)$. Condition C2 implies that $k \in X^*(\tau) \oplus U(\tau)$ or $k \in \bar{Y}^*(\tau) \oplus V(\tau)$. As τ is not red, it holds that $|X^*(\tau) \oplus U(\tau)| \leq \Delta \cdot j$ and $|\bar{Y}^*(\tau) \oplus U(\tau)| \leq \Delta \cdot j$. □

The motivation for considering blue elementary events is as follows. We have seen above that $\Omega(\tau)$, the set of all possible events if Eve sees τ, defines a probability distribution on $K(\tau)$, the set of all keys which are consistent with τ. This distribution is known to Eve. Eve could make a Bayes-decision and test the hypothesis that the secret key is the most probable key in $K(\tau)$.

Let us now define blue elementary events and green elementary events.

Blue elementary events $\omega = (k_\omega, P_\omega, F_\omega)$ will have the property that for $\tau = \tau_\omega$ it holds that $Pr_{\Omega(\tau)}[k_\omega]$ is large, i.e., if Alice chooses an blue elementary event then the success probability of a Bayes decision made by Eve will be non trivially high.

Definition 14. – *For all numbers j, $1 \leq j \leq M$, we call an elementary event $\omega \in \Omega$ to be j-blue if ω is j-alive and not black and if*

$$|(X(\tau_\omega^{\leq j}) \oplus k_\omega) \cap U(\tau_\omega^{\leq j})| > \Delta$$

or

$$|(\bar{Y}(\tau_\omega^{\leq j}) \oplus k_\omega) \cap V(\tau_\omega^{\leq j})| > \Delta.$$

– *Let Ω^j_{blue} denote the set of all j-blue elementary events.*
– *Let $\Omega^{blue} = \bigcup_{j=1}^{M} \Omega^j_{blue}$.*

Definition 15. – *For all numbers j, $1 \leq j \leq M$, an elementary event $\omega \in \Omega$ is called to be j-green if ω is j-alive and neither j-blue, nor j-red, nor j-black.*
– *Let Ω^j_{green} denote the set of all j-green elementary events.*
– *Let $\Omega^{green} = \Omega^M_{green}$*
– *For all numbers j, $1 \leq j \leq M$, a transcript $\tau \in \mathcal{T}^j$ is called green, if it is neither red nor black.*
– *Let $\mathcal{T}^j_{green}$ denote the set of green transcripts in $\mathcal{T}^j$.*

It is important to note the following difference between red and black events on the one side and green and blue events on the other side. Let τ be a transcript and let one elementary event in $\Omega(\tau)$ be black (resp. red). Then, by definition, all elementary events in $\Omega(\tau)$ are black (resp. red) which justifies to define τ to be black (resp. red).

On the other side, if a transcript τ is green, then the elementary events in $\Omega(\tau)$ are either blue or green. This is because blueness does not only depend on τ but also on the key-component k_ω of the elementary events $\omega \in \Omega(\tau)$.

We will prove Theorem 3 by showing that the probabilities of black, red, and black transcripts are exponentially small, that the probability of sudden-death

events is exponentially small, and that for green transcripts $\tau \in \mathcal{T}^M_{green}$, the probability that Eve publishes a correct challenge-response pair is exponentially small (see Lemma 4 in Subsection 4.8).

Therefore, let us take more insight into the structure of $\Omega(\tau)$ for green transcripts τ.

We know that the decision if an elementary event $\omega \in \Omega(\tau)$ is green or blue depends only on k_ω. This justifies the following definition.

Definition 16. – *Let τ denote a green transcript. We call a τ-consistent key $k \in K(\tau)$ to be τ-green if $|(X(\tau) \oplus k) \cap U(\tau)| \leq \Delta$ and $|(\bar{Y}(\tau) \oplus k) \cap V(\tau)| \leq \Delta$, and τ-blue otherwise.*
– *We denote by $K^{green}(\tau)$ (resp. $K^{blue}(\tau)$) the set of all τ-consistent keys, which are τ-green (resp. τ-blue).*

Note that by definition

$$K(\tau) = K^{green}(\tau) \cup K^{blue}(\tau).$$

4.8 The Structure of the Proof of Theorem 3

We have to derive an upper bound for Eve's success probability $Pr_\Omega[\Omega^{succ}]$. This probability can be upper bounded by

$$Pr_\Omega[\Omega^{succ}] \leq Pr_\Omega[\Omega^{black}] + Pr_\Omega[\Omega^{red}] + Pr_\Omega[\Omega^{blue}]$$
$$+Pr_\Omega[\Omega^{s.death} \setminus \left(\Omega^{black} \cup \Omega^{red} \cup \Omega^{blue}\right)] + Pr_\Omega[\Omega^{succ} \cap \Omega^{green}]. \quad (10)$$

The probability $Pr_\Omega[\Omega^{succ} \cap \Omega^{green}]$ can be written as

$$Pr_\Omega[\Omega^{succ} \cap \Omega^{green}] = Pr_\Omega[\Omega^{green}] \cdot Pr_{\Omega^{green}}[\Omega^{succ}]$$
$$\leq Pr_{\Omega^{green}}[\Omega^{succ}], \quad (11)$$

where $Pr_{\Omega^{green}}[\Omega^{succ}]$ can be written as

$$Pr_{\Omega^{green}}[\Omega^{succ}] = \sum_{\tau \in \mathcal{T}^M_{green}} Pr_{\Omega^{green}}[\Omega^{succ} \cap \Omega^{green}(\tau)]$$
$$= \sum_{\tau \in \mathcal{T}^M_{green}} Pr_{\Omega^{green}}[\tau] \cdot Pr_{\Omega^{green}(\tau)}[\Omega^{succ}]. \quad (12)$$

By Relations (10), (12) and (12), Theorem 3 follows directly from the following

Lemma 4. *(i) It holds that $Pr_\Omega[\Omega_{black}] \leq 34 \cdot 2^{-n}$.*
(ii) It holds that $Pr_\Omega[\Omega_{red} \cup \Omega_{blue}] \leq M \cdot e^{-n}$.
(iii) It holds that

$$Pr_\Omega\left[\Omega^{s.death} \setminus \left(\Omega^{black} \cup \Omega^{red} \cup \Omega^{blue}\right)\right] \leq 2^{-(n-1)} \cdot (\Delta + 1) \cdot M.$$

(iv) For all $\tau \in \mathcal{T}^M_{green}$ *it holds that*

$$Pr_{\Omega^{green}(\tau)}[\Omega^{succ}] \leq 11 \cdot (R + 4n) \cdot M \cdot 2^{-(n-1)}.$$

The Structure of the Proof of Lemma 4:

The proofs of parts (i), (ii), (iii), and (iv) will be given in Subsections 4.10, 4.12, 4.9, and 4.11, respectively.

Our main technical result is the following *Smoothness Lemma*, which will be proved in Subsection 4.14 and which shows that for all green transcripts the probabilities of the green keys do not differ too much.

Lemma 5. *For all green transcripts* τ *and all* $k, k' \in K^{green}(\tau)$ *it holds that*

$$Pr_{\Omega^{green}(\tau)}[k] \leq \sqrt{2} \cdot Pr_{\Omega^{green}(\tau)}[k'].$$

Lemma 5 implies the following corollary, which is an important tool for proving parts (ii), (iii) and (iv) of Lemma 4.

Corollary 2. *For all green transcripts* τ *the following is true.*

(a) For all $k \in \{0,1\}^n$ *it holds*

$$Pr_{\Omega^{green}(\tau)}[k_\omega = k] \leq 2^{-(n-1)}.$$

(b) For all $x, \bar{y} \in \{0,1\}^n$*, where* $x \notin X^*(\tau)$ *and* $\bar{y} \notin \bar{Y}^*(\tau)$ *and (*$x \notin X(\tau)$ *or* $\bar{y} \notin \bar{Y}(\tau)$*) it holds*

$$Pr_{\Omega^{green}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}] \leq 9 \cdot 2^{-(n-1)}.$$

(c) For all $x, x' \in \{0,1\}^n$*, where* $x \notin X(\tau)$ *and* $x' \in X(\tau)$*, and all* i*,* $-(n-1) \leq r \leq R + n - 2$*, it holds*

$$Pr_{\Omega^{green}(\tau)}\left[\pi^i\left(P_\omega(x \oplus k_\omega) \oplus k_\omega\right) = P_\omega(x' \oplus k_\omega) \oplus k_\omega\right] \leq 11 \cdot 2^{-(n-1)}.$$

We give here only the proof of part (a). Parts (b) and (c) will be proved in Subsection 4.13.

