Pencil: A Domain-Extended PRF with Full *n*-bit Security for Strengthening GCM and More

Ritam Bhaumik[©] Jean Paul Degabriele[®]

TII, Abu Dhabi, UAE bhuamik.ritam@gmail.com jeanpaul.degabriele@tii.ae

Abstract

We consider the problem of constructing efficient pseudorandom functions with Beyond-Birthday-Bound (BBB) security from blockciphers. More specifically, we are interested in variable-output-length pseudorandom functions (PRF) whose domain is twice that of the underlying blockcipher. We present two such constructions, Pencil and #Pencil, which provide weak PRF and full PRF security, respectively, where both achieve full *n*-bit security. While several recent works have focused on constructing BBB PRFs from blockciphers, much less attention has been given to weak PRF constructions which can potentially be constructed more efficiently and still serve as a useful primitive. Another understudied problem in this domain, is that of extending the domain of a BBB PRF, which turns out to be rather challenging. Besides being of theoretical interest in itself, this is also a very practical problem. Often, the input to the BBB PRF is a nonce, but random nonces are much easier to handle in practice as they do not require maintaining state—which can be very cumbersome in distributed systems and encrypted cloud storage. Accordingly, in order to maintain a BBB security bound, one requires random nonces of size between 1.5n and 2n bits long and corresponding BBB (weak) PRF constructions that admit matching input sizes. NIST has recently announced a pre-draft call for comments to standardise AEAD schemes that can encrypt larger amounts of data and admit larger nonces. The call lists two approaches. The first is to define an analogue of GCM using a 256-bit blockcipher, and the second is based on a recent proposal by Gueron, to extend GCM with a key derivation function (KDF) called DNDK to increase its security. In essence, DNDK is a BBB-secure expanding weak pseudorandom function with a domain size of 192 bits that is realised from AES. Our work makes relevant contributions to this domain in two important ways. Firstly, an immediate consequence of our work is that one can construct a GCM analogue with BBB security from *#Pencil*, without resorting to a 256-bit blockcipher. Our second contribution is that #Pencil can be used as a KDF in combination with GCM in an analogous manner to DNDK-GCM. However, #Pencil being a full PRF as opposed to DNDK which is only a weak PRF, allows one to prove the KDF-GCM composition secure as an AEAD scheme. Finally, when contrasting Pencil and DNDK as weak PRFs with comparable parameters, our construction requires only half the blockcipher calls.

Contents

1	Introduction	3
	1.1 Contribution	4
2	Preliminaries	6
	2.1 Distinguishing Advantage	6
	2.2 Weak Pseudorandom Functions	7
	2.3 Authenticated Encryption with Associated Data (AEAD)	7
	2.4 H-Coefficient Technique	9
	2.5 Mirror Theory	9
3	Pencil: An Optimally Secure Weak PRF	11
	3.1 Towards designing a weak PRF	11
	3.2 Formal Description	12
	3.3 Main Security Result	13
	3.4 Ideal World Sampling (Proof of Lemma 2)	14
	3.5 Bad Probability Calculations (Proof of Lemma 3)	15
4	Building a strong DDE from Doneil	17
4	A 1 Security Result	18
	4.1 Decurity result	18
	4.3 Proof of Lemma 11	10
		10
5	Pencil-based Key Derivation for GCM	22
	5.1 The CAU mode	23
	5.2 The new key-derivation proposal using $\sharp Pencil$	23
\mathbf{A}	Deferred Proofs of Lemmas from Sec. 3	30
	A.1 Proof of Lemma 1	30
	A.2 Proof of Lemma 4	30
	A.3 Proof of Lemma 5	31
	A.4 Proof of Lemma 6	32
	A.5 Proof of Lemma 7	32
	A.6 Proof of Lemma 8	33
в	Deferred Proofs of Lemmas from Sec. 4	34
	B.1 Proof of Lemma 9	34
	B.2 Proof of Lemma 12	36
	B.3 Proof of Lemma 13	37
	B.4 Proof of Lemma 14	37
	B.5 Proof of Lemma 15	39
	B.6 Proof of Lemma 16	41
	B.7 Proof of Lemma 17	41
	B.8 Proof of Lemma 18	42
	B.9 Proof of Lemma 19	42

1 Introduction

Pseudorandom functions (PRFs) have a rich history dating back to the seminal work of Goldreich, Goldwasser, and Micali in 1984 [GGM84]. They are a fundamental concept in cryptography spanning applications in all of its subfields and even permeating to other areas of computer science such as complexity theory, learning theory, and probabilistic data structures [BR17]. In the field of symmetric cryptography, they are arguably the most versatile cryptographic primitive. Yet, somewhat ironically, we are unable to construct them directly via the well-established iterative symmetric design techniques that have stood the test of time. We are very good at building pseudorandom permutations (PRPs) from scratch, like AES [AES01], but not pseudorandom functions. This is mainly due to the fact that pseudorandom permutations compose to give stronger pseudorandom permutations, whereas the converse is true for pseudorandom functions. Consequently, while symmetric constructions such as counter mode and Wegman-Carter MACs typically employ a blockcipher, they would benefit from better security if they were to be instantiated with a non-invertible pseudorandom function instead. This was already observed in 1998 by Bellare, Krovetz, and Rogaway in their paper titled "Luby-Rackoff Backwards" initiating the study of how to construct pseudorandom functions from pseudorandom permutations [BKR98].

In today's applications, the amount of data has grown so much that the birthday-bound security guaranteed by traditional schemes, like AES-GCM, no longer suffices. As a result, the Luby-Rackoff backwards problem has received renewed attention with several works revisiting the security of the sum of permutations [DHT17, GBJ⁺23], the truncated permutation construction [CLL19, GM22], the Encrypted Davies-Meyer (EDM) construction and its dual (EDMD) [CS16, MN17], and the newly introduced summationtruncation hybrid [GM20]. These PRF constructions vary in their output sizes, but their input size is always roughly equal to the block size of the underlying pseudorandom permutation. The summationtruncation hybrid yields the largest output size for the cost of evaluating two pseudorandom permutations, but the XORP construction can yield ℓ -block outputs at the cost of ℓ + 1 pseudorandom permutation evaluations [Iwa06]. In addition, in 2016, XORP and its extension CENC have been shown to achieve optimal beyond-birthday-bound security [IMV16] making them the most favourable constructions for many practical applications.

While the problem of building BBB-secure PRFs from PRPs with longer outputs has been addressed satisfactorily, the problem of building BBB-secure PRFs with larger domains has not. The latter, besides being in itself a fundamental problem of theoretical interest, is also highly relevant to cryptographic practice. In fact, the restricted input size of most of the existing BBB PRF constructions, including XORP and CENC, is a significant limitation for a number of practical applications. In particular, when the input to the PRF is a randomly sampled value, even if the PRF is BBB-secure the overall security of the scheme will still incur a birthday-bound term due to the possibility of collisions in the input. However, many practical applications require cryptographic schemes that can admit a randomly-generated nonce, as maintaining state is costly, cumbersome, or even unsafe in settings such as distributed systems and encrypted cloud storage [BGK99, GL17, KCC⁺23, Gue24a]. Accordingly, nonces must be larger than the block size for a BBB-secure stateless scheme.

The practical need for BBB PRFs with larger domains was already pointed out by Bellare, Goldreich, and Krawczyk, who in 1999 showed that for a random function $f : \{0,1\}^n \to \{0,1\}^n$ the construction $f(r_1) \oplus \cdots \oplus f(r_t)$ is pseudorandom, up to a security bound of $\mathcal{O}(t!) \cdot q^2/2^{nt}$ for $q < 2^n/\mathcal{O}(t)$, when r_1, \ldots, r_t are random but distinct values. Note that this result is far from trivial and the restriction on the inputs being random is necessary for the construction to be pseudorandom. Twenty-five years later, this remains the best BBB-secure construction for extending the domain of a PRF over random inputs and is in fact used in the Double Nonce Derive Key (DNDK) construction recently proposed by Gueron [Gue24b, Gue24a]. DNDK is a key derivation function specifically designed to be used in combination with GCM to address two of its limitations by deriving a fresh encryption key for every message. Namely, DNDK-GCM aims

$Pencil[\mathbf{U}, E]_K(\mathbf{R}, h_{\mathrm{out}})$	$Sharpen[E]_{ ilde{K}}(\mathbf{N})$
$1: \tilde{\mathbf{X}} \leftarrow \mathbf{U} \cdot \mathbf{R}$	$1: (K_1, K_2, K_3) \leftarrow \tilde{K}$
2: $(\tilde{X}_0, \dots, \tilde{X}_\ell) \leftarrow \tilde{\mathbf{X}}^T$	$2: (N_1, N_2) \leftarrow \mathbf{N}^{T}$
3: for $j = 0$ to ℓ do	$3: J \leftarrow E_{K_1}(N_2)$
$4: \qquad X_j \leftarrow \tilde{X}_j \ \langle h_{\text{out}} \rangle_\lambda$	$4: W_1 \leftarrow N_1 \oplus J$
$5: Y_j \leftarrow E_K(X_j)$	$5: W_2 \leftarrow N_1 \oplus 2 \cdot J$
6: if $j \ge 1$ then	$6: R_1 \leftarrow msb_{n-\lambda}(E_{K_2}(W_1))$
$7: \qquad Z_j \leftarrow Y_0 \oplus Y_j$	7: $R_2 \leftarrow msb_{n-\lambda}(E_{K_3}(W_2))$
8: $\mathbf{Z} \leftarrow (Z_1, \ldots, Z_\ell)^T$	8: $\mathbf{R} \leftarrow (R_1, R_2)^{T}$
9: return Z	9: return R
$\sharp Pencil[\mathbf{U},E]_{ ilde{K}}(\mathbf{U})$	$\mathbf{N}, h_{ ext{out}})$
$1: (K_1, K_2, K_3,$	$K_4) \leftarrow \tilde{K}$
$2: \mathbf{R} \leftarrow Sharper$	$[E]_{(K_1,K_2,K_3)}(\mathbf{N})$
3 : return Penc	$il[\mathbf{U}, E]_{K_4}(\mathbf{R}, h_{\mathrm{out}})$

Figure 1: Algorithms for $\mathsf{Pencil}[\mathbf{U}, E]$, $\mathsf{Sharpen}[E]$, and $\sharp\mathsf{Pencil}[\mathbf{U}, E]$.

to attain better quantitative security than GCM and admits a 192-bit random nonce¹ which allows it to encrypt a higher amount of data in a stateless setting, and it additionally derives a secondary tag for key-commitment security. In essence, DNDK is itself an expanding weak PRF consisting of two instances of the XORP [Iwa06] construction evaluated over independently sampled random inputs and combined in an XOR fashion using the result of Bellare, Goldreich, and Krawczyk [BGK99]. Combining the results of Iwata, Mennink, and Vizar [IMV16] and Bellare, Goldreich, and Krawczyk [BGK99] it follows that DNDK achieves $\mathcal{O}(q/2^n)$ security as a weak PRF. In terms of efficiency, DNDK requires $2(\ell + 1)$ AES calls to produce ℓ blocks of output, where the AES calls are parallelisable. DNDK-GCM is reportedly being used at Meta, is included in their high-performance cryptographic library Haberdashery, and is currently being proposed for standardisation as an RFC [Gue24a]. Moreover, besides its effort to standardise an Accordion mode, NIST has separately announced a pre-draft call for comments where it recognizes the need to standardize efficient AEAD schemes which can support larger nonces and the ability to encrypt larger amounts of data under the same key [Nat25]. The NIST call lists two possible approaches to address this, the first is to define an analogue of GCM using a 256-bit blockcipher, and the second is to augment GCM with a key derivation function as done in DNDK-GCM.

1.1 Contribution

Our work is primarily inspired and motivated by the use case of DNDK as a way to strengthen GCM and obtain stateless AEAD constructions with BBB security from blockciphers. However, from a more theoretical perspective, it highlights a rather understudied problem: that of constructing (weak) pseudorandom functions from blockciphers with extended domains and BBB security. We think that this problem is of independent interest, as it is likely to have application to other symmetric BBB constructions such as AEAD and Accordion modes. Our effort is directed towards improving over DNDK in two distinct ways. We first consider the question of efficiency, namely whether it is possible to improve over DNDK in terms of the number of its constituent blockcipher calls while retaining the same level of security. The second

¹Technically GCM admits nonces larger than 96 bits, but they are hashed internally to a 96-bit value thereby resulting in the same collision probability as a 96-bit nonce.

issue we address is that DNDK-GCM lacks a security proof² as a composite AEAD scheme and, in fact, it seems rather unlikely that such a result is possible. This is due to the fact that DNDK is only secure as a weak PRF. However, in the AEAD security game, the adversary can make decryption queries for any nonce of his choice and this nonce is what is input to DNDK. Thus during decryption DNDK can be fed non-random inputs—which falls outside the weak PRF security model. In addressing these two limitations of DNDK, we make the following contributions.