Proof of part (a):

We combine Lemma 5 with the following lower bound for the size of $K^{green}(\tau)$. Therefore we fix some number j, $1 \leq j \leq M$, and suppose that $\tau \in \mathcal{T}^j_{green}$.

By Lemma 3 it holds that

$$|K^{green}(\tau)| = |K(\tau)| - |K^{blue}(\tau)| \geq 2^n - B(j, R, n) - 2 \cdot \Delta \cdot j - |K^{blue}(\tau)|.$$

We show that

$$|K^{blue}(\tau)| \leq \frac{(R + 2n) \cdot j^2}{\Delta}.$$

This is because

$$\sum_{k\in\{0,1\}^n} |(X(\tau)\oplus k)\cap U(\tau)| = \sum_{k\in\{0,1\}^n} |\{(x,u)\in X(\tau)\times U(\tau);\ x\oplus u = k\}|$$
$$= |X(\tau)\times U(\tau)| = |X(\tau)|\cdot|U(\tau)|.$$

This implies that

$$|\{k;\ |(X(\tau)\oplus k)\cap U(\tau)| > \Delta\}| \le \frac{|X(\tau)|\cdot|U(\tau)|}{\Delta} \le \frac{j^2}{\Delta}.$$

In exactly the same way one can prove that

$$\left|\left\{k;\ \left|\left(\bar{Y}(\tau)\oplus k\right)\cap V(\tau)\right| > \Delta\right\}\right| \le \frac{|\bar{Y}(\tau)|\cdot|V(\tau)|}{\Delta} \le \frac{(R+n-1)\cdot j^2}{\Delta}.$$

Consequently

$$|K^{green}(\tau)| \ge 2^n - B(j,n,R) - 2\cdot\Delta\cdot j - \frac{(R+n)j^2}{\Delta} \ge \frac{1}{\sqrt{2}}\cdot 2^n$$

if n is large enough. The last inequality holds due to condition (2) of Definition 4.

By Lemma 5 we obtain that for all $k\in K^{green}(\tau)$

$$Pr_{\Omega^{green}(\tau)}[k] \le \sqrt{2}\cdot\frac{1}{|K^{green}(\tau)|} \le 2\cdot 2^{-n} = 2^{-(n-1)}.$$

which proves Corollary 2, part (a). □

4.9 Bounding the Probability of Sudden Death

In this subsection, we prove part (iii) of Lemma 4, namely that

$$Pr_\Omega\left[\Omega^{s.death}\setminus\left(\Omega^{black}\cup\Omega^{red}\cup\Omega^{blue}\right)\right] \le 2^{-(n-1)}\cdot(\Delta+1)\cdot M. \tag{13}$$

Note that for all elementary events ω it holds that

$$\omega\in\Omega^{s.death}\setminus\left(\Omega^{black}\cup\Omega^{red}\cup\Omega^{blue}\right)$$

if and only if there is some number j, $2\le j\le M-1$, such that ω is j-green, but $\omega\in\Omega_j^{s.death}$ (i.e., the $(j+1)$-th query causes a sudden death pair w.r.t. ω). This implies

$$Pr_\Omega[\Omega^{s.death}\setminus\left(\Omega^{black}\cup\Omega^{red}\cup\Omega^{blue}\right)] \le$$
$$\sum_{j=2}^{M-1}\sum_{\tau\in\mathcal{T}^j_{green}} Pr_\Omega[\tau]\cdot Pr_{\Omega^{green}(\tau)}[\Omega_j^{s.death}]. \tag{14}$$

Let us fix some number j, $2 \leq j \leq M-1$, some transcript $\tau \in \mathcal{T}^j_{green}$, and some $\omega \in \Omega^{s.death}_j \cap \Omega^{green}(\tau)$. The fact that $\omega \in \Omega^{s.death}_j$ implies that

$$k_\omega \in X^*(\tau') \oplus U(\tau'),$$

where τ' denotes a transcript obtained from τ by posing the uniquely determined next query after τ. Here, we took into account that $X^*(\tau')$ and $U(\tau')$ do not depend on the answer of this next query.

It holds by definition that

$$|U(\tau')| \leq |U(\tau)| + 1 \leq j + 1 \leq M.$$

Moreover, the next query after τ can increase $X^*(\tau)$ by at most two (in case of generating a new EE-collision), which implies

$$|X^*(\tau')| \leq |X^*(\tau)| + 2 \leq \Delta - 1 + 2 = \Delta + 1.$$

Consequently, by Corollary 2, part (a), it follows that

$$Pr_{\Omega^{green}(\tau)}[\Omega^{s.death}_j] \leq 2^{-(n-1)} \cdot (\Delta + 1) \cdot M,$$

which, by Relation (14), proves Relation (13) and part (iii) of Lemma 4. □

4.10 Bounding the Probability of Black Transcripts

In this subsection we prove part (i) of Lemma 4, namely that for all numbers j, $1 \leq j \leq M$, it holds that

$$Pr_\Omega\left[\Omega^j_{black}\right] = Pr_\Omega\left[\mathcal{T}^j_{black}\right] \leq 34 \cdot 2^{-n}. \tag{15}$$

Proof of Relation (15):

Remember that $Pr_\Omega\left[\mathcal{T}^j_{black}\right] = Pr_{\omega \in \Omega}\left[\tau^{\leq j}_\omega \in \mathcal{T}^j_{black}\right]$.

Theorem 2 says that the probability that

$$\mu(P_\omega, U(\tau^{\leq j}_\omega), X(\tau^{\leq j}_\omega), \bar{Y}(\tau^{\leq j}_\omega)) \leq B(j, R, n)$$

is bounded by $2 \cdot 2^{-n}$.

Here, we took into account that $|U(\tau^{\leq j}_\omega)| \leq j$, $|X(\tau^{\leq j}_\omega)| \leq j$ and $|\bar{Y}(\tau^{\leq j}_\omega)| \leq j \cdot R + n - 2$.

Note that for all $\omega \in \Omega$ it holds by definition that the number of $\tau^{\leq j}_\omega$-critical keys is bounded by $\mu(P_\omega, U(\tau^{\leq j}_\omega), X(\tau^{\leq j}_\omega), \bar{Y}(\tau^{\leq j}_\omega))$.

This implies that the probability that the number of $\tau^{\leq j}_\omega$-critical keys exceeds $B(j, R, n)$ is bounded by $2 \cdot 2^{-n}$.

We proceed with the proof by showing that for all $U \subseteq \{0,1\}^n$ with $|U| \leq j \leq 2^{(2/3)n}$ it holds that

$$Pr[Max(P, U) \geq 6] \leq 32 \cdot 2^{-n},$$

where the probability Pr is taken w.r.t. a uniformly distributed random permutation P over $\{0,1\}^n$.

Clearly, the event $Max(P,U) \geq 6$ implies the existence of some $U' \subseteq U$, $|U'| = 6$, such that $u \equiv_P u'$ for all $u, u' \in U'$. Given a subset $U' \subseteq U$ with 6 elements, the probability for the event that $u \equiv_P u'$ for all $u, u' \in U'$ equals

$$\prod_{i=1}^{5} \frac{1}{2^n - i} \leq \left(\frac{1}{1/2 \cdot 2^n}\right)^5 = 2^5 \cdot 2^{-5 \cdot n}.$$

Consequently,

$$Pr[Max(P,U) \geq 6] \leq |U|^6 \cdot 2^5 \cdot 2^{-5 \cdot n}$$

$$\leq 2^5 \cdot 2^{6 \cdot (2/3)n} \cdot 2^{-5 \cdot n} = 2^5 \cdot 2^{4 \cdot n} \cdot 2^{-5 \cdot n}$$

$$= 32 \cdot 2^{-n}. \; \square$$

4.11 Completing the Proof of Theorem 3 by proving Part (iv) of Lemma 4

Let τ be a green transcript of length M, i.e., $\tau \in \mathcal{T}^M_{green}$. We have to bound the probability that Eve is successful under the condition that Alice has chosen a green elementary event $\omega = (k_\omega, P_\omega, F_\omega) \in \Omega^{green}(\tau)$.