A New Domain-Extended BBB Weak PRF. Our first contribution is Pencil (Fig. 1, top left, and Fig. 5, left), a blockcipher-based variable-output-length weak PRF construction on double-block inputs. Compared to DNDK, Pencil requires about half the number of blockcipher calls, while retaining the same optimal (full *n*-bit) security bound. Pencil is inspired by CENC in that it follows a two-level structure where the output is evaluated in chunks of w blocks. However, as we discuss in detail later, there are some important challenges to overcome in order to adapt XORP to take two random nonces instead of one. Specifically, we compose the general structure of XORP with a matrix over a binary field where the matrix is required to satisfy a condition we call local non-degeneracy. Note that this matrix results in minimal overhead as it only adds $(\ell + 1)$ binary-field multiplications by 2, which can be realised via shift and XOR operations. Using mirror theory we prove Pencil secure as a weak PRF up to $\mathcal{O}(\ell^2 q/2^{n-\lambda})$ where ℓ is the number of *n*-bit blocks in each chunk and λ is the length of the output handle in bits (so that each random IV is of length $2n - 2\lambda$ bits and can be re-used over at most 2^{λ} chunks). While Pencil, like DNDK. cannot be proven secure when composed with GCM we believe it is of independent interest. For instance, it readily yields a *stateless* BBB IND-CPA encryption scheme requiring roughly a single blockipher call per message block, when employed as a stream cipher. To the best of our knowledge, no other construction achieves this from a blockcipher.

Domain-Extended BBB Strong PRF. Next we consider the problem of constructing a domainextended BBB full-fledged PRF. We accomplish this by augmenting Pencil with a 2n-to-2n preprocessing stage called Sharpen (Fig. 1, top right, and Fig. 5, right) to yield a strong PRF #Pencil (Fig. 1, bottom). As a domain-extended variable-output-length PRF #Pencil requires only three additional independentlykeyed blockcipher calls more than Pencil, and attains a PRF security bound of $\mathcal{O}(\ell^2 q/2^{n-\lambda} + n\ell^2 q/2^n)$. We describe Sharpen and prove the PRF security of \sharp Pencil in Section 4. Besides being amenable as a key derivation function in combination with GCM and other AEAD schemes, #Pencil has several other applications which we briefly mention here but do not pursue further in this paper. The first immediate application is to combine #Pencil with an Almost-XOR-Universal hash function to yield a BBB Carter-Wegman MAC that admits nonces of size 2n, and can thus be operated in a stateless manner without degrading security. Better still, one can use #Pencil as a stream cipher and combine it with an Almost-XOR-Universal hash function to obtain a blockcipher-based BBB AEAD scheme, analogous to GCM, with 2n-bit nonces. In particular, this presents a third avenue for addressing NIST's pre-draft call [Nat25]; namely a GCM analogue with BBB security that does not require a 256-bit blockcipher and can be readily instantiated with a 128-bit blockcipher like AES. Note that while there exist other blockcipher-based BBB AEAD designs, such as SCM [CLLL21], OCB+ [BBN22], and XOCB [BHI+23], such constructions do not admit 2n-bit nonces and thus cannot be operated in a stateless fashion without degrading to birthdaybound security—which is the scenario under consideration by NIST.

Composition with CAU/GCM. We conclude by showing that *#Pencil* can be combined with the CAU AEAD scheme (a generalisation of GCM [BT16]) to yield a composite AEAD scheme Pencil-DK-CAU

²Confirmed via private communication with Shay Gueron.

analogous to DNDK-GCM. In contrast to DNDK-GCM, which lacks a security proof as an AEAD scheme, we show that Pencil-DK-CAU is provably secure as an AEAD scheme with a significantly better security bound than plain CAU/GCM. To prove its security we make use of the multi-user security analysis of CAU/GCM by Hoang, Tessaro, and Thiruvengadam [HTT18]. In Pencil-DK-CAU, the key derivation adds only 7 additional blockcipher calls per encryption while attaining a similar bound to that claimed by Gueron for DNDK-GCM [Gue24a]. In contrast to DNDK-GCM which fixes the GCM nonce to a constant and only derives a new GCM key per encryption, we derive a random nonce-key pair for each message. However, DNDK-GCM also claims to provide key-committing security, albeit without a mathematical proof, whereas we make no such security claim for Pencil-DK-CAU. We leave the problem of extending Pencil-DK-CAU to be key-committing (if at all possible) as an open problem for future work.

2 Preliminaries

For $m \leq n$, we will write [m..n] to denote the range $\{m, \ldots, n\}$. We will use the Pochhammer falling factorial power notation

$$(n)_m := n(n-1) \cdot \ldots \cdot (n-m+1).$$

 S_n will denote the symmetric group over *n* elements. For a finite set S we'll write $R \leftarrow S$ to denote *R* being uniformly sampled from S.

For an $x \leq 2^d$, $\langle x \rangle_d$ will denote the *d*-bit encoding of *x*. x || y will denote the concatenation of two bit-strings *x* and *y*. $|x|_b$ will denote the length of *x* in bits, $|x|_B$ will denote the length of *x* in bytes, and $|x|_n$ will denote its length in *n*-bit blocks. $\mathsf{lsb}_d(x)$ and $\mathsf{msb}_d(x)$ will respectively denote the right-most and left-most *d*-bit substring of *x*.

Bold face capital letters will usually denote vectors or matrices over $\mathbb{GF}(2^d)$ for some bit-length d. Unless there is scope for confusion, we'll not make a distinction between a field element $x \in \mathbb{GF}(2^d)$ and its d-bit encoding $\langle x \rangle_d \in \{0,1\}^d$, and we'll treat these two sets interchangeably. Vectors will conventionally be treated as column vectors, with \mathbf{V}^{\intercal} denoting the dual row vector obtained by transposing a column vector \mathbf{V} .

Markov's Inequality. For a non-negative random variable X and some a > 0, Markov's Inequality states that

$$\Pr[X \ge a] \le \frac{\mathbb{E}(X)}{a}$$

2.1 Distinguishing Advantage

For any game G defined with respect to some primitive F and any adversary \mathcal{A} we denote the adversary's corresponding advantage by $\mathbf{Adv}_{F}^{\mathsf{G}}(\mathcal{A})$. We use $\mathcal{A}^{\mathsf{G}} \Rightarrow b'$ to denote the event where the adversary interacts with game G and returns the bit b' upon terminating the game. When considering the distinguishing advantage between two primitives F and F^* with respect to a security game G, we denote this by $\mathbf{Adv}_{F,F^*}^{\mathsf{G}}(\mathcal{A})$. When the security game is simply the adversary's ability to distinguish between access to two oracles \mathcal{O}_0 and \mathcal{O}_1 , we use $\mathcal{A}^{\mathcal{O}_b} \Rightarrow b'$ to denote the event that the adversary outputs bit b' after interacting with oracle \mathcal{O}_b and define the adversary's advantage as follows:

$$\mathbf{Adv}^{\mathcal{O}_1,\mathcal{O}_0}(\mathcal{A}) := \Big| \Pr[\mathcal{A}^{\mathcal{O}_1} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{O}_0} \Rightarrow 1] \Big|.$$
(1)

Typically, \mathcal{O}_0 represents an ideal primitive, while \mathcal{O}_1 represents either an actual construction or a mode of operation.

$\operatorname{Game} WPRF_F^\mathcal{A}$	$\mathrm{EVAL}(h_{\mathrm{in}},h_{\mathrm{out}})$
$K \leftarrow \mathcal{K}$	$\mathbf{if}h_{\mathrm{in}}\not\inIn$
$b \leftarrow \$ \{0,1\}$	$ln[h_{\mathrm{in}}] \gets \!\!\! \mathfrak{X}$
$In \leftarrow [], Out \leftarrow [,]$	$\mathbf{if} \ (In[h_{\mathrm{in}}],h_{\mathrm{out}}) \not\in Out$
$b' \leftarrow \mathcal{A}^{\mathrm{Eval}(\cdot, \cdot)}$	$\mathbf{if} \ b = 0 \ \mathbf{then}$
return $b = b'$	$Out[ln[h_{\mathrm{in}}],h_{\mathrm{out}}] \leftarrow \mathfrak{Y}$
	else
	$Out[ln[h_{\mathrm{in}}], h_{\mathrm{out}}] \leftarrow F_K(ln[h_{\mathrm{in}}], h_{\mathrm{out}})$
	$\mathbf{return}~(In[h_{\mathrm{in}}],Out[In[h_{\mathrm{in}}],h_{\mathrm{out}}])$

Figure 2: The game used to define wPRF security.

2.2 Weak Pseudorandom Functions

A function family is a set of functions defined over a given domain and range. In practice, it is typically realised as an efficient algorithm F with an associated key space \mathcal{K} such that sampling a random key Kfrom \mathcal{K} is equivalent to sampling a random function $\mathsf{F}(K, \cdot)$ from the function family. Accordingly, we will use F to denote both the function family and the algorithm for evaluating the function family.

A weak pseudorandom function is a function family that, when evaluated over randomly-sampled inputs, is computationally indistinguishable from a random function over the same domain and range. This is formally defined through the WPRF game described in Figure 2. Our game may appear more elaborate than the standard weak PRF definition but this is simply because we endow the function family with a slightly more elaborate syntax. We are mainly interested in function families with large expansion. However, the output for a given input does not need to be evaluated all at once, but can instead be generated on demand. For this reason, we define F to take three strings as input: a key $K \in \mathcal{K}$, an input $X \in \mathcal{X}$, and an output handle $h_{\text{out}} \in \mathcal{H}_O$ specifying which portion of the output is to be returned. In the WPRF game, the adversary interacts with an evaluation oracle EVAL that it can query on an input handle h_{in} and an output handle h_{out} . The input handle allows the adversary to repeat queries on the same input (with a different output handle) without giving it the ability to choose the input. In each evaluation query the input value X is returned to the adversary. The corresponding weak PRF advantage is defined below.

Definition 1 (wPRFAdvantage). Let $F : \mathcal{K} \times \mathcal{X} \times \mathcal{H}_O \to \mathcal{Y}$ be a function family. Then for any adversary \mathcal{A} its wPRF advantage is defined as:

$$\mathbf{Adv}_{\mathsf{F}}^{\mathsf{wPRF}}(\mathcal{A}) := \left| \Pr[\mathcal{A}^{\mathsf{WPRF}} \Rightarrow 1 \,|\, b = 1] - \Pr[\mathcal{A}^{\mathsf{WPRF}} \Rightarrow 1 \,|\, b = 0] \right|.$$

2.3 Authenticated Encryption with Associated Data (AEAD)

AEAD syntax. A nonce-based AEAD scheme $\Pi = (\Pi.Enc, \Pi.Dec)$ consists of the following pair of algorithms:

• A deterministic encryption algorithm Π .Enc : $\mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{M} \to \mathcal{C}$ takes as input a secret key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, associated data $AD \in \mathcal{AD}$, and a message $M \in \mathcal{M}$ and returns a ciphertext $C \in \mathcal{C}$. We require Π .Enc to have constant expansion, i.e. for any $(K, N, AD, M) \in (\mathcal{K}, \mathcal{N}, \mathcal{AD}, \mathcal{M})$, the expansion $\tau = |\Pi$.Enc $(K, N, AD, M)|_b - |M|_b$ is constant.

Game $AEAD^{\mathcal{A}}_{\varPi}$	$\operatorname{Enc}(N, AD, M)$	$\operatorname{Dec}(N, AD, C)$
$K \leftarrow \mathfrak{K}$	if $b = 0$	if $b = 0$
$b \gets \$ \{0,1\}$	$C \gets \Pi.Enc(K,N,AD,M)$	$M \gets \Pi.Dec(K,N,AD,C)$
$b' \leftarrow \mathcal{A}^{\mathrm{Enc}(\cdot,\cdot,\cdot),\mathrm{Dec}(\cdot,\cdot,\cdot)}$	else	else
$\mathbf{return} \ b = b'$	$C \leftarrow \$ \{0,1\}^{ M _b + \tau}$	$M \leftarrow \bot$
	return C	$\mathbf{return} \ M$

Figure 3: The game used to define AEAD security.

• A deterministic decryption algorithm Π . Dec : $\mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{C} \to \mathcal{M} \cup \{\bot\}$ takes as input a secret key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, associated data $AD \in \mathcal{AD}$, and a ciphertext $C \in \mathcal{C}$ and returns either a message $M \in \mathcal{M}$ or the symbol \bot to indicate an invalid ciphertext.

We refer to the associated sets \mathcal{K} , \mathcal{N} , \mathcal{AD} , \mathcal{M} , and \mathcal{C} as the key space, the nonce space, the associateddata space, the message or plaintext space and the ciphertext space, respectively. Every nonce-based AEAD should satisfy correctness and tidiness. Correctness requires that for all $(K, N, AD, M) \in (\mathcal{K}, \mathcal{N}, \mathcal{AD}, \mathcal{M})$, it must hold that if $C \leftarrow \Pi.\mathsf{Enc}(K, N, AD, M)$ then $M \leftarrow \Pi.\mathsf{Dec}(K, N, AD, C)$, and tidiness requires that for all $(K, N, AD, C) \in (\mathcal{K}, \mathcal{N}, \mathcal{AD}, \mathcal{C})$, if $\bot \neq M \leftarrow \Pi.\mathsf{Dec}(K, N, AD, C)$ then $C \leftarrow \Pi.\mathsf{Enc}(K, N, AD, M)$.

AEAD security. AEAD security is defined via the game described in Fig. 3. The adversary \mathcal{A} is given access to an encryption oracle $\mathsf{Enc}(N, AD, M)$ and a decryption oracle $\mathsf{Dec}(N, AD, C)$. Such an adversary is considered valid if it never makes a decryption query $\mathsf{Dec}(N, AD, C)$ with C being the output of a previous encryption query $\mathsf{Enc}(N, AD, M)$. Moreover an adversary is said to be nonce-respecting if it never repeats a nonce N across encryption queries. The AEAD advantage of an adversary is defined below.

Definition 2 (AEAD advantage). Let $\Pi = (\Pi. \text{Enc}, \Pi. \text{Dec})$ be a nonce-based AEAD scheme with expansion τ , defined over $(\mathcal{K}, \mathcal{N}, \mathcal{AD}, \mathcal{M}, \mathcal{C})$. For any valid nonce-respecting adversary \mathcal{A} , we define its AEAD advantage with respect to Π to be:

$$\mathbf{Adv}_{II}^{\mathsf{AEAD}}(\mathcal{A}) := \left| \Pr[\mathcal{A}^{\mathsf{AEAD}} \Rightarrow 1 \,|\, b = 1] - \Pr[\mathcal{A}^{\mathsf{AEAD}} \Rightarrow 1 \,|\, b = 0] \right|.$$

where AEAD is the game defined in Fig. 3.

Multi-User AEAD security (mu-AEAD). Multi-user AEAD security is an extension of AEAD security where the adversary can interact with multiple independently keyed instances of an AEAD scheme, where, depending on the value of the bit b, either all oracles follow the scheme or they all behave in an ideal way. The corresponding security game is described in Fig. 4 and the corresponding advantage is defined analogously to Def. 2.

Almost XOR Universal (AXU) Hash. Consider a keyed hash function $\mathcal{H} : \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ for some positive integer n. Then \mathcal{H} is said to be *c*-almost-XOR-universal if for all bit string pairs (X_1, X_2) , such that $X_1 \neq X_2$, and all $Y \in \{0,1\}^n$ it holds that:

$$\Pr_{\mathrm{HK} \leftarrow \$\{0,1\}^n} [\mathcal{H}_{\mathrm{HK}}(X_1) \oplus \mathcal{H}_{\mathrm{HK}}(X_2) = Y] \le \frac{c \cdot \max(|X_1|_n, |X_2|_n)}{2^n}.$$

Game	$\operatorname{Enc}(i, N, AD, M)$	Dec(i, N, AD, C)
$\underline{mu-AEAD}_{\Pi}$	$\mathbf{if} \ b = 0$	if $b = 0$
$K_1,\ldots,K_u \leftarrow \mathcal{K}$	$C \leftarrow \Pi.Enc(K_i, N, AD, M)$	$M \leftarrow \Pi.Dec(K_i, N, AD, C)$
$b \gets \{0,1\}$	else	else
$b' \leftarrow \mathcal{A}^{\mathrm{Enc}(\cdot,\cdot,\cdot),\mathrm{Dec}(\cdot,\cdot,\cdot)}$	$C \gets \$ \ \{0,1\}^{ M _b + \tau}$	$M \leftarrow \bot$
$\mathbf{return} b = b'$	return C	$\mathbf{return} \ M$

Figure 4: The game used to define mu-AEAD security.

2.4 H-Coefficient Technique

The H-coefficient technique is a proof technique devised by Patarin [Pat09] and popularised by the exposition due to Chen and Steinberger [CS14]. We outline the main idea below; for a more detailed exposition, the reader is referred to [CS14, JN22].

A distinguisher \mathcal{A} interacts with one of two oracles, possibly providing an interface to multiple functionalities— \mathcal{O}_1 in the real world and \mathcal{O}_0 in the ideal world. A record of its interaction with oracle \mathcal{O} is collected in a transcript Trs ($\mathcal{A}^{\mathcal{O}}$). The transcript may optionally include additional information that is revealed to the adversary at the end of the interactive phase. We assume, without loss of generality, that the oracles sample all their random coins, typically a key or an ideal primitive, before the experiment starts. A transcript tr is called *attainable* if \mathcal{A} can observe tr with non-zero probability in the ideal world, i.e., if $\Pr[\text{Trs } (\mathcal{A}^{\mathcal{O}_0}) = \text{tr}] > 0$. The Fundamental Theorem of the H-coefficient technique states the following:

Theorem 1 (H-Coefficient Technique [Pat09]). Suppose we can partition the set \mathcal{T} of all attainable transcripts as $\mathcal{T} = \mathcal{T}_{\mathsf{bad}} \sqcup \mathcal{T}_{\mathsf{good}}$, and find $\epsilon_1, \epsilon_2 \geq 0$ such that

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right)\in\mathcal{T}_{\mathsf{bad}}\right]\leq\epsilon_{1},\tag{2}$$

and for any $tr \in \mathcal{T}_{good}$,

$$\frac{\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = tr\right]}{\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = tr\right]} \ge 1 - \epsilon_{2}.$$
(3)

Then the distinguishing advantage of \mathcal{A} obeys the bound

$$\mathbf{Adv}^{\mathcal{O}_0,\mathcal{O}_1}(\mathcal{A}) \le \epsilon_1 + \epsilon_2. \tag{4}$$

2.5 Mirror Theory

The mirror theory of Patarin [Pat06, Pat10b, Pat03] gives a lower bound on the number of solutions to a systems of bivariate equations. Consider a system of m bivariate equations over $\mathbb{GF}(2^n)$ on r variables (Y_1, \ldots, Y_r) , that can be written as

$$Y_i \oplus Y_j = Z_{i,j},\tag{5}$$

for some $i \neq j$. Informally, mirror theory says the following: if $Z_{i,j} \neq 0$ in all of the equations and the graph corresponding to these equations (where the variables are nodes and the equations are edges) does not have a cycle or a 0-sum path, and provided that the size ξ_{max} of the largest component obeys certain bounds, the number of solutions to this system of equations where $Y_i \neq Y_j$ for all i, j is at least

$$\frac{2^n)_r}{2^{nm}}.\tag{6}$$

The intuition behind this lower bound is that the numerator in the above expression is the total number of solutions satisfying just the distinctness constraint, and any randomly chosen solution has a probability of around $1/2^{nm}$ of satisfying all m bivariate equations.

Mirror theory has a somewhat contentious history. It was originally proposed by Patarin and then refined in a serious of works [Pat08, Pat10a, CLP15]. After that, several works have used it in their security analysis to obtain better security bounds [IMV16, MN17, ZHY18, BBN22, BCF⁺24, CLL24]. At the same time, consensus was growing among a number of cryptographers that the original proof of mirror theory contained a number of gaps that could not be readily justified. However, these gaps in the proof do not seem to have been documented anywhere. Subsequently, Dutta et al. [DNS22] provided a more complete proof of the bound for $\xi_{\text{max}} = 2$, and Cogliati et al. [CDN⁺23] followed it up with a proof for a wider range of ξ_{max} . Following these two works, the technique has gained wider acceptance by the community. In this work, we use one of the results from [CDN⁺23], which we formally restate below as Theorem 2.

Formal Description. We represent the variables as a vector $\mathbf{Y} := (Y_1, \ldots, Y_r)^{\mathsf{T}}$, the differences (after re-labelling them in some serial order) as a vector $\mathbf{Z} := (Z_1, \ldots, Z_m)^{\mathsf{T}}$, and the coefficients as a matrix \mathbf{A} whose (i, j)-th entry is denoted by A_{ij} , so that the system of equations in Eqn. (5) can be concisely described as

$$\mathbf{A}_{m \times r} \cdot \mathbf{Y} = \mathbf{Z}.\tag{7}$$

We write $\Phi := \Phi[\mathbf{A}, \mathbf{Z}]$ to denote the system of equations described by Eqn (7), parametrised by \mathbf{A} and \mathbf{Z} . We call $\Phi[\mathbf{A}, \mathbf{Z}]$ a *bivariate mirror system* if \mathbf{A} has the special form where each row of \mathbf{A} has *exactly* two 1's and (r-2) 0's. A solution to Φ which satisfies the constraint that $Y_i \neq Y_j$ for all $i, j \in [1..r]$ with $i \neq j$ is called a *mirror solution*; let $\Gamma(\Phi)$ denote the set of all mirror solutions to the system Φ .

We associate a weighted undirected graph $\mathcal{G} := \mathcal{G}(\Phi)$ with a bivariate mirror system $\Phi = \Phi[\mathbf{A}_{m \times r}, \mathbf{Z}]$ as follows: \mathcal{G} has r vertices labelled Y_1, \ldots, Y_r , and m edges with weights Z_1, \ldots, Z_m , subject to the following rule: there is an edge between Y_i and Y_j with weight Z_t if and only if $A_{ti} = A_{tj} = 1$. We call $\Phi[\mathbf{A}, \mathbf{Z}]$ redundancy-free if $m \leq r - 1$ and \mathbf{A} is of full row-rank; in which case it is easy to see that Φ is redundancy-free if and only if $\mathcal{G}(\Phi)$ is acyclic. Assuming that $\Phi[\mathbf{A}, \mathbf{Z}]$ is redundancy-free and following graph theoretic terminology, we call \mathcal{G} a forest and each of its connected components a tree. Then a basic result from graph theory tells us that \mathcal{G} has exactly c := r - m trees.

As observed in [CDN⁺23], we can assume without loss of generality that each tree in \mathcal{G} is in fact a *star*, meaning that all of its nodes except one are *leaf nodes* (of degree 1). We call the solitary non-leaf node the *center* of the star. The ξ variables involved in a particular star component can be reordered to begin with the center, so that the corresponding coefficient matrix becomes $(\mathbf{1}_{\xi-1}, \mathbf{I}_{\xi-1})$, where **1** denotes a vector of 1's, and **I** denotes the identity matrix. Then Φ can be decomposed into c systems Φ^1, \ldots, Φ^c , where for each $p \in [1..c]$, $\Phi^p := \Phi^p[\mathbf{A}^p := (\mathbf{1}_{\xi_p-1}, \mathbf{I}_{\xi_p-1}), \mathbf{Z}^p := (Z_1^p, \ldots, Z_{\xi_p}^p)^{\mathsf{T}}]$, with ξ_p denoting the size of the p-th component.

With the above setup in mind, we call Φ a *consistent mirror system* if for each $p \in [1..c]$, the *p*-th component satisfies the following conditions:

- $Z_i^p \neq 0$ for each $i \in [1..\xi_p]$;
- $Z_i^p \neq Z_j^p$ for each $i, j \in [1..\xi_p]$ with $i \neq j$.

 Φ being a consistent mirror system is a necessary and sufficient condition to ensure $|\Gamma(\Phi)| > 0$. We note that we define consistency only for redundancy-free mirror systems; this does not lead to loss of generality since for every mirror system Φ we can find a redundancy-free mirror system Φ' such that Φ and Φ' have an identical set of solutions. Moreover, it may be interesting to observe that the characterisation of a system of equations $\Phi[\mathbf{A}, \mathbf{Z}]$ as a bivariate mirror system or as redundancy-free depends solely on the coefficient matrix \mathbf{A} , while its consistency depends solely on the difference vector \mathbf{Z} . With these definitions laid out, we are now ready to restate the main mirror theory result [CDN+23, Theorem 1] which we will employ later in this paper.

Theorem 2 (Mirror Theorem [CDN⁺23]). Let Φ be a consistent mirror system of m equations in r variables, and let ξ_{\max} denote the size of the largest component in $\mathcal{G}(\Phi)$. Then, if either $m \leq 2^{n/2}$ holds, or ξ_{\max} satisfies the conditions $n\xi_{\max}^2 + \xi_{\max} \leq 2^{n/2}$ and $12m\xi_{\max} \leq 2^n$, it follows that

$$|\Gamma(\Phi)| \ge \frac{(2^n)_r}{2^{nm}}.\tag{8}$$

3 Pencil: An Optimally Secure Weak PRF

3.1 Towards designing a weak PRF

Before describing Pencil, we justify and motivate its design by first considering a natural attempt at constructing a weak PRF that accepts a 2-block random IV but that unfortunately does not work. We then explain why this approach fails and propose a fix to circumvent this problem.

First Approach. We wish to design a weak PRF mode F based on a block cipher E of width n bits which accepts a random nonce of length $2n - 2\lambda$ bits, and outputs a keystream of ℓn bits. A natural approach would be to mimic the CENC construction. That is, split the nonce in half as $R_1 || R_2$, and reserve the last λ bits of each call to E_K for domain separation (we assume $\lambda \ll n$). We then take each output block to be of the form $F_{i,j}(R_1, R_2) := E_K(R_1 || \langle i \rangle_{\lambda}) \oplus E_K(R_2 || \langle j \rangle_{\lambda})$ for some $i, j \in [0..2^{\lambda} - 1]$. Let $\mathcal{I} \subseteq [0..2^{\lambda} - 1]^2$ be the index set of size ℓ such that $F(R_1, R_2)$ is made up of the blocks $\{F_{i,j}(R_1, R_2) \mid (i, j) \in \mathcal{I}\}$ in some order.