Depending on τ, Eve publishes a pair $(chall(\tau), res(\tau)) \in \{0,1\}^n \times \{0,1\}^n$, where $chall(\tau) \notin X(\tau)$. Eve wins if and only if $res(\tau)$ equals the block of the first n keystream bits of the packet generated on input $chall(\tau)$ under ω, i.e.,

$$res(\tau) = F_\omega(P_\omega(chall(\tau) \oplus k_\omega) \oplus k_\omega).$$

For all $\omega \in \Omega^{good}(\tau)$ let y_ω denote the value

$$y_\omega = P_\omega(chall(\tau) \oplus k_\omega) \oplus k_\omega.$$

We have to bound the probability

$$Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = res(\tau)].$$

We do this by dividing $\Omega^{green}(\tau)$ into two disjoint subsets IND and DEP, where IND contains all those elementary events $\omega \in \Omega^{good}(\tau)$ for which $F_\omega(y_\omega)$ is independent from the queries and answers contained in τ, and $DEP = \Omega^{green}(\tau) \setminus DEP$.

Note that $\omega \in DEP$ if and only if

(I) there is some i, $-(n-1) \leq i \leq n-1$, such that $\pi^i(y_\omega) \in Y(\tau)$, or
(II) there is some i, $-(n-1) \leq i \leq n-1$, some $x \in X(\tau)$, and some r, $0 \leq r \leq R-1$, such that $\pi^i(y_\omega) = \pi^r(P_\omega(x \oplus k_\omega) \oplus k_\omega)$.

In case (I), $F_\omega(y_\omega)$ is not independent from the answer of the F-query with input $\pi^i(y_\omega)$, in case (II) $F_\omega(y_\omega)$ is not independent from the answer of the E-query with input x (in particular, from the block starting at position r in packet $E_\omega(x)$).

Corresponding to this, DEP can be written as

$$DEP = DEP_1 \cup DEP_2,$$

where DEP_1 contains all $\omega \in \Omega^{good}(\tau)$ for which case (I) is fulfilled and DEP_2 contains all $\omega \in \Omega^{good}(\tau)$ for which case (II) is fulfilled.

Note that

$$\begin{aligned} &Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = \\ &res(\tau)] = Pr_{\Omega^{green}(\tau)}[DEP] \cdot Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = res(\tau)|DEP] \\ &+Pr_{\Omega^{green}(\tau)}[IND] \cdot Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = res(\tau)|IND] \\ &\leq Pr_{\Omega^{green}(\tau)}[DEP] + Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = res(\tau)|IND], \end{aligned}$$

i.e.,

$$\begin{aligned} Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = res(\tau)] &\leq Pr_{\Omega^{green}(\tau)}[DEP_1] + Pr_{\Omega^{green}(\tau)}[DEP_2] \\ &+Pr_{\Omega^{green}(\tau)}[F_\omega(y_\omega) = res(\tau)|IND]. \end{aligned} \tag{16}$$

It quite obvious that

$$Pr_{\Omega^{good}(\tau)}[F_\omega(y_\omega) = res(\tau)|IND] = 2^{-n}, \tag{17}$$

as $\omega \in IND$ implies that $F_\omega(y_\omega)$ can take all values in $\{0,1\}^n$ with the same probability.

Next observe that for all $\omega \in \Omega^{green}(\tau)$ it holds that $\omega \in DEP_1$ if and only if

$$P_\omega(chall_\tau \oplus k_\omega) \oplus k_\omega = \bar{y}$$

for some $\bar{y} \in \bigcup_{y \in Y(\tau)} \{\pi^i(y); -(n-1) \leq i \leq n-1\}$, a set of size at most $(2n-1)M$.

As $chall(\tau) \notin X(\tau)$, it follows by Corollary 2, part (b), that

$$Pr_{\Omega^{green}(\tau)}[DEP_1] \leq (2n-1) \cdot M \cdot 9 \cdot 2^{-(n-1)}. \tag{18}$$

Observe further that for all $\omega \in \Omega^{green}(\tau)$ it holds that $\omega \in DEP_2$ if and only if

$$\pi^i\left(P_\omega(chall_\tau \oplus k_\omega) \oplus k_\omega\right) = P_\omega(x \oplus k_\omega) \oplus k_\omega$$

for some $x \in X(\tau)$ and number i, $-(n-1) \leq i \leq R+n-2$.

As $chall(\tau) \notin X(\tau)$, it follows by Corollary 2, part (c), that

$$Pr_{\Omega^{green}(\tau)}[DEP_2] \leq (R+2n-2) \cdot M \cdot 11 \cdot 2^{-(n-1)}. \tag{19}$$

Putting Relations (16),(17), (18), and (19) together yields

$$\begin{aligned} &Pr_{\Omega^{green}(\tau)}[\Omega^{green}(\tau) \cap \Omega^{succ}] \\ &\leq (2 + (2n-1) \cdot M \cdot 9 + (R+2n-2) \cdot M \cdot 11) \cdot 2^{-(n-1)} \\ &< 11 \cdot (R+4n) \cdot M \cdot 2^{-(n-1)}. \ \square \end{aligned} \tag{20}$$

4.12 The Proof of part (ii) of Lemma 4

We have to show that

$$Pr_{\Omega}[\Omega^{red} \cup \Omega^{blue}] \leq M \cdot 2^{-n}. \tag{21}$$

In the proof we will use a Chernov Bound argument which is described in the Appendix, Subsection B.

The proof of Relation (21):

Note first that for all $\omega \in \Omega^{red} \cup \Omega^{blue}$ there is some j, $1 \leq j \leq M$, such that the j-th query makes ω red or blue. Consequently,

$$\Omega^{red} \cup \Omega^{blue} = \bigcup_{j=1}^{M} \Omega^{j-1}_{green} \cap \left(\Omega^{j}_{red} \cup \Omega^{j}_{blue}\right)$$

which implies

$$Pr_{\Omega}\left[\Omega^{red} \cup \Omega^{blue}\right] \leq \sum_{j=1}^{M} Pr_{\Omega}\left[\Omega^{j-1}_{green} \cap \left(\Omega^{j}_{red} \cup \Omega^{j}_{blue}\right)\right]$$

$$\leq \sum_{j=1}^{M} Pr_{\Omega}[\Omega^{j}_{red} \cup \Omega^{j}_{blue} | \Omega^{j-1}_{green}] \cdot Pr_{\Omega}[\Omega^{j-1}_{green}]$$

$$\leq \sum_{j=1}^{M} Pr_{\Omega}[\Omega^{j}_{red} \cup \Omega^{j}_{blue} | \Omega^{j-1}_{green}]. \tag{22}$$

Hence, for proving Relation (21), it is sufficient to show that for all j, $1 \leq j \leq M$, it holds

$$Pr_{\Omega^{j-1}_{green}}[\Omega^{j}_{red} \cup \Omega^{j}_{blue}] = Pr_{\Omega}[\Omega^{j}_{red} \cup \Omega^{j}_{blue} | \Omega^{j-1}_{green}] < e^{-n}. \tag{23}$$

We show Relation (23) by induction on j.

Note first that Relation (23) is true if $j < \frac{\Delta}{R+n-1}$, as the for all transcripts τ with j queries it holds that the cardinalities of $X(\tau)$ and $\bar{Y}(\tau)$ are smaller than Δ.

For the induction step fix some arbitrary number j, $\frac{\Delta}{R+n-1} \leq j \leq M$, and suppose that Relation (23) is true for all numbers J, $1 \leq J \leq j-1$.

For all J, $1 \leq J \leq j-1$, we define a random variable $DB_J \in \{0,1\}$ over Ω, where $DB_J(\omega) = 1$ if and only if ω is J-alive and the J-th query along τ_ω increases $(X(\tau_\omega) \oplus k_\omega) \cap U(\tau)$ or increases $(\bar{Y}(\tau_\omega) \oplus k_\omega) \cap V(\tau)$ or increases $X^*(\tau)$. Formally,

$$DB_J(\omega) = 1 \iff$$
$$|(X(\tau_\omega^{\leq J}) \oplus k_\omega) \cap U(\tau_\omega^{\leq J})| > |(X(\tau_\omega^{\leq J-1}) \oplus k_\omega) \cap U(\tau_\omega^{\leq J-1})| \text{ or}$$
$$|(\bar{Y}(\tau_\omega^{\leq J}) \oplus k_\omega) \cap V(\tau_\omega^{\leq J})| > |(\bar{Y}(\tau_\omega^{\leq J-1}) \oplus k_\omega) \cap U(\tau_\omega^{\leq J-1})| \text{ or}$$

$$|X^*(\tau_\omega^{\leq J})| > |X^*(\tau_\omega^{\leq J-1})|. \tag{24}$$

Note that the event $\omega \in \Omega^j_{red} \cap \Omega^j_{blue}$ implies the event that

$$\sum_{J=1}^{j-1} DB_J(\omega) \geq \frac{\Delta - (R+n-1)}{R+n-1}. \tag{25}$$

This is because each query along τ_ω increases $(X(\tau_\omega) \oplus k_\omega) \cap U(\tau)$ by at most one and $(\bar{Y}(\tau_\omega) \oplus k_\omega) \cap V(\tau)$ by at most $R+n-1$ and $X^*(\tau_\omega)$ by at most two.