Consider the bipartite graph \mathcal{G} where the vertex set is $\{1,2\} \times [0..2^{\lambda} - 1]$, and the edge set is $\{\{(1,i), (2,j)\} \mid (i,j) \in \mathcal{I}\}$, i.e., there is an edge between (1,i) and (2,j) if one of the output blocks is $F_{i,j}(R_1, R_2)$. However, we cannot allow a cycle in \mathcal{G} as it leads to a trivial distinguisher. More specifically, if $(i,j), (i,j'), (i',j'), (i',j) \in \mathcal{I}$ and $i \neq i, j \neq j$, meaning that (1,i), (2,j), (1,i'), (2,j') lie on a cycle in \mathcal{G} , then a distinguisher can test for the following condition: $F_{i,j}(R_1, R_2) \oplus F_{i,j'}(R_1, R_2) \oplus F_{i',j'}(R_1, R_2) \oplus F_{i',j}(R_1, R_2) \oplus F_{i',j'}(R_1, R_2) \oplus F_{i',j'}(R_1,$

Why this doesn't work. However, this approach doesn't work if we want BBB security from the weak PRF. This is because if at least one vertex (1, i) has two neighbours (2, j) and (2, j') in \mathcal{G} , then we have two output blocks $Z := F_{i,j}(R_1, R_2)$ and $Z' := F_{i,j'}(R_1, R_2)$. Then $Z \oplus Z' = E_K(R_2 ||\langle j \rangle_{\lambda}) \oplus E_K(R_2 ||\langle j' \rangle_{\lambda})$ is a function of R_2 , and any collision on R_2 (which should happen within less than $2^{n/2}$ nonces) leads to a collision in $Z \oplus Z'$, leading to a distinguishing attack.

Using a Linear Transformation. We observe that the above problem is caused by the fact that each E_K call is function of exactly one of R_1 and R_2 , so that a collision in either leads to a collision in the outputs of *all* calls involving it. We get around this by generating 2^{λ} independent linear combinations of R_1 and R_2 , to be used with the 2^{λ} domain separators. The idea is that if two of them are to collide simultaneously (which is needed for the above attack), it should have about the same probability as a collision over the whole $2n - 2\lambda$ bits.

One option could be to use the following inputs: $R_1 \|\langle 0 \rangle_{\lambda}$, $(R_1 \oplus R_2) \|\langle 1 \rangle_{\lambda}$, $(R_1 \oplus 2 \cdot R_2) \|\langle 2 \rangle_{\lambda}$, ..., $(R_1 \oplus 2^{2^{\lambda-1}-2} \cdot R_2) \|\langle 2^{\lambda-1}-1 \rangle_{\lambda}$ for domain separators beginning in 0, and $R_2 \|1\| \langle 0 \rangle_{\lambda-1}$, $(2 \cdot R_1 \oplus R_2) \|1\| \langle 1 \rangle_{\lambda-1}$,

..., $(2^{2^{\lambda-1}-1} \cdot R_1 \oplus R_2) \|1\| \langle 2^{\lambda-1} - 1 \rangle_{\lambda-1}$ for domain separators beginning in 1. This has the advantage that all the inputs can be computed using around 2^{λ} multiplications by 2, and no other field multiplications are needed.

Resistance to attack. For the above attack to work, we need to find a pair of nonces $R_1 || R_2$ and $R'_1 || R'_2$ and indices *i* and *j* such that the inputs to *i* for the two nonces collide with each other, and the inputs to *j* collide with each other. If $1 \le i, j < 2^{\lambda-1}$, this is equivalent to finding $R_1 || R_2$ and $R'_1 || R'_2$ such that

$$R_1 \oplus 2^{i-1} \cdot R_2 = R'_1 \oplus 2^{i-1} \cdot R'_2,$$

$$R_1 \oplus 2^{j-1} \cdot R_2 = R'_1 \oplus 2^{j-1} \cdot R'_2.$$

Together they imply that $(2^{i-1} \oplus 2^{j-1}) \cdot (R_2 \oplus R'_2) = 0$, from which we can see that $R_2 = R'_2$ and hence $R_1 = R'_1$. Thus, this needs a collision on the entire $(2n - 2\lambda)$ -bit nonce. A similar reasoning works if $i, j > 2^{\lambda-1}$.

For $i < 2^{\lambda-1}, j > 2^{\lambda-1}$, we need to find $R_1 || R_2$ and $R'_1 || R'_2$ such that

$$R_1 \oplus 2^{i-1} \cdot R_2 = R'_1 \oplus 2^{i-1} \cdot R'_2$$
$$2^{j'} \cdot R_1 \oplus R_2 = 2^{j'} \cdot R'_1 \oplus R'_2,$$

where $j' := j - 2^{\lambda-1}$ (i.e., $\langle j \rangle_a = 1 || \langle j' \rangle_{\lambda-1}$). These two equations together imply that $(2^{i-1+j'} \oplus 1) \cdot (R_2 \oplus R'_2) = 0$, so we again get $R_2 = R'_2$ and $R_1 = R'_1$. Finally, when $i \in \{0, 2^{\lambda-1}\}$ or $j \in \{0, 2^{\lambda-1}\}$, we directly have $R_1 = R'_1$ or $R_2 = R'_2$ as one of the

Finally, when $i \in \{0, 2^{\lambda-1}\}$ or $j \in \{0, 2^{\lambda-1}\}$, we directly have $R_1 = R'_1$ or $R_2 = R'_2$ as one of the necessary equations, and whichever we have will imply the other from the other equation. Thus, the attack is equivalent to finding a collision on $2n - 2\lambda$ bits.

Computing PRF outputs. The 2^{λ} outputs of E_K for a nonce $R_1 || R_2$ can be arranged in a tree to produce $2^{\lambda} - 1$ output blocks. The specific choice of the tree does not affect security, since all pairwise sums of the E_K outputs can be computed from any tree. For the design we propose, we choose the same tree as in the multi-block XORP function in CENC, fixing the first call as a 'root' and treating the other calls as 'leaves', so that the output of each leaf is XOR-ed to the output of the root to get one block of final output.

Pencil: An Optimally-Secure Weak PRF. We generalise and adapt the design idea discussed in Sec. 3.1 above with some changes into a mode we call Pencil. For generating the expanded input vector from the random IV, Pencil can use any linear transformation U whose transformation matrix has pairwise independent rows; we dub such transformations *locally non-degenerate*.

We first observe that when using linearly independent combinations of R_1 and R_2 as input vectors, the domain separator is no longer necessary, and can be done away with. This has two implications: first, the number of blocks ℓ in the output is no longer tied to λ , and we can set it from other considerations; second, this frees up the last λ bits of each call to E_K , and we use these to incorporate a non-random input into Pencil that can be used as a *chunk identifier*—like in CENC, each random IV can be used in multiple calls to Pencil (with distinct chunk identifier values) to get an output of up to $2^{\lambda}\ell$ blocks.

3.2 Formal Description

Let the *i*-th 2-block IV be denoted by $\mathbf{R}^{(i)} = (R_1^{(i)}, R_2^{(i)})^{\intercal}$, and the *i*-th output handle be denoted by $h_{\text{out}}^{(i)}$, where $R_1^{(i)}, R_2^{(i)} \in \{0, 1\}^{n-\lambda}$, and $h_{\text{out}}^{(i)} \in \{0, 1\}^{\lambda}$. For generating the ℓ block-cipher inputs we use an $(\ell + 1) \times 2$ matrix **U** over $\mathbb{GF}(2^{n-\lambda})$ with $\ell + 1$ pairwise independent rows; we call such a matrix



Figure 5: Diagram showing the computation of $\mathsf{Pencil}[\mathbf{U}, E]_K((R_1, R_2)^\intercal, h_{\text{out}})$ (left); and $\mathsf{Sharpen}[E]_{(K_1, K_2, K_3)}((N_1, N_2)^\intercal)$ (right).

locally non-degenerate. The input prefix vector for the *i*-th query is denoted $\tilde{\mathbf{X}}^{(i)} := (\tilde{X}_0^{(i)}, \dots, \tilde{X}_\ell^{(i)})^{\mathsf{T}}$, and computed as $\tilde{\mathbf{X}}^{(i)} \leftarrow \mathbf{U} \cdot \mathbf{R}^{(i)}$, i.e.,

$$\begin{pmatrix} \tilde{X}_{0}^{(i)} \\ \vdots \\ \tilde{X}_{\ell}^{(i)} \end{pmatrix} \leftarrow \mathbf{U}_{(\ell+1)\times 2} \cdot \begin{pmatrix} R_{1}^{(i)} \\ R_{2}^{(i)} \end{pmatrix}.$$
(9)

The input vector for the *i*-th query, denoted $\mathbf{X}^{(i)} := (X_0^{(i)}, \dots, X_{\ell}^{(i)})^{\mathsf{T}}$, is then computed by appending the output handle as a suffix to each block prefix: $X_j^{(i)} \leftarrow \tilde{X}_j^{(i)} || \langle h_{\text{out}} \rangle_{\lambda}$ for each $j \in [0..\ell]$.

The intermediate output vector for the *i*-th query is denoted $\mathbf{Y}^{(i)} := (Y_0^{(i)}, \ldots, Y_\ell^{(i)})^{\mathsf{T}}$, and computed as $Y_j^{(i)} \leftarrow E_K(X_j^{(i)})$ for each $j \in [0..\ell]$. The final output vector of the weak PRF for the *i*-th query is denoted $\mathbf{Z}^{(i)} := (Z_1^{(i)}, \ldots, Z_\ell^{(i)})^{\mathsf{T}}$, and computed as $Z_j^{(i)} \leftarrow Y_0^{(i)} \oplus Y_j^{(i)}$ for each $j \in [0..\ell]$. We denote the entire construction (mapping $\mathbf{R}^{(i)}$ to $\mathbf{Z}^{(i)}$) as Pencil[\mathbf{U}, E] (implicitly keyed with K). Fig. 5 (left) depicts the computation of Pencil[\mathbf{U}, E] with key K on an input ($\mathbf{R} = (R_1, R_2)^{\mathsf{T}}, h_{\text{out}}$), while Fig. 1 (top left) describes its algorithm.

3.3 Main Security Result

As the main security result for Pencil, we show the following.

Theorem 3. Suppose U is a locally non-degenerate $(\ell + 1) \times 2$ matrix over $\mathbb{GF}(2^{n-\lambda})$ with $\ell \geq 3$ and $n^3\ell^2 + n\ell \leq 2^{n/2}$. For any q-query wPRF-adversary \mathcal{A} , we can find a PRP-adversary \mathcal{B} making at most $q(\ell + 1)$ queries to its oracle such that

$$\mathbf{Adv}_{\mathsf{Pencil}[\mathbf{U},E]}^{\mathsf{wPRF}}(\mathcal{A}) \leq \frac{2\ell^2 q}{2^{n-\lambda}} + \frac{n\ell^2 q}{2^n} + \mathbf{Adv}_E^{\mathsf{PRP}}(\mathcal{B}),$$
(10)

as long as $(\ell+1)^2 q \leq 2^{n-\lambda-1}$ and $n\ell^2 q \leq 2^{n-4}$.

³The bound is of the same order even for smaller ℓ , but the constant factors degrade slightly, by a factor of about 1.5 for $\ell = 2$ and about 2.5 for $\ell = 1$.

Proof. As a first step we consider the unkeyed hybrid construction $\text{Pencil}[\mathbf{U}, \pi^*]$, which replaces the keyed block cipher E_K with a uniform random permutation $\pi^* : \{0,1\}^n \to \{0,1\}^n$.⁴ We will show the following bound in Appendix A.1.

Lemma 1. For any q-query wPRF-adversary \mathcal{A} , we can find a q-query wPRF-adversary \mathcal{A}' and a $q(\ell+1)$ query PRP-adversary \mathcal{B} such that

$$\mathbf{Adv}_{\mathsf{Pencil}[\mathbf{U},E]}^{\mathsf{wPRF}}(\mathcal{A}) \leq \mathbf{Adv}_{\mathsf{Pencil}[\mathbf{U},\pi^*]}^{\mathsf{wPRF}}(\mathcal{A}') + \mathbf{Adv}_E^{\mathsf{PRP}}(\mathcal{B}).$$
(11)

In the rest of this section we will establish a bound on $\operatorname{Adv}_{\operatorname{Pencil}[\mathbf{U},\pi^*]}^{\operatorname{WPRF}}(\mathcal{A})$ for any q-query adversary \mathcal{A} . Specifically, we will prove the following lemma.

Lemma 2. Suppose U is a locally non-degenerate $(\ell+1) \times 2$ matrix over $\mathbb{GF}(2^n)$ with $\ell \geq 3$ and $n^3\ell^2 + n\ell \leq 2^{n/2}$. For any q-query wPRF-adversary \mathcal{A} with $(\ell+1)^2q \leq 2^{n-\lambda-1}$ and $n\ell^2q \leq 2^{n-4}$,

$$\mathbf{Adv}_{\mathsf{Pencil}[\mathbf{U},\pi^*]}^{\mathsf{wPRF}}(\mathcal{A}) \le \frac{2\ell^2 q}{2^{n-\lambda}} + \frac{n\ell^2 q}{2^n}.$$
(12)

Theorem 3 follows from Lemmas 1 and 2.

3.4 Ideal World Sampling (Proof of Lemma 2)

For proving Lemma 2, we need to bound the advantage of a q-query wPRF-adversary \mathcal{A} against Pencil[U, π^*]. In the real world, for each input $(\mathbf{R}^{(i)}, h_{out}^{(i)})$, the vectors $\tilde{\mathbf{X}}^{(i)}$, $\mathbf{X}^{(i)}$, $\mathbf{Y}^{(i)}$, and $\mathbf{Z}^{(i)}$ are computed in sequence as described in Sec. 3.2, except that π^* is used in place of E_K for computing $\mathbf{Y}^{(i)}$ from $\mathbf{X}^{(i)}$; the final output vector sent to \mathcal{A} is $\mathbf{Z}^{(i)}$. At the end of the query phase, the q vectors $\mathbf{Y}^{(i)}$ for $i \in [1..q]$ are also released to \mathcal{A} ($\mathbf{X}^{(i)}$, of course, can be computed by \mathcal{A} , since U is public). In the ideal world, on receiving a query ($\mathbf{R}^{(i)}, h_{out}^{(i)}$), the oracle \mathcal{O}_0 computes and returns $\mathbf{Z}^{(i)} \leftarrow F^*(\mathbf{R}^{(i)}, h_{out}^{(i)})$; at the end of the query phase \mathcal{O}_0 samples $\mathbf{Y} := (\mathbf{Y}^{(1)}, \dots, \mathbf{Y}^{(q)})$ as described below and returns it to \mathcal{A} .

In order to sample \mathbf{Y} , \mathcal{O}_0 first computes $\mathbf{\tilde{X}} \leftarrow \mathbf{U} \cdot \mathbf{R}$, where $\mathbf{\tilde{X}} := (\mathbf{\tilde{X}}^{(1)}, \dots, \mathbf{\tilde{X}}^{(q)})$ and $\mathbf{R} := (\mathbf{R}^{(1)}, \dots, \mathbf{R}^{(q)})$, and sets $X_j^{(i)} = \tilde{X}_j^{(i)} || \langle s \rangle_{\lambda}$ for each $i \in [1..q], j \in [0..\ell]$. It looks at the set of distinct values $\{X_j^{(i)} \mid i \in [1..q], j \in [0..\ell]\}$, which are relabelled as X_1, \dots, X_r , where r denotes the number of distinct values taken by $X_j^{(i)}$. Let $h : [1..q] \times [0..\ell] \to [1..r]$ denote the relabelling function, such that for each $i \in [1..q], j \in [0..\ell], X_{h(i,j)} = X_j^{(i)}$. Next, \mathcal{O}_0 constructs a mirror system of ℓq equations Φ on r variables Y_1, \dots, Y_r as follows: for each $i \in [1..q], j \in [1..\ell], \mathcal{O}_0$ adds to Φ the equation $Y_{h(i,0)} \oplus Y_{h(i,j)} = Z_j^{(i)}$. Finally, if Φ is not a consistent mirror system, \mathcal{O}_0 samples $\mathbf{Y}_i^{(i)} \leftarrow_{\$} \{0,1\}^{(\ell+1)n}$ for each $i \in [1..q]$; otherwise, it samples $(Y_1, \dots, Y_r)^{\intercal} \leftarrow_{\$} \Gamma(\Phi)$, and assigns $Y_j^{(i)} = Y_{h(i,j)}$ for each $i \in [1..q], j \in [0..\ell]$.

Partitioning the Transcripts. Next we classify the set \mathcal{T} of all attainable transcripts into \mathcal{T}_{bad} and \mathcal{T}_{good} . Each transcript tr is represented as a tuple $(\mathbf{R}, \mathbf{h}_{out}, \mathbf{Z}, \mathbf{Y})$, where $\mathbf{h}_{out} := (h_{out}^{(1)}, \dots, h_{out}^{(q)})$; analogously, for each oracle \mathcal{O} , let the stochastic component of Trs $(\mathcal{A}^{\mathcal{O}})$ be parsed as $(\text{Trs } (\mathcal{A}^{\mathcal{O}}; 1), \text{Trs } (\mathcal{A}^{\mathcal{O}}; 2), \text{Trs } (\mathcal{A}^{\mathcal{O}}; 3))$, to denote the randomised nonce vector, output vector, and intermediate output vector respectively. Let Φ_{tr} be the system of equations associated with a transcript tr in the manner described above (where Φ is completely determined by \mathbf{R} , \mathbf{h}_{out} , and \mathbf{Z}), and, when Φ_{tr} is a mirror system, let $\xi_{max}(tr)$ be

⁴To be precise, π^* can be thought of as the family of all permutations over $\{0, 1\}^n$, and the particular choice of permutation can be thought of as a key. These nuances don't affect the proof, and therefore with slight abuse of notation we continue to call the hybrid construction Pencil[\mathbf{U}, π^*].

the size of the largest component in $\mathcal{G}(\phi_{tr})$; for a positive integer L we say Φ_{tr} is L-scattered if $\xi_{max}(tr) \leq L$. We first define the following two sets:

$$\begin{split} \mathcal{T}_{\mathsf{bad},1} &:= \{\mathsf{tr} \mid \Phi_{\mathsf{tr}} \text{ is not a redundancy-free}, \ \textit{n}\ell\text{-scattered mirror system}\}, \\ \mathcal{T}_{\mathsf{bad},2} &:= \{\mathsf{tr} \mid \Phi_{\mathsf{tr}} \text{ is not a consistent mirror system}\}. \end{split}$$

Then we define $\mathcal{T}_{\mathsf{bad}} := \mathcal{T}_{\mathsf{bad},1} \cup \mathcal{T}_{\mathsf{bad},2}$, and $\mathcal{T}_{\mathsf{good}} := \mathcal{T} \setminus \mathcal{T}_{\mathsf{bad}}$. We state below two lemmas, which we will prove in Sec. 3.5 and Appendix A.2 respectively.

Lemma 3. For any q-query adversary \mathcal{A} ,

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right)\in\mathcal{T}_{\mathsf{bad}}\right]\leq\frac{2\ell^{2}q}{2^{n-\lambda}}+\frac{n\ell^{2}q}{2^{n}},\tag{13}$$

under the assumptions that $\ell \geq 3$ and $(\ell+1)^2 q \leq 2^{n-\lambda-1}$.

Lemma 4. For any q-query adversary \mathcal{A} and for any $tr \in \mathcal{T}_{good}$,

$$\frac{\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = tr\right]}{\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = tr\right]} \ge 1.$$
(14)

under the assumptions that $n^3\ell^2 + n\ell \leq 2^{n/2}$, and $n\ell^2 q \leq 2^{n-4}$.

Lemma 2 follows from Theorem 1 and Lemmas 3 and 4, by choosing $\epsilon_1 = 2\ell^2 q/2^{n-\lambda} + n\ell^2 q/2^n$ and $\epsilon_2 = 0$.

3.5 Bad Probability Calculations (Proof of Lemma 3)

In this subsection, we'll denote $\operatorname{Trs} (\mathcal{A}^{\mathcal{O}_0})$ as $\operatorname{tr} = (\mathbf{R}, \mathbf{h}_{out}, \mathbf{Z}, \mathbf{Y})$; of these, \mathbf{h}_{out} is fully under adversarial control, and the rest we treat as random variables sampled in the ideal world as described earlier. First we observe that whether or not $\operatorname{tr} \in \mathcal{T}_{\mathsf{bad},1}$ is determined entirely by $(\mathbf{R}, \mathbf{h}_{out})$, so we begin by bounding various kinds of degeneracy events on the sampling of \mathbf{R} . Let $\mathbf{U}_{k*}^{\mathsf{T}}$ denote the k-th row of \mathbf{U} for each $k \in [0..\ell]$.

Bounding within-query collisions. Let \mathcal{E}_1 denote the event that for some $i \in [1..q]$ and $j < j' \in [0..\ell]$ with $j \neq j'$,

 $X_{i'}^{(i)} = X_i^{(i)}.$ (15)

We will show the following bound on $\Pr[\mathcal{E}_1]$ in Appendix A.3.

Lemma 5.

$$\Pr[\mathcal{E}_1] \le \frac{\ell(\ell+1)q}{2^{n-\lambda+1}}.$$
(16)

Bounding two-query cycles. Let \mathcal{E}_2 denote the event that for some $i_1, i_2 \in [1..q]$ with $i_1 < i_2$, and some $j_1, j'_1, j_2, j'_2 \in [0..\ell]$ with $j_1 < j'_1, j_2 < j'_2$,

$$(X_{j_2}^{(i_2)}, X_{j'_2}^{(i_2)}) = (X_{j_1}^{(i_1)}, X_{j'_1}^{(i_1)}).$$
(17)

We will show the following bound on $\Pr[\mathcal{E}_2]$ in Appendix A.4.

Lemma 6.

$$\Pr[\mathcal{E}_2] \le \frac{\ell^2 (\ell+1)^2 q(q-1)}{2^{2n-2\lambda+3}}.$$
(18)

Bounding long paths. Let \mathcal{E}_3 denote the event that for some $i_1, \ldots, i_{n+1} \in [1..q]$ with $i_1 < \cdots < i_{n+1}$, and some $j_1, \ldots, j_n, j'_2, \ldots, j'_{n+1} \in [0..\ell]$,

$$(X_{j'_2}^{(i_2)}, \dots, X_{j'_{n+1}}^{(i_{n+1})}) = (X_{j_1}^{(i_1)}, \dots, X_{j_n}^{(i_n)}).$$
(19)

We will show the following bound on $\Pr[\mathcal{E}_3]$ in Appendix A.5.

Lemma 7. As long as $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$,

$$\Pr[\mathcal{E}_3] \le \frac{q}{2^n}.\tag{20}$$

Bounding multi-query cycles. For each $k \in [3..n]$, let $\mathcal{E}_{4,k}$ denote the event that for some $i_1, \ldots, i_k \in [1..q]$ with $i_1 < \cdots < i_k$, and some $j_1, \ldots, j_k, j'_1, \ldots, j'_k \in [0..\ell]$,

$$(X_{j'_2}^{(i_2)}, \dots, X_{j'_k}^{(i_k)}, X_{j'_1}^{(i_1)}) = (X_{j_1}^{(i_1)}, \dots, X_{j_{k-1}}^{(i_{k-1})}, X_{j_k}^{(i_k)}).$$

$$(21)$$

Let \mathcal{E}_4 denote the event $\mathcal{E}_{4,3} \lor \cdots \lor \mathcal{E}_{4,n}$. We will show the following bound on $\Pr[\mathcal{E}_4]$ in Appendix A.6. Lemma 8. As long as $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$,

$$\Pr[\mathcal{E}_4] \le \frac{(\ell+1)^6 q^3}{2^{3n-3\lambda-1}}.$$
(22)

Getting a bound for $\Pr[\mathsf{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},1}]$. Let $\mathcal{E}_{\mathsf{bad},1}$ be the event $\mathsf{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},1}$. We observe that

$$\mathcal{E}_{\mathsf{bad},1} \subseteq \mathcal{E}_1 \lor \mathcal{E}_2 \lor \mathcal{E}_3 \lor \mathcal{E}_4.$$
⁽²³⁾

Thus, applying union-bound to Eqns. (16), (18), (20), and (22), we get

$$\Pr[\mathcal{E}_{\mathsf{bad},1}] \leq \Pr[\mathcal{E}_{1}] + \Pr[\mathcal{E}_{2}] + \Pr[\mathcal{E}_{3}] + \Pr[\mathcal{E}_{4}]$$

$$\leq \frac{\ell(\ell+1)q}{2^{n-\lambda+1}} + \frac{\ell^{2}(\ell+1)^{2}q(q-1)}{2^{2n-2\lambda+3}} + \frac{q}{2^{n}} + \frac{(\ell+1)^{6}q^{3}}{2^{3n-3\lambda-1}}$$

$$\leq \frac{(\ell+1)^{2}q}{2^{n-\lambda}} \left[\frac{1}{2} + \frac{(\ell+1)^{2}q}{2^{n-\lambda+3}} + \frac{1}{(\ell+1)^{2}2^{\lambda}} + \frac{(\ell+1)^{4}q^{2}}{2^{2n-2\lambda-1}}\right]$$

$$\leq \frac{(\ell+1)^{2}q}{2^{n-\lambda}} \left[\frac{1}{2} + \frac{1}{16} + \frac{1}{(\ell+1)^{2}2^{\lambda}} + \frac{1}{2}\right] \leq \frac{9}{8} \frac{(\ell+1)^{2}q}{2^{n-\lambda}} \leq \frac{2\ell^{2}q}{2^{n-\lambda}}, \quad (24)$$

the last inequality following from the assumption that $\ell \geq 3$.

Bounding zero blocks. For the rest of this proof, we condition on $\neg \mathcal{E}_{\mathsf{bad},1}$, so we will only consider the such that Φ_{tr} is redundancy-free and $n\ell$ -scattered. As discussed in Sec. 2.5, we can assume without loss of generality that each component of $\mathcal{G}(\Phi_{\mathsf{tr}}) = \Phi[\mathbf{A}, \mathbf{Z}]$ is a star graph. Let \mathcal{E}_5 be the event that $Z_j = 0$ for some $j \in [1..\ell q]$. Then

$$\Pr[\mathcal{E}_5 \mid \neg \mathcal{E}_{\mathsf{bad},1}] \le \frac{\ell q}{2^n}.$$
(25)

⁵For $\ell = 2$, we can bound this by $3\ell^2 q/2^{n-\lambda}$, and for $\ell = 1$, by $5\ell^2 q/2^{n-\lambda}$.