In particular, each E-query can increases $(X(\tau_\omega) \oplus k_\omega) \cap U(\tau)$ by at most one and $X^*(\tau_\omega)$ by at most two, each P- or P^{-1}-query can increases $(X(\tau_\omega) \oplus k_\omega) \cap U(\tau)$ and $(\bar{Y}(\tau_\omega) \oplus k_\omega) \cap V(\tau)$ by at most one, and each F-query can increase $(\bar{Y}(\tau_\omega) \oplus k_\omega) \cap V(\tau)$ by at most $R+n-1$ and $X^*(\tau_\omega)$ by at most one.

We bound the probability of the event in relation (25) over Ω^{j-1}_{green}.

We do this by bounding the probability of the event $DB_J(\omega) = 1$ over Ω^{j-1}_{green} for all $J = 1, \cdots, j-1$.

Let us fix a number J, $1 \leq J \leq j-1$.

Note that

$$Pr_{\Omega^{j-1}_{green}}[DB_J(\omega) = 1] = \sum_{\tau \in \mathcal{T}^J_{green}} Pr_{\Omega^{j-1}_{green}}[\tau] \cdot Pr_{\Omega^{j-1}_{green}(\tau)}[DB_J(\omega) = 1|]. \tag{26}$$

Note further that for all $\tau \in \mathcal{T}^J_{green}$ and $\omega \in \Omega^{j-1}_{green}(\tau)$ it holds that $DB_J(\omega) = 1$ if and only if at least one of the following conditions is fulfilled.

(A) The J-th query in τ is a P-query with input u or an P^{-1}-query with output u and $k_\omega \in u \oplus X(\tau)$.
(B) The J-th query in τ is a P-query with output v or an P^{-1}-query with input v and $k_\omega \in v \oplus \bar{Y}(\tau)$.
(C) The J-th query in τ is an F-query with input y and there is some r, $0 \leq r \leq R-1$, such that $k_\omega \in \pi^{-r}(y) \oplus V(\tau)$.
(D) The J-th query in τ is an E-query with input x and $k_\omega \in x \oplus U(\tau)$.
(E) The J-th query in τ is an E-query with input x and $P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}$ for some $\bar{y} \in \bar{Y}(\tau)$.
(F) The J-th query in τ is an F-query with input y and $y = \pi^i(P_\omega(x \oplus k_\omega) \oplus k_\omega)$ for some $x \in X(\tau) \setminus X^*(\tau)$ and some number i, $-(n-1) \leq i \leq R-1$.
(G) The J-th query in τ is an E-query with input x and $P_\omega(x \oplus k_\omega) \oplus k_\omega = \pi^i(P_\omega(x \oplus k_\omega) \oplus k_\omega)$ for some $x' \in X(\tau)$ and some number r, $-(R-1) \leq i \leq R-1$.

Note that (A) and (E) are the situations in which query J increases $(X(\tau_\omega) \oplus k_\omega) \cap U(\tau_\omega)$, that (B) and (C) are the situations in which query J increases $(\bar{Y}(\tau_\omega) \oplus k_\omega) \cap V(\tau_\omega)$, that (E) and (F) are the situations in which query J generates a new structural EF-collision (i.e., increases $X^*(\tau)$ by one), and that (G) is the situation in which query J generates a new structural EE-collision (i.e., increases $X^*(\tau)$ by one or two).

Note further that conditions (A,B,D) imply that k_ω belongs to a set of at most $J-1$ elements, or to a set of at most $(R+n-1)\cdot(J-1)$ elements (condition (C)).

From Corollary 2, part (a), it follows that these events have probability at most $2^{-(n-1)} \cdot (R+n-1) \cdot (J-1)$.

From Corollary 2, part (b), it follows that condition (E) has probability at most $9 \cdot |\bar{Y}(\tau_\omega)| \cdot 2^{-(n-1)} \leq 9 \cdot (R+n-1) \cdot (J-1)$, and that condition (F) has probability at most $9 \cdot (2n-1) \cdot |X(\tau_\omega)| \cdot 2^{-(n-1)} \leq 9 \cdot (2n-1) \cdot (J-1)$.

From Corollary 2, part (c), it follows that condition (E) has probability at most $11 \cdot (2R-1) \cdot |X(\tau_\omega)| \cdot 2^{-(n-1)} \leq 11 \cdot (2R-1) \cdot (J-1) \cdot 2^{-(n-1)}$.

We obtain that for all J, $1 \leq J \leq j-1$,

$$Pr_{\Omega^J_{green}}[DB_J(\omega) = 1] \leq 11 \cdot 2^{-(n-1)} \cdot (2R-1) \cdot (J-1).$$

$$\leq 22 \cdot 2^{-(n-1)} \cdot R \cdot (j-1). \tag{27}$$

Relation (27) enables us to apply the Chernov Bound Method from Lemma 8 in subsection B with $N = j-1$, $p = 22 \cdot 2^{-(n-1)} \cdot R \cdot (j-1)$ and $D = n$, and to obtain directly that

$$Pr_{\tilde{\Omega}^{good,j-1}}\left[\sum_{J=1}^{j-1} DB_J(\omega) > 22 \cdot 2^{-(n-1)} \cdot R \cdot (j-1)^2 + \sqrt{\frac{n \cdot (j-1)}{2}}\right] < e^{-n}. \tag{28}$$

Note that relation (3) of Definition 4 says that

$$22 \cdot 2^{-(n-1)} \cdot R \cdot (j-1)^2 + \sqrt{\frac{n \cdot (j-1)}{2}}$$

$$\leq 22 \cdot 2^{-(n-1)} \cdot R \cdot M^2 + \sqrt{\frac{n \cdot M}{2}} \leq \frac{\Delta - (R+n-1)}{R+n-1}. \tag{29}$$

Thus, Relation (28) together with Relation (29) proves Relations (23) and (21), and, consequently, Lemma 4, part (ii). □

4.13 The Proof of Corollary 2, Parts (b) and (c)

Let us fix an arbitrary number j, $1 \leq j \leq M$, and a green transcript $\tau \in \mathcal{T}^j_{green}$. We assume that part (a) of Corollary 2 holds, i.e., that for all $k \in K^{green}(\tau)$

$$Pr_{\Omega^{green}(\tau)}[k_\omega = k] \leq 2^{-(n-1)}. \tag{30}$$

Let us first prove part (b) of Corollary 2. We fix some $x, \bar{y} \in \{0,1\}^n$, where $x \notin X^*(\tau)$ and $\bar{y} \notin \bar{Y}^*(\tau)$ and ($x \notin X(\tau)$ or $\bar{y} \notin \bar{Y}(\tau)$). We have to show

$$Pr_{\Omega^{green}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}] \leq 9 \cdot 2^{-(n-1)}. \tag{31}$$

Proof of Relation (31):

We divide $K^{green}(\tau)$ into two subsets Ω_1 and Ω_2, where

$$\Omega_1 = \{\omega \in \Omega^{green}(\tau); x \oplus k_\omega \notin U(\tau)\},$$
$$\Omega_2 = \{\omega \in \Omega^{green}(\tau); x \oplus k_\omega \in U(\tau)\}, \tag{32}$$

and denote

$$K_1 = \{k \in K^{green}(\tau); x \oplus k \notin U(\tau)\}.$$
$$K_2 = \{k \in K^{green}(\tau); x \oplus k \in U(\tau)\}. \tag{33}$$

The sets Ω_2 and K_2 define another set $W \subseteq \{0,1\}^n$ by

$$W = \{P_\omega(x \oplus k_\omega) \oplus k_\omega; \omega \in \Omega_2\} = \{P_\tau(x \oplus k) \oplus k; k \in K_2\}.$$

Here, P_τ denotes the restriction of P_ω to $U(\tau)$ which, by definition, is equal for all $\omega \in \Omega(\tau)$.

Note that $|W| \leq |K_2| = |U(\tau)| \leq j \leq M$.

Let us now define an equivalence relation on K_2.

For keys $k, k' \in K_2$ we define that $k \equiv k'$ if $P_\tau(x \oplus k) \oplus k = P_\tau(x \oplus k') \oplus k'$.

Let $L_1, \cdots, L_s$ denote the equivalence classes corresponding to the equivalence relation $\equiv$ on K_2.

Clearly, $s = |W|$ and for each class L_j, $1 \leq j \leq s$, there is exactly one $w \in W$ such that $P_\tau(x \oplus k) \oplus k = w$ for all $k \in L_j$.