Bounding output collisions. Let \mathcal{E}_6 be the event that $Z_i^p = Z_j^p$ for some $p \in [1..c]$ and $i, j \in [1..\xi_p]$ with $i \neq j$. Then

$$\Pr[\mathcal{E}_6 \mid \neg \mathcal{E}_{\mathsf{bad},1}] \le \sum_{p=1}^c \binom{\xi_p}{2} \frac{1}{2^n} \le \frac{\xi_{\max}}{2^{n+1}} \sum_{p=1}^c \xi_p \le \frac{n\ell^2 q}{2^{n+1}}.$$
(26)

Getting a bound for $\Pr[\mathsf{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},2} \mid \neg \mathcal{E}_{\mathsf{bad},1}]$. Let $\mathcal{E}_{\mathsf{bad},2}$ be the event $\mathsf{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},2}$. We observe that

$$\mathcal{E}_{\mathsf{bad},2} \land \neg \mathcal{E}_{\mathsf{bad},1} \subseteq (\mathcal{E}_5 \land \neg \mathcal{E}_{\mathsf{bad},1}) \lor (\mathcal{E}_6 \land \neg \mathcal{E}_{\mathsf{bad},1}).$$

Thus, applying union-bound to Eqns. (25) and (26), we get

$$\Pr[\mathcal{E}_{\mathsf{bad},2} \mid \neg \mathcal{E}_{\mathsf{bad},1}] \leq \Pr[\mathcal{E}_5 \mid \neg \mathcal{E}_{\mathsf{bad},1}] + \Pr[\mathcal{E}_6 \mid \neg \mathcal{E}_{\mathsf{bad},1}]$$
$$\leq \frac{\ell q}{2^n} + \frac{n\ell^2 q}{2^{n+1}} = \frac{n\ell^2 q}{2^n} \left(\frac{1}{2} + \frac{1}{n\ell}\right) \leq \frac{n\ell^2 q}{2^n}.$$
(27)

Getting a bound for $\Pr[\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad}}]$. From the definitions of $\mathcal{E}_{\mathsf{bad},1}$, $\mathcal{E}_{\mathsf{bad},2}$, and $\mathcal{T}_{\mathsf{bad}}$, and from Eqns. (24) and (27), we get

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) \in \mathcal{T}_{\mathsf{bad}}\right] = \Pr[\mathcal{E}_{\mathsf{bad},1} \lor \mathcal{E}_{\mathsf{bad},2}]$$
$$= \Pr[\mathcal{E}_{\mathsf{bad},1}] + \Pr[\mathcal{E}_{\mathsf{bad},2} \mid \neg \mathcal{E}_{\mathsf{bad},1}]$$
$$\leq \frac{2\ell^{2}q}{2^{n-\lambda}} + \frac{n\ell^{2}q}{2^{n}}, \tag{28}$$

thus establishing Eqn. (13), and completing the proof of Lemma 3.

4 Building a strong PRF from **Pencil**

Here we describe how to build a strong PRF from Pencil, by adding a preprocessing layer to the input. Specifically, we design a function Sharpen : $\{0,1\}^{3\kappa} \times \{0,1\}^{2n} \to \{0,1\}^{2n-2\lambda}$ that uses a 3κ -bit key and accepts a 2n-bit user chosen input, and outputs a 'randomised' $(2n - 2\lambda)$ -bit IV that can be fed into Pencil. We use it to build a PRF \sharp Pencil : $\{0,1\}^{4\kappa} \times \{0,1\}^{2n} \times \{0,1\}^{\lambda} \to \{0,1\}^{\ell n}$,⁶ which uses a 4κ -bit key and transforms a 2n-bit input along with a λ -bit output handle to an ℓn -bit output chunk. The function Sharpen with key $\tilde{K} := (K_1, K_2, K_3) \in \{0,1\}^{3\kappa}$ is defined as

$$\begin{aligned} \mathsf{Sharpen}[E]_{\tilde{K}}(N_1, N_2) &:= (\mathsf{msb}_{n-\lambda}(E_{K_2}(N_1 \oplus E_{K_1}(N_2))), \\ & \mathsf{msb}_{n-\lambda}(E_{K_3}(N_1 \oplus 2 \cdot E_{K_1}(N_2)))) \,. \end{aligned}$$

Fig. 5 (right) depicts the computation of Sharpen[E] with key (K_1, K_2, K_3) on an input $\mathbf{N} = (N_1, N_2)^{\intercal}$, while Fig. 1 (top right) describes its algorithm. The PRF \sharp Pencil is then defined as

$$\sharp \mathsf{Pencil}[\mathbf{U}, E]_{\tilde{K}, K_4}(N_1, N_2, h_{\mathrm{out}}) := \mathsf{Pencil}[\mathbf{U}, E]_{K_4}(\mathsf{Sharpen}[E]_{\tilde{K}}(N_1, N_2)^\intercal, h_{\mathrm{out}})$$

Fig. 1 (bottom) describes the algorithm of $\sharp \mathsf{Pencil}[\mathbf{U}, E]$ with key (K_1, K_2, K_3, K_4) on an input $(\mathbf{N} = (N_1, N_2)^{\mathsf{T}}, h_{\mathrm{out}})$.

⁶Pronounced 'sharp pencil'.

4.1 Security Result

As the main security result for *#Pencil*, we show the following.

Theorem 4. Suppose U is a locally non-degenerate $(\ell + 1) \times 2$ matrix over $\mathbb{GF}(2^{n-\lambda})$, with $\ell \geq 3$ and $n^3\ell^2 + n\ell \leq 2^{n/2}$. For any q-query PRF-adversary \mathcal{A} , we can find three PRP-adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ each making at most q queries to its oracle and a PRP-adversary \mathcal{B}_4 making at most $q(\ell + 1)$ queries to its oracle such that

$$\mathbf{Adv}_{\sharp \mathsf{Pencil}[\mathbf{U},E]}^{\mathsf{PRF}}(\mathcal{A}) \leq \frac{13\ell^2 q}{2^{n-\lambda}} + \frac{n\ell^2 q}{2^n} + \sum_{i=1}^4 \mathbf{Adv}_E^{\mathsf{PRP}}(\mathcal{B}_i),$$
(29)

as long as $(\ell+1)^2 q \leq 2^{n-\lambda-1}$ and $n\ell^2 q \leq 2^{n-4}$.

Proof. The structure of the proof follows closely that of Theorem 3. As a first step we consider the unkeyed hybrid construction $\sharp \mathsf{Pencil}[\mathbf{U}, \tilde{\pi}^* := (\pi_1^*, \pi_2^*, \pi_3^*, \pi_4^*)]$, which replaces E_{K_i} with a uniform random permutation $\pi_i^* : \{0, 1\}^n \to \{0, 1\}^n$ for each $i \in [1..4]$.⁷ We will show the following bound in Appendix B.1.

Lemma 9. For any q-query PRF-adversary \mathcal{A} , we can find a q-query PRF-adversary \mathcal{A}' , three q-query PRP-adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$, and a $q(\ell + 1)$ -query PRP-adversary \mathcal{B}_4 such that

$$\mathbf{Adv}_{\sharp Pencil[\mathbf{U},E]}^{PRF}(\mathcal{A}) \leq \mathbf{Adv}_{\sharp Pencil[\mathbf{U},\tilde{\pi}^*]}^{PRF}(\mathcal{A}') + \sum_{i=1}^{4} \mathbf{Adv}_{E}^{PRP}(\mathcal{B}_{i}).$$
(30)

In the rest of this section we will establish a bound on $\mathbf{Adv}_{\sharp\mathsf{Pencil}[\mathbf{U},\tilde{\pi}^*]}^{\mathsf{wPRF}}(\mathcal{A})$ for any q-query adversary \mathcal{A} . Specifically, we will prove the following lemma.

Lemma 10. Suppose U is a locally non-degenerate $(\ell + 1) \times 2$ matrix over $\mathbb{GF}(2^n)$, with $\ell \geq 3$ and $n^3\ell^2 + n\ell \leq 2^{n/2}$. For any q-query PRF-adversary \mathcal{A} ,

$$\mathbf{Adv}_{\sharp Penci/[\mathbf{U},\tilde{\pi}^*]}^{PRF}(\mathcal{A}) \leq \frac{13\ell^2 q}{2^{n-\lambda}} + \frac{n\ell^2 q}{2^n},\tag{31}$$

as long as $(\ell+1)^2 q \leq 2^{n-\lambda-1}$ and $n\ell^2 q \leq 2^{n-4}$.

Theorem 4 follows from Lemmas 9 and 10.

4.2 Proof of Lemma 10

For proving Lemma 10, we need to bound the advantage of a q-query PRF-adversary \mathcal{A} against \sharp Pencil[U, $\tilde{\pi}^*$]. As in the proof of Lemma 2, we first describe how all the intermediate and final outputs are computed in the two worlds. In the real world, for each input $(\mathbf{N}^{(i)}, h_{out}^{(i)})$, $J^{(i)}$, $\mathbf{W}^{(i)}$, and $\mathbf{R}^{(i)}$ are first computed by running Sharpen[$(\pi_1^*, \pi_2^*, \pi_3^*)$]—which replaces the calls to E_{K_1} , E_{K_2} , and E_{K_3} with calls to $\pi_1^*, \pi_2^*, \pi_3^*$ respectively—as follows: $J^{(i)} \leftarrow \pi_1^*(N_2^{(i)})$, $\mathbf{W}^{(i)} := (W_1^{(i)}, W_2^{(i)})^{\mathsf{T}} \leftarrow (\frac{1}{1}\frac{1}{2}) \cdot (N_1^{(i)}, J^{(i)})^{\mathsf{T}}$, $R_1^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(\pi_2^*(W_1^{(i)}))$, $R_2^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(\pi_3^*(W_2^{(i)}))$. The vectors $\tilde{\mathbf{X}}^{(i)}$, $\mathbf{X}^{(i)}$, $\mathbf{Y}^{(i)}$, and $\mathbf{Z}^{(i)}$ are then computed in sequence using Pencil[U, π_4^*]; the final output vector sent to \mathcal{A} is $\mathbf{Z}^{(i)}$. At the end of the query phase, $\mathbf{J} := (J^{(1)}, \ldots, J^{(q)})$, $\mathbf{R} := (\mathbf{R}^{(1)}, \ldots, \mathbf{R}^{(q)})$, and $\mathbf{Y} := (\mathbf{Y}^{(1)}, \ldots, \mathbf{Y}^{(q)})$ are also released to \mathcal{A} ; $\mathbf{W} := (\mathbf{W}^{(1)}, \ldots, \mathbf{W}^{(q)})$ and $\mathbf{X} := (\mathbf{X}^{(1)}, \ldots, \mathbf{X}^{(q)})$ can be computed by \mathcal{A} .

In the ideal world, on receiving a query $(\mathbf{N}^{(i)}, h_{out}^{(i)})$, the oracle \mathcal{O}_0 computes and returns $\mathbf{Z}^{(i)} \leftarrow F^*(\mathbf{N}^{(i)}, h_{out}^{(i)})$; at the end of the query phase \mathcal{O}_0 computes \mathbf{J} and \mathbf{R} exactly as in the real world, by running Sharpen[$(\pi_1^*, \pi_2^*, \pi_3^*)$]; it then samples \mathbf{Y} as described in Sec. 3.4, and returns \mathbf{J}, \mathbf{R} , and \mathbf{Y} to \mathcal{A} .

⁷Again, with slight abuse of notation, we continue to call the hybrid construction $\sharp \mathsf{Pencil}[\mathbf{U}, \pi^*]$.

Partitioning the Transcripts. Each transcript tr is represented as a tuple $(\mathbf{N}, \mathbf{h}_{out}; \mathbf{Z}; \mathbf{J}, \mathbf{R}, \mathbf{Y})$, where $\mathbf{h}_{out} := (h_{out}^{(1)}, \ldots, h_{out}^{(q)})$. We will classify the set \mathcal{T} of all attainable transcripts into \mathcal{T}_{bad} and \mathcal{T}_{good} . For each oracle \mathcal{O} , let the stochastic component of Trs $(\mathcal{A}^{\mathcal{O}})$ be parsed as $(\text{Trs } (\mathcal{A}^{\mathcal{O}}; 1), \text{Trs } (\mathcal{A}^{\mathcal{O}}; 2), \text{Trs } (\mathcal{A}^{\mathcal{O}}; 3))$, to denote the preprocessed input vector, final output vector, and intermediate output vector respectively. Let Φ_{tr} be the system of equations associated with a transcript tr in the manner described above (where Φ is completely determined by $\mathbf{R}, \mathbf{h}_{out}, \text{ and } \mathbf{Z}$), and, when Φ_{tr} is a mirror system, let $\xi_{max}(tr)$ be the size of the largest component in $\mathcal{G}(\phi_{tr})$. We recall that for a positive integer L we say Φ_{tr} is L-scattered if $\xi_{max}(tr) \leq L$. We first define the following two sets:

 $\mathcal{T}_{\mathsf{bad},1} := \{\mathsf{tr} \mid \Phi_{\mathsf{tr}} \text{ is not a redundancy-free, } n\ell \text{-scattered mirror system}\},\$

 $\mathcal{T}_{\mathsf{bad},2} := \{\mathsf{tr} \mid \Phi_{\mathsf{tr}} \text{ is not a consistent mirror system}\}.$

Then we define $\mathcal{T}_{\mathsf{bad}} := \mathcal{T}_{\mathsf{bad},1} \cup \mathcal{T}_{\mathsf{bad},2}$, and $\mathcal{T}_{\mathsf{good}} := \mathcal{T} \setminus \mathcal{T}_{\mathsf{bad}}$. We state below two lemmas, which we will prove in Sec. 4.3 and Appendix B.2 respectively.

Lemma 11. For any q-query adversary \mathcal{A} ,

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) \in \mathcal{T}_{\mathsf{bad}}\right] \leq \frac{13\ell^{2}q}{2^{n-\lambda}} + \frac{n\ell^{2}q}{2^{n}},\tag{32}$$

under the assumptions that $\ell \geq 3$ and $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$.

Lemma 12. For any q-query adversary \mathcal{A} and for any $tr \in \mathcal{T}_{good}$,

$$\frac{\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = tr\right]}{\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = tr\right]} \ge 1.$$
(33)

under the assumptions that $n^3\ell^2 + n\ell \leq 2^{n/2}$, and $n\ell^2 q \leq 2^{n-4}$.

Lemma 10 follows from Theorem 1 and Lemmas 11 and 12, by choosing $\epsilon_1 = 13\ell^2 q/2^{n-\lambda} + n\ell^2 q/2^n$ and $\epsilon_2 = 0$.

4.3 Proof of Lemma 11

In this subsection, we'll denote $\operatorname{Trs} (\mathcal{A}^{\mathcal{O}_0})$ as $\operatorname{tr} = (\mathbf{N}, \mathbf{h}_{out}; \mathbf{Z}; \mathbf{J}, \mathbf{R}, \mathbf{Y})$; of these, \mathbf{N} and \mathbf{h}_{out} are under adversarial control, and the rest we treat as random variables sampled in the ideal world as described earlier. First we observe that whether or not $\operatorname{tr} \in \mathcal{T}_{\mathsf{bad},1}$ is determined entirely by $(\mathbf{R}, \mathbf{h}_{out})$. So we begin by bounding various kinds of degeneracy events on the sampling of \mathbf{R} . Let $\mathbf{U}_{k*}^{\mathsf{T}}$ denote the k-th row of \mathbf{U} for each $k \in [0..\ell]$, and let U_{ks} denote the s-th symbol of $\mathbf{U}_{k*}^{\mathsf{T}}$ for $s \in \{1, 2\}$.

Bounding Arms and Elbows. For distinct $i_1, i_2 \in [1..q]$, the pair (i_1, i_2) is called an *arm* if either $W_1^{(i_1)} = W_1^{(i_2)}$ or $W_2^{(i_1)} = W_2^{(i_2)}$. Let \mathcal{S}_{ar} denote the set of all arms. Let \mathcal{E}_{ar} denote the event that $|\mathcal{S}_{ar}| > q$. We will show the following bound on $\Pr[\mathcal{E}_{ar}]$ in Appendix B.3.

Lemma 13.

$$\Pr[\mathcal{E}_{ar}] \le \frac{2q}{2^n}.\tag{34}$$

For distinct $i_1, i_2, i_3 \in [1..q]$, the triple (i_1, i_2, i_3) is called an *elbow* if $W_1^{(i_1)} = W_1^{(i_2)}$ and $W_2^{(i_2)} = W_2^{(i_3)}$. Let $\mathcal{S}_{\mathsf{el}}$ denote the set of all elbows. Let $\mathcal{E}_{\mathsf{el}}$ denote the event that $|\mathcal{S}_{\mathsf{el}}| > q$. We will show the following bound on $\Pr[\mathcal{E}_{\mathsf{el}}]$ in Appendix B.4.

Lemma 14.

$$\Pr[\mathcal{E}_{el}] \le \frac{q}{2^n} + \frac{q^2}{2^{2n}}.$$
(35)

Bounding Stale Nodes on Chains. For some $k \ge 2$ and distinct $i_1, \ldots, i_k \in [1..q]$, we call $\zeta := (i_1, \ldots, i_k)$ a k-chain if for some $j_1, \ldots, j_{k-1}, j'_2, \ldots, j'_k \in [0..\ell]$,

$$(X_{j'_2}^{(i_2)}, \dots, X_{j'_k}^{(i_k)}) = (X_{j_1}^{(i_1)}, \dots, X_{j_{k-1}}^{(i_{k-1})}).$$
(36)

Each query index i_d for $d \in [1..k]$ in a k-chain ζ is called a *node* of ζ . A node i_d for $d \ge 2$ is called *fresh* if either $W_1^{(i_d)} \notin \{W_1^{(i_a)} \mid 1 \le a < d\}$ or $W_2^{(i_d)} \notin \{W_2^{(i_a)} \mid 1 \le a < d\}$ (or both), and *stale* otherwise. Let $\mathcal{E}_{\mathsf{ch},k}$ denote the event that there exists a k-chain $\zeta = (i_1, \ldots, i_k)$ such that i_d is stale for some

Let $\mathcal{E}_{\mathsf{ch},k}$ denote the event that there exists a k-chain $\zeta = (i_1, \ldots, i_k)$ such that i_d is stale for some $d \in [2..k]$. Let $\mathcal{E}_{\mathsf{ch}}$ denote the event $\mathcal{E}_{\mathsf{ch},3} \lor \cdots \lor \mathcal{E}_{\mathsf{ch},n+1}$. We will show the following bound on $\Pr[\mathcal{E}_{\mathsf{ch}}]$ in Appendix B.5.

Lemma 15. As long as $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$,

$$\Pr[\mathcal{E}_{ch}] \le \frac{q}{2^n} + \frac{q^2}{2^{2n}} + \frac{(\ell+1)^2 q}{2^{n-\lambda-1}}.$$
(37)

Bounding within-query collisions. Let \mathcal{E}_1^{\dagger} denote the event that for some $i \in [1..q]$ and $j < j' \in [0..\ell]$ with $j \neq j'$,

$$X_{j'}^{(i)} = X_j^{(i)}. (38)$$

We will show the following bound on $\Pr[\mathcal{E}_1^{\dagger}]$ in Appendix B.6.

Lemma 16.

$$\Pr[\mathcal{E}_1^{\dagger}] \le \frac{\ell(\ell+1)q}{2^{n-\lambda+1}}.\tag{39}$$

Bounding two-query cycles. Let \mathcal{E}_2^{\dagger} denote the event that for some $i_1, i_2 \in [1..q]$ with $i_1 < i_2$, and some $j_1, j'_1, j_2, j'_2 \in [0..\ell]$ with $j_1 < j'_1, j_2 < j'_2$,

$$(X_{j_2}^{(i_2)}, X_{j'_2}^{(i_2)}) = (X_{j_1}^{(i_1)}, X_{j'_1}^{(i_1)}).$$

$$(40)$$

We will show the following bound on $\Pr[\mathcal{E}_2^{\dagger} \mid \neg \mathcal{E}_{ar}]$ in Appendix B.7.

Lemma 17.

$$\Pr[\mathcal{E}_2^{\dagger} \mid \neg \mathcal{E}_{ar}] \le \frac{\ell(\ell+1)q}{2^{n-\lambda}} + \frac{\ell^2(\ell+1)^2 q^2}{2^{2n-2\lambda+4}}.$$
(41)

Bounding long paths. Let \mathcal{E}_3^{\dagger} denote the event that for some $i_1, \ldots, i_{n+1} \in [1..q]$ with $i_1 < \cdots < i_{n+1}$, and some $j_1, \ldots, j_n, j'_2, \ldots, j'_{n+1} \in [0..\ell]$,

$$(X_{j'_2}^{(i_2)}, \dots, X_{j'_{n+1}}^{(i_{n+1})}) = (X_{j_1}^{(i_1)}, \dots, X_{j_n}^{(i_n)}).$$

$$(42)$$

We will show the following bound on $\Pr[\mathcal{E}_3^{\dagger} \mid \neg \mathcal{E}_{ch}]$ in Appendix B.8.

Lemma 18. As long as $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$,

$$\Pr[\mathcal{E}_3^{\dagger} \mid \neg \mathcal{E}_{ch}] \le \frac{q}{2^n}.$$
(43)

Bounding multi-query cycles. For each $k \in [3..n]$, let $\mathcal{E}_{4,k}^{\dagger}$ denote the event that for some $i_1, \ldots, i_k \in [1..q]$ with $i_1 < \cdots < i_k$, and some $j_1, \ldots, j_k, j'_1, \ldots, j'_k \in [0..\ell]$,

$$(X_{j'_2}^{(i_2)}, \dots, X_{j'_k}^{(i_k)}, X_{j'_1}^{(i_1)}) = (X_{j_1}^{(i_1)}, \dots, X_{j_{k-1}}^{(i_{k-1})}, X_{j_k}^{(i_k)}).$$

$$(44)$$

Let \mathcal{E}_4^{\dagger} denote the event $\mathcal{E}_{4,3}^{\dagger} \vee \cdots \vee \mathcal{E}_{4,n}^{\dagger}$. We will show the following bound on $\Pr[\mathcal{E}_4^{\dagger} \mid \neg \mathcal{E}_{ch}, \neg \mathcal{E}_{ar}]$ in Appendix B.9.

Lemma 19. As long as $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$,

$$\Pr[\mathcal{E}_4^{\dagger} \mid \neg \mathcal{E}_{ch}, \neg \mathcal{E}_{ar}] \le \frac{6(\ell+1)^4 q^2}{2^{2n-2\lambda}}.$$
(45)

Getting a bound for $\Pr[\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},1}]$. Let $\mathcal{E}^{\dagger}_{\mathsf{bad},1}$ be the event $\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},1}$. We observe that $\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0})$ cannot have redundancy except by triggering \mathcal{E}^{\dagger}_1 , \mathcal{E}^{\dagger}_2 , or \mathcal{E}^{\dagger}_4 , and cannot be $n\ell$ -scattered except by triggering \mathcal{E}^{\dagger}_3 . Thus,

$$\mathcal{E}_{\mathsf{bad},1}^{\dagger} \subseteq \mathcal{E}_{1}^{\dagger} \lor \mathcal{E}_{2}^{\dagger} \lor \mathcal{E}_{3}^{\dagger} \lor \mathcal{E}_{4}^{\dagger}. \tag{46}$$

Define $\mathcal{E}_{\mathsf{aux}} := \mathcal{E}_{\mathsf{ar}} \vee \mathcal{E}_{\mathsf{ch}}$. Then we can write

$$Pr[\mathcal{E}_{\mathsf{bad},1}^{\dagger}] = Pr[\mathcal{E}_{\mathsf{bad},1}^{\dagger} \wedge \mathcal{E}_{\mathsf{aux}}] + Pr[\mathcal{E}_{\mathsf{bad},1}^{\dagger} \wedge \neg \mathcal{E}_{\mathsf{aux}}]$$

$$\leq Pr[\mathcal{E}_{\mathsf{aux}}] + \sum_{i=1}^{4} Pr[\mathcal{E}_{i}^{\dagger} \wedge \neg \mathcal{E}_{\mathsf{aux}}]$$

$$\leq Pr[\mathcal{E}_{\mathsf{ar}}] + Pr[\mathcal{E}_{\mathsf{ch}}] + Pr[\mathcal{E}_{1}^{\dagger}] + Pr[\mathcal{E}_{2}^{\dagger} \wedge \neg \mathcal{E}_{\mathsf{ar}}]$$

$$+ Pr[\mathcal{E}_{3}^{\dagger} \wedge \neg \mathcal{E}_{\mathsf{ch}}] + Pr[\mathcal{E}_{4}^{\dagger} \wedge \neg \mathcal{E}_{\mathsf{aux}}]$$

$$\leq Pr[\mathcal{E}_{\mathsf{ar}}] + Pr[\mathcal{E}_{\mathsf{ch}}] + Pr[\mathcal{E}_{1}^{\dagger}] + Pr[\mathcal{E}_{2}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{ar}}]$$

$$+ Pr[\mathcal{E}_{3}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{ch}}] + Pr[\mathcal{E}_{4}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{ar}}, \neg \mathcal{E}_{\mathsf{ch}}]. \tag{47}$$

Substituting the bounds from Eqns. (34), (37), (39), (41), (43), and (45) (Lemmas 13, 15, 16, 17, 18, and 19) in Eqn. (47) gives

$$\Pr[\mathcal{E}_{\mathsf{bad},1}^{\dagger}] \leq \frac{2q}{2^{n}} + \frac{q}{2^{n}} + \frac{q^{2}}{2^{2n}} + \frac{(\ell+1)^{2}q}{2^{n-\lambda-1}} + \frac{\ell(\ell+1)q}{2^{n-\lambda+1}} + \frac{\ell(\ell+1)q}{2^{n-\lambda+1}} + \frac{\ell(\ell+1)q}{2^{2n-2\lambda+4}} + \frac{q}{2^{n}} + \frac{6(\ell+1)^{4}q^{2}}{2^{2n-2\lambda}} \\ \leq \frac{7(\ell+1)^{2}q}{2^{n-\lambda+1}} + \frac{7(\ell+1)^{4}q^{2}}{2^{2n-2\lambda}} \leq \frac{7(\ell+1)^{2}q}{2^{n-\lambda}} \leq \frac{13\ell^{2}q}{2^{n-\lambda}},$$
(48)

using the assumption $\ell \geq 3$ for the last inequality and the assumption $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$ for the one before.