Note that $k \equiv k'$ implies that $x \oplus k \equiv_{P_\tau} x \oplus k'$ in the sense of Definition 11 and remember that, as τ is not black, that $Max(P_\tau, U(\tau)) \leq 5$. This implies

Lemma 6. *For all $w \in W$, the number of keys $k \in K_2$ for which $P_\tau(x \oplus k) \oplus k = w$ is at most five.* □

Note that $Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}]$ equals

$$Pr_{\Omega^{good}(\tau)}[\Omega_1] \cdot Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_1]$$
$$+Pr_{\Omega^{good}(\tau)}[\Omega_2] \cdot Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_2],$$

i.e.,

$$Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}] \leq$$
$$Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_1]$$
$$+Pr_{\Omega^{good}(\tau)}[\Omega_2] \cdot Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_2]. \tag{34}$$

For estimating $Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_1]$ note that if $k_\omega \notin U(\tau)$ then $P_\omega(x \oplus k_\omega)$ takes all values in $\{0,1\}^n$, which are outside of $V(\tau) \cup (\bar{Y}(\tau) \oplus k_\omega)$, with the same probability (see the proof of Lemma 2).

This implies that

$$Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_1] \leq \frac{1}{2^n - (R+n-2)M} \leq 2^{-(n-1)} \tag{35}$$

if n is large enough.

Observe next that by Relation (30) it holds that

$$Pr_{\Omega^{good}{}_\tau}[\Omega_2] \leq 2^{-(n-1)} \cdot |K_2|. \tag{36}$$

For estimating $Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_2]$ we consider first the case that $\bar{y} \notin W$. Then, by the definition of W, it holds that

$$Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_2] = 0.$$

Assume now that $\bar{y} \in W$. From Lemma 6 and the Smoothness Lemma (Lemma 5) it follows that

$$Pr_{\Omega^{good}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}|\Omega_2] \leq \sqrt{2}\frac{5}{|K_2|} \leq \frac{8}{|K_2|}. \tag{37}$$

Putting relations (35), (36), and (37) together yields

$$\begin{aligned} Pr_{\Omega^{good}}[P_\omega(x \oplus k_\omega) \oplus k_\omega = \bar{y}] &\leq 2^{-(n-1)} + 2^{-(n-1)} \cdot |K_2| \cdot \frac{8}{|K_2|} \\ &= 9 \cdot 2^{-(n-1)}. \ \square \end{aligned} \tag{38}$$

Let us now prove part (c) of Corollary 2. We fix some $x \neq x' \in \{0,1\}^n$, where (w.l.o.g.) $x \notin X(\tau)$, and some number i, $-(n-1) \leq i \leq R+n-2$. We have to show

$$Pr_{\Omega^{green}(\tau)}[Ev(x,x',i)] \leq 11 \cdot 2^{-(n-1)}, \tag{39}$$

where the event $Ev(x,x',i) \subseteq \Omega^{green}(\tau)$ is defined to be

$$Ev(x,x',i) = \left\{\omega \in \Omega^{green}(\tau); \pi^i\left(P_\omega(x \oplus k_\omega) \oplus k_\omega\right) = P_\omega(x' \oplus k_\omega) \oplus k_\omega\right\}.$$

Proof of Relation (39):

Let us first handle the case that $x' \in X^*(\tau)$ and denote by y' the unique value for which $(x',y') \in Coll(\tau)$. Then, by the definition of EF-collisions, it holds that

$$P_\omega(x' \oplus k_\omega) \oplus k_\omega = y'$$

for all $\omega \in \Omega^{green}(\tau)$.

Consequently, for all $\omega \in \Omega^{green}(\tau)$ it holds that $\omega \in Ev(x,x',i)$ if and only if

$$P_\omega(x \oplus k_\omega) \oplus k_\omega = \pi^{-i}(y').$$

From part (b) of Corollary 2 it follows that if $x' \in X^*(\tau)$ then

$$Pr_{\Omega^{green}(\tau)}[Ev(x,x',i)] \leq 9 \cdot 2^{-(n-1)} < 11 \cdot 2^{-(n-1)}.$$

Now let us consider the case that $x' \in X(\tau) \setminus X^*(\tau)$.

For arbitrary points $z \in \{0,1\}^n$ we define

$$\Omega^{green}(\tau, z) = \{\omega \in \Omega^{green}(\tau); P_\omega(x \oplus k_\omega) \oplus k_\omega = z\}$$

and,

$$K^{green}(\tau, z) = \{k \in \{0,1\}^n ; \exists \omega \in \Omega^{green}(\tau, z) : k_\omega = k\}.$$

Moreover, for $b \in \{1,2\}$ we define

$$\Omega_b(z) = \Omega^{green}(\tau, z) \cap \Omega_b,$$

and

$$K_b(z) = K^{green}(\tau, z) \cap K_b,$$

where the sets Ω_1 and Ω_2 (and the sets K_1 and K_2) are defined as in relations (32) and (33).

Let us clarify how the keys in elementary events in Ω_1 and Ω_2 and the keys in $K_1(z)$ and $K_2(z)$ are looking like.

It can be easily checked that for all $\omega = (k_\omega, P_\omega, F_\omega) \in \Omega_1$ it holds $\omega \in \Omega_1(z)$ if and only if $z \oplus k_\omega \notin V(\tau)$ and $P_\omega(x \oplus k_\omega) = z \oplus k_\omega$.

Moreover, for all $\omega = (k_\omega, P_\omega, F_\omega) \in \Omega_2$ it holds $\omega \in \Omega_2(z)$ if and only if $P_\tau(x \oplus k_\omega) \oplus k_\omega = z$, which implies by Lemma 6 that

$$|K_2(z)| \leq 5. \tag{40}$$

We obtain that

$$|K^{green}(\tau, z)| \geq |K^1(z)| \geq |K_1| - |V(\tau)| = |K^{green}(\tau)| - |K_2| - |V(\tau)|$$

$$\geq |K^{green}(\tau)| - 2 \cdot |V(\tau)| \geq |K^{green}(\tau)| - 2M \geq \frac{1}{\sqrt{2}} \cdot 2^n \tag{41}$$

if n is large enough.

By exactly the same arguments as in the Smoothness Lemma (Lemma 5) one can show that for all $k, k' \in K^{green}(\tau, z)$ it holds that

$$Pr_{\Omega^{green}(\tau,z)}[k_\omega = k] \leq \sqrt{2} \cdot Pr_{\Omega^{green}(\tau,z)}[k_\omega = k']. \tag{42}$$

if n is large enough.

Relations (41) and (42) imply directly that for all $k \in K^{green}(\tau, z)$ it holds

$$Pr_{\Omega^{green}(\tau,z)}[k_\omega = k] \leq 2^{-(n-1)} \tag{43}$$

if n is large enough.

Note that

$$Pr_{\Omega^{green}(\tau)}[Ev(x, x', i)] =$$

$$\sum_{z \in \{0,1\}^n} Pr_{\Omega^{green}(\tau)}[P_\omega(x \oplus k_\omega) \oplus k_\omega = z] \cdot Pr_{\Omega^{green}(\tau,z)}[Ev(x, x', i)]. \tag{44}$$

For deriving an upper bound for $Pr_{\Omega^{green}(\tau,z)}[Ev(x,x',i)]$ we write

$$\begin{aligned}Pr_{\Omega^{green}(\tau,z)}[Ev(x,x',i)] &= Pr_{\Omega^{green}(\tau,z)}[\Omega_1^{green}(\tau,z)] \cdot Pr_{\Omega_1^{green}(\tau,z)}[Ev(x,x',i)] \\ &+Pr_{\Omega^{green}(\tau,z)}[\Omega_2^{green}(\tau,z)] \cdot Pr_{\Omega_2^{green}(\tau,z)}[Ev(x,x',i)]. \\ &\leq Pr_{\Omega_1^{green}(\tau,z)}[Ev(x,x',i)] + Pr_{\Omega^{green}(\tau,z)}[\Omega_2^{green}(\tau,z)] \\ &\leq Pr_{\Omega_1^{green}(\tau,z)}[Ev(x,x',i)] + 5 \cdot 2^{-(n-1)}, \end{aligned} \tag{45}$$

where the last inequality follows from Relations (40) and (42).

We write $K_1(z)$ as

$$K_1(z) = K_3(z) \cup K_4(z) \cup K_5(z),$$

where

- $K_3(z) = \{k \in K_1(z); x' \oplus k \in U(\tau),\ P_\tau(x' \oplus k) \oplus k = \pi^i(z)\}$,
- $K_4(z) = \{k \in K_1(z); x' \oplus k \in U(\tau),\ P_\tau(x' \oplus k) \oplus k \neq \pi^i(z)\}$,
- $K_5(z) = \{k \in K_1(z); x' \oplus k \notin U(\tau)\}$.

From Lemma 6 we know that $|K_3^z| \leq 5$ and that for all $k \in K_4^z$ it holds

$$Pr_{\Omega_1^{green}(\tau,z)}[Ev(x,x',i) \cap (k_\omega \in K_4(z))] = 0.$$

Consequently,

$$\begin{aligned}Pr_{\Omega_1^{green}(\tau,z)}[Ev(x,x',i)] &\leq Pr_{\Omega_1^{green}(\tau,z)}[Ev(x,x',i) \cap (k_\omega \in K_5(z))] + 5 \cdot 2^{-(n-1)} \\ &\leq Pr_{\Omega_5^{green}(\tau,z)}[Ev(x,x',i)] + 5 \cdot 2^{-(n-1)}, \end{aligned} \tag{46}$$

where $\Omega_5^{green}(\tau,z) = \{\omega \in \Omega_1^{green}(\tau,z); k_\omega \in K_5(z)\}$.

Note that for all $\omega \in \Omega_5^{green}(\tau,z)$, the condition that $\omega \in Ev(x,x',i)$ is equivalent to

$$P_\omega(x' \oplus k) = \pi^i(z) \oplus k_\omega,$$

which has probability 0 if $\pi^i(z) \oplus k_\omega \in V(\tau)$ and probability at most

$$\frac{1}{2^n - (|V(\tau| + 1) - |\bar{Y}(\tau)|} \leq 2^{-(n-1)}$$

if $\pi^i(z) \oplus k_\omega \notin V(\tau)$ and n is large enough, see relation (35) and the comment before relation (35).

We obtain that

$$Pr_{\Omega_5^{green}(\tau,z)}[Ev(x,x',i)] \leq 2^{-(n-1)} \tag{47}$$

if n is large enough.

Putting Relations (47), (46), and (45) we obtain that for all $z \in \{0,1\}^n$

$$Pr_{\Omega^{green}(\tau,z)}[Ev(x,x',i)] \leq 11 \cdot 2^{-(n-1)},$$

which implies by Relations (44) that

$$Pr_{\Omega^{green}(\tau)}[Ev(x,x',i)] \leq 11 \cdot 2^{-(n-1)}. \ \square$$

4.14 The Proof of the Smoothness Lemma (Lemma 5)

We fix an arbitrary number j, $1 \leq j \leq M$ and a green transcript $\tau \in \mathcal{T}^j_{green}$. We analyze the probability distribution $Pr_{\Omega(\tau)}$ on $K^{green}(\tau)$ by showing that for all $k \in K^{green}(\tau)$ it holds that this distribution is close to the uniform distribution on $K^{green}(\tau)$.

$$Pr_{\Omega(\tau)}[k] \leq \delta \cdot |K^{green}(\tau)|^{-1},$$
$$\text{where } \delta = \left(\frac{2^n}{2^n - ((n+R+2)j + \Delta)}\right)^{2\Delta}. \tag{48}$$

Note that relation (5) of Definition 4 implies $\delta \leq \sqrt{2}$.

This is because we can write δ as

$$\delta = \left(\frac{T}{T-t}\right)^{2\Delta} = \left(\frac{1}{1-t/T}\right)^{2\Delta} = \left(\left(\frac{1}{1-t/T}\right)^{T/t}\right)^{\frac{2\Delta t}{T}} \approx e^{\frac{2\Delta t}{T}}.$$

for $t = (n+R+2)j + \Delta$ and $T = 2^n$.

Relation (4) of Definition 4 says that $\Delta \cdot t \leq \frac{\ln(2) \cdot T}{4}$ which is equivalent to

$$\frac{2\Delta t}{T} \leq \frac{\ln 2}{2}.$$

The Proof of Relation (48)

The proof of Lemma 2 shows how, for keys $k \in K(\tau)$, completions P' of P_τ on $\{0,1\}^n \setminus U(\tau)$ and F' of F_τ on $\{0,1\}^n \setminus Y(\tau)$ have to be constructed such that (k, P', F') belongs to $\Omega(\tau)$. In particular:

(1) The function values of P' on $X^*(\tau) \oplus k$, a set of size $|X^*(\tau)|$, are determined.
(2) The function values of P' on the set $((X(\tau) \setminus X^*(\tau)) \oplus k) \setminus U(\tau)$ are forbidden to fall into the set $((\bar{Y}(\tau) \setminus \bar{Y}^*(\tau)) \oplus k) \setminus V(\tau)$.
(3) The function values of F' are determined on a set of size $|X(\tau) \setminus X^*(\tau)|$.

Note that for proving Lemma 5 it is sufficient to show that for all pairs $k, k' \in K^{green}(\tau)$

$$\frac{Pr_{\Omega(\tau)}[k]}{Pr_{\Omega(\tau)}[k']} \leq \delta.$$

For this purpose, let us denote by $ConsP_\tau(k)$ the set of all completions P' of P_τ on $\{0,1\}^n \setminus U(\tau)$ for which there is some completion F' of F_τ on $\{0,1\}^n \setminus Y(\tau)$ such that the elementary event (k, P', F') belongs to $\Omega(\tau)$.

The above statement (3) implies that for all $k \in K(\tau)$ and completions $P' \in ConsP_\tau(k)$, the number of such completions F' is the same, i.e., does not depend on k.

This implies that

$$\frac{Pr_{\Omega(\tau)}[k]}{Pr_{\Omega(\tau)}[k']} = \frac{|ConsP_\tau(k)|}{|ConsP_\tau(k')|}.$$

Note that due to requirement (2) (see above), the size of $ConsP_\tau(k)$ depends on the sizes of the sets $((X(\tau)\setminus X^*(\tau))\oplus k)\setminus U(\tau)$ and $(\bar{Y}(\tau)\setminus\bar{Y}^*(\tau))\oplus k)\setminus V(\tau)$, which can vary between 0 and Δ.

Thus, for $k \in K^{green}(\tau)$, the value $|ConsP_\tau(k)|$ is minimal if

$$|((X(\tau)\setminus X^*(\tau))\oplus k)\cap U(\tau)| = |((\bar{Y}(\tau)\setminus\bar{Y}^*(\tau))\oplus k)\cap V(\tau)| = 0, \qquad (49)$$

and maximal if

$$|((X(\tau)\setminus X^*(\tau))\oplus k)\cap U(\tau)| = \Delta, \text{ or } (X(\tau)\setminus X^*(\tau))\oplus k \subseteq U(\tau)$$

and

$$|((\bar{Y}(\tau)\setminus\bar{Y}^*(\tau))\oplus k)\cap V(\tau)| = \Delta, \text{ or } (\bar{Y}(\tau)\setminus\bar{Y}^*(\tau))\oplus k \subseteq V(\tau). \qquad (50)$$

Note here that the cases that $(X(\tau)\setminus X^*(\tau))\oplus k \subseteq U(\tau)$ and $(\bar{Y}(\tau)\setminus\bar{Y}^*(\tau))\oplus k \subseteq V(\tau)$ can only occur if $|(X(\tau)\setminus X^*(\tau)| \leq \Delta$ and $|\bar{Y}(\tau)\setminus\bar{Y}^*(\tau)| \leq \Delta$, respectively.

We have now to distinguish four cases corresponding to if $|(X(\tau)\setminus X^*(\tau)| > \Delta$ or not and if $|\bar{Y}(\tau)\setminus\bar{Y}^*(\tau)| > \Delta$ or not.

Case 1: $|(X(\tau)\setminus X^*(\tau)| > \Delta$ and $|\bar{Y}(\tau)\setminus\bar{Y}^*(\tau)| > \Delta$.
In this case, it follows from (49) that $|ConsP_\tau(k)|$ is at least

$$T!\cdot S(S-1)\cdots(S-(t-1))$$

$$= T!\cdot S(S-1)\cdots(S-(t-1)+2\Delta)(S-(t-1)+2\Delta-1)\cdots(S-(t-1)),$$

where we denote $T = 2^n - |U(\tau)| - |X(\tau)|$ and $t = |X(\tau)\setminus X^*(\tau)|$ and $S = 2^n - |V(\tau)| - |\bar{Y}(\tau)|$ and $s = |\bar{Y}(\tau)\setminus\bar{Y}(\tau)|$.
Moreover, relation (50) yields that $|ConsP_\tau(k)|$ is at most

$$(T+\Delta)!\cdot(S+\Delta)\cdot(S+\Delta-1)\cdots(S+\Delta-(t-\Delta-1))$$

$$= (T+1)\cdots(T+\Delta)\cdot T!\cdot(S+1)\cdots(S+\Delta)\cdot S(S-1)\cdots(S-(t-1)+2\Delta).$$

This implies that the $Pr_{\Omega(\tau)}$-values of elements from $K^{green}(\tau)$ can differ by a factor δ which is at most $\delta_1\cdot\delta_2$, where

$$\delta_1 = \frac{(T+1)(T+2)\cdots(T+\Delta)}{(S-(t-1))(S-(t-1)+1)\cdots(S-(t-1)+\Delta-1)},$$

$$\delta_2 = \frac{(S+1)(S+2)\cdots(S+\Delta)}{(S-(t-1)+\Delta)(S-(t-1)+\Delta+1)\cdots(S-(t-1)+2\Delta-1)}.$$

Note that

$$\delta_2 \leq \left(\frac{S}{S-t+\Delta}\right)^{\Delta}.$$

Here we used the fact that from $a > b$ it follows that $\frac{a}{b} > \frac{a+1}{b+1}$.

For upper bounding δ_1 we have to distinguish the two cases $S \geq T$ and $S < T$.

If $S \geq T$ then

$$\delta_1 \leq \frac{(S+1)(S+2)\cdots(S+\Delta)}{(S-(t-1))(S-(t-1)+1)\cdots(S-(t-1)+\Delta-1)} \leq \left(\frac{S}{S-t}\right)^{\Delta}$$

If $S < T$ then observe that $S \geq T-(R+n-1)j$. This holds because $|\bar{Y}(\tau)| \leq (R+n-1)j$. Consequently,

$$\delta_1 \leq \left(\frac{T}{T-t-n(R+n-1)j}\right)^{\Delta} \leq \left(\frac{T}{T-(R+n-1)j}\right)^{\Delta}.$$

With similar arguments, the other four cases can be handled.

Case 2: $|(X(\tau) \setminus X^*(\tau)| > \Delta$ and $|\bar{Y}(\tau) \setminus \bar{Y}^*(\tau)| \leq \Delta$.
Here, relation (49) yields that $|ConsP_\tau(k)|$ is at least

$$T!(T-\Delta+1)\cdots(T-\Delta+t)$$

and relation (49) yields that $|ConsP_\tau(k)|$ is at most $(T+t)!$.

This implies that the $Pr_{\Omega(\tau)}$-values of elements from $K^{green}(\tau)$ can differ by a factor

$$\delta = \frac{(T+1)(T+2)\cdots(T+t)}{(T-\Delta+1)(T-\Delta+2)\cdots(T-\Delta+t)}$$

$$= \frac{(T+t-(\Delta-1))\cdots(T+t)}{(T-(\Delta-1))\cdots T} \leq \left(\frac{T+t-\Delta}{T-\Delta}\right)^{\Delta}.$$

Case 3: $|(X(\tau) \setminus X^*(\tau)| \leq \Delta$ and $|\bar{Y}(\tau) \setminus \bar{Y}^*(\tau)| > \Delta$.
Here, relation (49) yields that $|ConsP_\tau(k)|$ is at least

$$(S+s-\Delta)!S(S-1)\cdots(S-(\Delta-1))$$

and relation (50) yields that $|ConsP_\tau(k)|$ is at most $(S+s)!$.

This implies that the $Pr_{\Omega(\tau)}$-values of elements from $K^{green}(\tau)$ can differ by a factor

$$\delta = \frac{(S+s-(\Delta-1))\cdots(S+s)}{(S-(\Delta-1))\cdots(S-1)S} \leq \left(\frac{S+s-\Delta}{S-\Delta}\right)^{\Delta}.$$

Case 4: $|(X(\tau) \setminus X^*(\tau)| \leq \Delta$ and $|\bar{Y}(\tau) \setminus \bar{Y}^*(\tau)| \leq \Delta$.
Here, relation (49) yields that $|ConsP_\tau(k)|$ is at least

$$S! \cdot S \cdot (S-1)\cdots(S-(\Delta-1))$$

and relation (50) yields that $|ConsP_\tau(k)|$ is at most $(S+\Delta)!$,

This implies that the $Pr_{\Omega(\tau)}$-values of elements from $K^{green}(\tau)$ can differ by a factor

$$\delta = \frac{(S+1)\cdots(S+\Delta)}{(S-(\Delta-1))\cdots(S-1)S} \leq \left(\frac{S}{S-\Delta}\right)^{\Delta}.$$

Summarizing all four cases we obtain that

$$\delta \leq \left(\frac{2^n}{2^n-((n+R+2)j+\Delta)}\right)^{2\Delta}. \square$$

5 Concluding Remarks

In this paper, we introduced for the first time an ideal primitive model (IPM) for KSG-based stream ciphers and proved a sharp asymptotic $(2/3)n$-bound on the security of the LIZARD-construction, which underlies the stream cipher LIZARD [14], against generic chosen-IV key recovery and packet prediction TMD tradeoff attacks. We hope that the security model and the lower bound techniques developed in this paper help to prove similar sharp security bounds for other stream cipher constructions like, e.g., the concatenation method underlying the state initialization of Trivium and Grain (see relations (3) and (4)), or the Sprout-construction (see [2]). We have further shown that for a packet length $R > n$, where n denotes the inner state length of the underlying KSG, KSG-based stream ciphers are only $n/2$-secure w.r.t. generic TMD tradeoff distinguishing attacks. It would be interesting to analyze the case $R = n$. Our conjecture is that for $R = n$, the LIZARD-construction is $(2/3)n$-secure even against distinguishing attacks. Clearly, this is a problem of rather theoretical nature as, from a technical point of view, it may appear questionable if KSG-based stream ciphers of packet length $R = n$ make much sense, because the reinitialization effort per keystream bit would be high. But in the context of the further development of security lower bound proof techniques, this problem is interesting and should be solved.

References

1. Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the indifferentiability of key-alternating ciphers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 531–550. Springer, 2013.
2. Frederik Armknecht and Vasily Mikhalev. On lightweight stream ciphers with shorter internal state. In *To appear at Fast Software Encryption*. Springer, 2015.
3. S.H. Babbage. Improved "exhaustive search" attacks on stream ciphers. In *Security and Detection, 1995., European Convention on*, pages 161–166, May 1995.
4. Alex Biryukov and Adi Shamir. Cryptanalytic time/memory/data tradeoffs for stream ciphers. In Tatsuaki Okamoto, editor, *Advances in Cryptology — ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 1–13. Springer Berlin Heidelberg, 2000.

5. Andrey Bogdanov, LarsR. Knudsen, Gregor Leander, Francois-Xavier Standaert, John Steinberger, and Elmar Tischhauser. Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer Berlin Heidelberg, 2012.
6. Christophe De Cannière and Bart Preneel. Trivium - specifications (eSTREAM). Technical report, ECRYPT (European Network of Excellence for Cryptology), 2005. `http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf`.
7. Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John Steinberger. Minimizing the two-round even-mansour cipher. In JuanA. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 39–56. Springer Berlin Heidelberg, 2014.
8. Shan Chen and John Steinberger. Tight security bounds for key-alternating ciphers. In PhongQ. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 327–350. Springer Berlin Heidelberg, 2014.
9. Orr Dunkelman and Nathan Keller. Treatment of the initial value in time-memory-data tradeoff attacks on stream ciphers. Cryptology ePrint Archive, Report 2008/311, 2008. `http://eprint.iacr.org/2008/311`.
10. Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The even-mansour scheme revisited. In *Proceedings of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'12, pages 336–354, Berlin, Heidelberg, 2012. Springer-Verlag.
11. Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In Hideki Imai, RonaldL. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology — ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 210–224. Springer Berlin Heidelberg, 1993.
12. Peter Gazi and Stefano Tessaro. Secret-key cryptography from ideal primitives: A systematic overview. In *Information Theory Workshop (ITW), 2015 IEEE*, pages 1–5, April 2015.
13. Vahid Amin Ghafari, Honggang Hu, and Chengxin Xie. Fruit: Ultra-lightweight stream cipher with shorter internal state. Cryptology ePrint Archive, Report 2016/355, 2016. `http://eprint.iacr.org/2016/355`.
14. Matthias Hamann, Matthias Krause, and Willi Meier. LIZARD – A Lightweight Stream Cipher for Power-constrained Devices. Cryptology ePrint Archive, Report 2016/926, 2016. `http://eprint.iacr.org/2016/926`.
15. Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. The Grain family of stream ciphers. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*, pages 179–190. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.
16. Martin Hell, Thomas Johansson, and Willi Meier. Grain - a stream cipher for constrained environments (eSTREAM). Technical report, ECRYPT (European Network of Excellence for Cryptology), 2005. `http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain_p3.pdf`.
17. Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. Cryptology ePrint Archive, Report 2016/578, 2016. `http://eprint.iacr.org/2016/578`.

18. Jacques Patarin. The "coefficients H" technique. In RobertoMaria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer Berlin Heidelberg, 2009.
19. Bluetooth SIG. Bluetooth core specification 4.2, 2014. `https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439`.

A An $O(2^{n/2})$ Distinguishing Attack against the LIZARD-Construction

Let us first define an adequate distinguishing game between Alice and Eve. This can be easily obtained by modifying the Definition 3 in the following points

Definition 17. *(i) The game depends on the global parameters π, M, n, R, where π denotes a fixed bijective state transition function $\pi : \{0,1\}^n \longrightarrow \{0,1\}^n$, M, n, R denote natural numbers, and n, R, π fulfill the conditions [A1, A2]. The game is divided into a query phase and a decision phase.*

(ii) At the beginning. Alice chooses randomly and w.r.t. the uniform distribution a secret 5-tuple $\omega = (b_\omega, k_\omega, P_\omega, F_\omega, E_\omega)$, where

- *$b_\omega \in \{0,1\}$*
- *$k_\omega \in \{0,1\}^n$ denotes the session secret key.*
- *$P_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ denotes a random permutation,*
- *$F_\omega : \{0,1\}^n \longrightarrow \{0,1\}^n$ denotes a random π-iterative function.*
- *$E_\omega : \{0,1\}^n \longrightarrow \{0,1\}^R$ denotes a random function.*

We denote by Ω the corresponding probability space of all such triples together with the uniform distribution.

(iii) The adversary Eve is supposed to be a randomized oracle algorithm of potentially unbounded computational power, who is allowed to pose component oracle queries of type $P(u) =?$, or $P^{-1}(v) =?$-, or $F(y) =?$ for inputs $u, v \in \{0,1\}^n$ and $y \in \{0,1\}^n$, which are correctly answered by Alice by $P_\omega(u)$, $(P_\omega)^{-1}(v)$, or $F_\omega(y)$, respectively.

(iv) Moreover, Eve can pose construction oracle queries of the form $E(x) =?$, where $x \in \{0,1\}^n$.
If $b_\omega = 0$ (the truly random case), Alice answers such questions with the random packet $E_\omega(x)$.
If $b_\omega = 1$ (the pseudorandom case), Alice answers such questions in accordance with Definition 3, i.e., with the keystream packet corresponding to the initial state $y := P_\omega(x \oplus k_\omega) \oplus k_\omega$ induced by the session key k_ω and the initial value x. Note again that this keystream packet is the concatenation of the R/n F-values

$$F_\omega(y)||F_\omega(\pi^n(y))||\cdots||F_\omega(\pi^{n(R/n-1)}(y)).$$

(v) In the query phase, Eve is allowed to pose exactly M oracle queries. In the decision phase, Eve has to submit some $b \in \{0,1\}^n$. Eve wins if $b = b_\omega$.

(vi) Besides the running time and the number M of oracle queries, the essential cost parameter is the advantage reached by Eve, which is defined to be the absolute value of the difference of the probabilities that Eve outputs 1 under the condition that $b_\omega = 0$ and $b_\omega = 1$, respectively. measured with respect to the uniform distribution on Ω and the internal randomization of Eve.

Note that in the truly random case, Alice outputs keystream packets in dependence of input initial values $x \in \{0,1\}^n$ according to a truly random function, and independently of k_ω and the ideal primitives P_ω and F_ω. We prove

Theorem 4. *If $R > n$, then Eve can reach advantage $1/4$ with $M = \Theta(2^{n/2})$ oracle queries and running time $M = \Theta(2^{n/2})$.*

Proof: We only sketch the proof, which is quite straightforward. Using the same idea as in the proof of Theorem 1, one can show that with $\Theta(2^{n/2})$ E-queries and $\Theta(2^{n/2})$ F-queries, Eve can generate an EF-collision (x, y) with probability greater $1/2$. Here, a pair $(x, y) \in \{0,1\}^n \times \{0,1\}^n$ is called EF-collision, if and only if the block the first n bits of z coincides with $F_\omega(y)$, where $z \in \{0,1\}^R$ denotes the answer of the E-query with input x.

Alice outputs $b = 1$ (pseudorandom!) if z_{n+1} equals the last bit of $F_\omega(\pi(y))$.

Note that if $b_\omega = 1$ (the pseudorandom scenario) the probability that Eve outputs $b = 1$ is one. In the random scenario, this probability is exactly $1/2$. □

B A Short Excursion to Chernov Bounds

At several places of our proof we have to apply a technique called *Chernov Bounds* in the literature. The basic *Chernov Bound* argument is the following.

Theorem 5. *Let N be a positive integer, $p \in (0,1)$, and $A_1, \cdots, A_N$ be a set of mutually independent random variables, where, for all $i = 1, \cdots, N$, it holds that $Pr[A_i = 1 - p] = p$ and $Pr[A_i = -p] = 1 - p$. Let $A = \sum_{i=1}^{N} A_i$. Then*

$$Pr[A > a] < e^{-\frac{2a^2}{N}} \tag{51}$$

for all $a > 0$.

For a **proof** see, e.g., Alon, Spencer, Erdos, The Probabilistic Method, Wiley Interscience 1992, Theorem A4 on page 235. □

We derive from Theorem 5 a corresponding result for random $\{0,1\}$-variables.

Lemma 7. *Let p, N, and A_i for $i = 1, \cdots, N$ be defined as in Lemma 7, and let $B_i = A_i + p$. Note that $B_i \in \{0,1\}$ and $Pr[B_i = 1] = p$. Let $B = \sum_{i=1}^{N} B_i$. Then, for all $d > 0$, it holds*

$$Pr[B > (p + d)N] < e^{-2 \cdot d^2 \cdot N}. \tag{52}$$

Proof of Lemma 7: By definition, $B = A + N \cdot p$. The proof is completed by putting $a = d \cdot N$ into the relation in Theorem 5. □

We will apply Chernov Bound arguments in the following modified scenario.

Lemma 8. *Let $C_1, \cdots, C_N$ denote a collection of (not necessarily independent) random $\{0,1\}$-variables fulfilling $Pr[C_i = 1] = p_i < p$ for all i, $1 \leq i \leq N$, and some p, $0 < p < 1$. Let $C = \sum_{i=1}^{N} C_i$.*

We suppose that, for $i > 1$, the probabilities p_i depend deterministically on (and can be computed from) the outcomes of the experiments $E_1, \cdots, E_{i-1}$ behind $C_1, \cdots, C_{i-1}$.

Then, for all $d > 0$, it holds

$$Pr[C > (p+d)N] < e^{-2 \cdot d^2 \cdot N}.$$

At several places we will take $d = \sqrt{D/(2N)}$ and obtain

$$Pr[C > (p+d)N] = Pr\left[C > pN + \sqrt{\frac{D \cdot N}{2}}\right] < e^{-D}. \tag{53}$$

Proof of Lemma 8: We construct a collection of mutually independent binary random variables $B_1, \cdots, B_N$ satisfying

- $C_i = 1$ implies $B_i = 1$,
- $Pr[B_i = 1] = p$

for all i, $1 \leq i \leq N$.

This proves our Lemma 8, as $\sum_{i=1}^{N} C_i \leq \sum_{i=1}^{N} B_i$ with probability one, and as Lemma 7 can be applied to $B = \sum_{i=1}^{N} B_i$.

The experiments $\tilde{E}_i$ behind B_i are for all i, $1 \leq i \leq N$, defined as follows:

- Compute p_i from the outcomes of the experiments $E_1, \cdots, E_{i-1}$.
- Perform E_i and output one (i.e., $B_i = 1$) if E_i is successful (i.e., if $C_i = 1$).
- If E_i is not successful (i.e., $C_i = 0$), then perform a completely independent experiment E_i' with success probability $q_i = \frac{p - p_i}{1 - p_i}$ and output one (i.e., $B_i = 1$) if E_i' is successful.

Note that $Pr[B_i = 1]$ equals

$$Pr[B_i = 1 | C_i = 1] \cdot Pr[C_i = 1] + Pr[B_i = 1 | C_i = 0] \cdot Pr[C_i = 0]$$

$$= 1 \cdot p_i + q_i \cdot (1 - p_i) = p.$$

□