Bounding zero blocks. For the rest of this proof, we condition on $\neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}$, so we will only consider tr such that Φ_{tr} is redundancy-free and $n\ell$ -scattered. As discussed in Sec. 2.5, we can assume without loss of generality that each component of $\mathcal{G}(\Phi_{\mathsf{tr}}) = \Phi[\mathbf{A}, \mathbf{Z}]$ is a star graph. Let \mathcal{E}_5^{\dagger} be the event that $Z_j = 0$ for some $j \in [1..\ell q]$. Then

$$\Pr[\mathcal{E}_5^{\dagger} \mid \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}] \le \frac{\ell q}{2^n}.\tag{49}$$

CAU	$[E, \mathcal{H}]$.Enc (EK, \tilde{N}, AD, M)	CAL	$U[E,\mathcal{H}].Dec(\mathrm{EK},\tilde{N},\mathrm{AD},C,T)$
1:	$IV \leftarrow \langle \tilde{N} \rangle_r \ 0^{n-r-1} 1$	1:	$IV \leftarrow \langle \tilde{N} \rangle_r \ 0^{n-r-1} 1$
2:	$L_M \leftarrow M _{\mathrm{B}}$	2:	$L_{\rm AD} \leftarrow {\rm AD} _{\rm B}$
3:	$\mu \leftarrow \lceil L_M / 16 \rceil$	3 :	$L_M \leftarrow C _{\mathrm{B}}$
4:	for $j = 1$ to μ do	4:	data $\leftarrow \mathrm{AD} \ C \ \langle L_{\mathrm{AD}} \rangle_{64} \ \langle L_M \rangle_{64}$
5:	$Z_i \leftarrow E(\text{EK}, IV + i)$	5:	$\mathrm{HK} \leftarrow E(\mathrm{EK}, 0^n)$
6:	$Z \leftarrow msb_{8L_M}(Z_1 \ \dots \ Z_\mu)$	6:	$T' \leftarrow \mathcal{H}(\mathrm{HK},\mathrm{data}) \oplus E(\mathrm{EK},IV)$
7:	$C \leftarrow M \oplus Z$	7:	if $T' \neq T$
8:	$L_{\mathrm{AD}} \leftarrow \mathrm{AD} _{\mathrm{B}}$	8:	$\mathbf{return} \perp$
9:	data $\leftarrow \operatorname{AD} \ C \ \langle L_{\operatorname{AD}} \rangle_{64} \ \langle L_M \rangle_{64}$	9:	$\mu \leftarrow \lceil L_M/16 \rceil$
10:	$\mathrm{HK} \leftarrow E(\mathrm{EK}, 0^n)$	10:	for $j = 1$ to μ do
11 :	$T \leftarrow \mathcal{H}(\mathrm{HK}, \mathrm{data}) \oplus E(\mathrm{EK}, IV)$	11:	$Z_i \leftarrow E(\mathrm{EK}, IV + i)$
12:	$\mathbf{return}\ (C,T)$	12:	$Z \leftarrow msb_{8L_M}(Z_1 \ \dots \ Z_\mu)$
		13:	$M \leftarrow C \oplus Z$
		14:	$\mathbf{return} \ M$

Figure 6: Algorithm of $CAU[E, \mathcal{H}]$.

Bounding output collisions. Let \mathcal{E}_6^{\dagger} be the event that $Z_i^p = Z_j^p$ for some $p \in [1..c]$ and $i, j \in [1..\xi_p]$ with $i \neq j$. Then

$$\Pr[\mathcal{E}_{6}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}] \le \sum_{p=1}^{c} {\binom{\xi_{p}}{2}} \frac{1}{2^{n}} \le \frac{\xi_{\max}}{2^{n+1}} \sum_{p=1}^{c} \xi_{p} \le \frac{n\ell^{2}q}{2^{n+1}}.$$
(50)

Getting a bound for $\Pr[\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},2} \mid \neg \mathcal{E}^{\dagger}_{\mathsf{bad},1}]$. Let $\mathcal{E}^{\dagger}_{\mathsf{bad},2}$ be the event $\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad},2}$. We observe that

$$\mathcal{E}_{\mathsf{bad},2}^{\dagger} \land \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger} \subseteq (\mathcal{E}_{5}^{\dagger} \land \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}) \lor (\mathcal{E}_{6}^{\dagger} \land \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}).$$

Thus, applying union-bound to Eqns. (49) and (50), we get

$$\Pr[\mathcal{E}_{\mathsf{bad},2}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}] \le \Pr[\mathcal{E}_{5}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}] + \Pr[\mathcal{E}_{6}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}] \le \frac{\ell q}{2^{n}} + \frac{n\ell^{2}q}{2^{n+1}}.$$
(51)

Getting a bound for $\Pr[\operatorname{Trs}(\mathcal{A}^{\mathcal{O}_0}) \in \mathcal{T}_{\mathsf{bad}}]$. From the definitions of $\mathcal{E}^{\dagger}_{\mathsf{bad},1}$, $\mathcal{E}^{\dagger}_{\mathsf{bad},2}$, and $\mathcal{T}_{\mathsf{bad}}$, and from Eqns. (48) and (51), we get

$$\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) \in \mathcal{T}_{\mathsf{bad}}\right] = \Pr\left[\mathcal{E}_{\mathsf{bad},1}^{\dagger} \lor \mathcal{E}_{\mathsf{bad},2}^{\dagger}\right]$$
$$= \Pr\left[\mathcal{E}_{\mathsf{bad},1}^{\dagger}\right] + \Pr\left[\mathcal{E}_{\mathsf{bad},2}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{bad},1}^{\dagger}\right]$$
$$\leq \frac{13\ell^{2}q}{2^{n-\lambda}} + \frac{\ell q}{2^{n}} + \frac{n\ell^{2}q}{2^{n+1}} \leq \frac{13\ell^{2}q}{2^{n-\lambda}} + \frac{n\ell^{2}q}{2^{n}}, \tag{52}$$

thus establishing Eqn. (32), and completing the proof of Lemma 11.

5 **Pencil**-based Key Derivation for GCM

In this section, we present an alternative to DNDK-GCM [Gue24a, Gue24b]. The idea of using a keyderivation function to derive the key of an AEAD from the input nonce and key has been used earlier

Pen	$cil\text{-}DK\text{-}CAU[\mathbf{U}, E, \mathcal{H}].Enc(\mathrm{rK}, \mathbf{N}, \mathrm{AD}, M)$
1:	$(\mathrm{EK}, \tilde{N}) \leftarrow msb_{\kappa+r}(\sharpPencil[\mathbf{U}, E](\mathrm{rK}, \mathbf{N}, 0^{\lambda}))$
2:	return $CAU[E, \mathcal{H}].Enc(\mathrm{EK}, \tilde{N}, \mathrm{AD}, M)$
Pen	$cil-DK-CAU[\mathbf{U}, E, \mathcal{H}].Dec(\mathrm{rK}, \mathbf{N}, \mathrm{AD}, C, T)$
1:	$(\mathrm{EK}, \tilde{N}) \leftarrow msb_{\kappa+r}(\sharpPencil[\mathbf{U}, E](\mathrm{rK}, \mathbf{N}, 0^{\lambda}))$
2:	return $CAU[E, \mathcal{H}].Dec(\mathrm{EK}, \tilde{N}, \mathrm{AD}, C, T)$

Figure 7: Algorithm of Pencil-DK-CAU $[\mathbf{U}, E, \mathcal{H}]$.

in designs like AES-GCM-SIV [GL17]. In DNDK-GCM the key-derivation function is DNDK, which derives the AES-GCM key from a 24-byte nonce and then proceeds to execute AES-GCM with the derived key and a fixed nonce 0⁹⁶. Our proposed new mode Pencil-DK-CAU (defined as a modification of CAU, the generalisation of AES-GCM) accepts a larger nonce like DNDK-GCM, with the added advantage that the nonce does not have to be randomly sampled.

5.1 The CAU mode

We first recall the AEAD mode CAU, which is a generalisation of GCM. Let $E : \{0,1\}^{\kappa} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with a κ -bit key and an *n*-bit output, and let $\mathcal{H} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be an *c*-AXU hash function with an *n*-bit hash key and an *n*-bit output. CAU uses a single κ -bit key EK, and generates the *n*-bit hash key as HK $\leftarrow E(\text{EK}, 0^n)$. It accepts an *r*-bit nonce \tilde{N} for some r < n, and sets the *n*-bit IV as $IV \leftarrow \langle \tilde{N} \rangle_r || 0^{n-r-1} 1$.

Encryption of an L_M -byte message M is done in counter mode, with the *i*-th block of the keystream being generated as E(EK, IV+i), and the final keystream block being truncated if needed to bring the total number of keystream bytes to L_M . The authentication tag is generated from the L_{AD} -byte associated data AD and L_M -byte ciphertext as $T \leftarrow \mathcal{H}(\text{HK}, \text{AD} \| C \| \langle L_{\text{AD}} \rangle_{64} \| \langle L_M \rangle_{64}) \oplus E(K, IV)$, and truncated down to the desired length.

Fig. 6 gives a formal description of the encryption and decryption algorithms of CAU. Note that AES-GCM is an instantiation of CAU, with E = AES, $\mathcal{H} = GHASH$, n = 128, r = 96, and $\kappa = 128$ or 256. In particular, this means that the construction we propose next is also applicable to AES-GCM.

Hoang et al. [HTT18] showed the following multi-user security bound for CAU in the ideal cipher model.

Theorem 5 ([HTT18], Theorem 3.1). For an adversary \mathcal{A} playing an mu-AEAD game against $CAU[E, \mathcal{H}]$, making $p \leq 2^{n-2}$ ideal cipher queries to E and q total construction queries with the total number of queried blocks not exceeding σ and the number of queried blocks for each user not exceeding B, and subject to the restriction that each nonce is repeated by at most d users, the advantage of \mathcal{A} satisfies the bound

$$\mathbf{Adv}_{\mathcal{CAU}[E,\mathcal{H}]}^{\textit{mu-AEAD}}(\mathcal{A}) \leq \frac{d(p+q) + n(p+q+\sigma)}{2^{\kappa}} + \frac{\sigma(2B+cn+3)}{2^{n}} + \frac{2q+1}{2^{2n}} + \frac{\sigma(\sigma+cnd)+2pq}{2^{\kappa+n}}.$$
(53)

5.2 The new key-derivation proposal using **#Pencil**

In our proposed mode Pencil-DK-CAU, instead of using a fixed 0^r as the nonce for CAU, a random r-bit nonce \tilde{N} is derived from the root key rK and the input nonce N in addition to the encryption key. This

modification has the effect of reducing the number of users who repeat the same nonce (the quantity d in Theorem 5).

Pencil-DK-CAU[U, E, \mathcal{H}] works as follows: it uses a 4κ -bit root key rK := (K_1, \ldots, K_4) (where κ is the key-length of E and hence of $\mathsf{CAU}[E, \mathcal{H}]$), and accepts a 2n-bit nonce N; for each fresh nonce N, it makes one call to $\sharp\mathsf{Pencil}[\mathbf{U}, E]$ with N and the output handle set to 0^{λ} , and truncates the $n\ell$ -bit output to $\kappa + r$ bits (assuming $\kappa + r \leq n\ell$). This output is parsed as (EK, \tilde{N}), which become respectively the encryption key and nonce in the ensuing call to the appropriate interface of $\mathsf{CAU}[E, \mathcal{H}]$, with the rest of the inputs to Pencil -DK-CAU passed on untouched. Fig. 7 gives a concise formal definition of the encryption and decryption functions of Pencil -DK-CAU.

We show the following result for Pencil-DK-CAU[$\mathbf{U}, E, \mathcal{H}$].

Theorem 6. For an AEAD adversary \mathcal{A} playing against Pencil-DK-CAU[U, E, \mathcal{H}], making $p \leq 2^{n-2}$ ideal cipher queries to E and $q \leq 2^{r-1}$ total construction queries with the total number of queried blocks not exceeding σ and the number of queried blocks for each nonce not exceeding B, we can find—one, an mu-AEAD adversary \mathcal{A}' playing against CAU[E, \mathcal{H}], making p ideal cipher queries to E and q total construction queries with the total number of queried blocks not exceeding σ and the number of queried blocks not exceeding σ and the number of queried blocks for each nonce is repeated by at most q users; and two, a PRF adversary playing against $\text{Pencil}[\mathbf{U}, E]$, making p ideal cipher queries to E and q construction queries;—such that the advantage of \mathcal{A} satisfies the bound

$$\mathbf{Adv}_{Pencil-DK-CAU[\mathbf{U},E,\mathcal{H}]}^{AEAD}(\mathcal{A}) \leq \mathbf{Adv}_{CAU[E,\mathcal{H}]}^{mu-AEAD}(\mathcal{A}') + \mathbf{Adv}_{\sharp Pencil[\mathbf{U},E]}^{PRF}(\mathcal{B}) + \frac{4(p+q)}{2^{\kappa}} + \frac{q}{2^{n}}.$$
(54)

The following Corollary to Theorem 6 immediately follows from the bounds in Theorems 4 and 5.

Corollary 1. For an AEAD adversary \mathcal{A} playing against Pencil-DK-CAU[U, \mathcal{E}, \mathcal{H}], making $p \leq 2^{n-2}$ ideal cipher queries to \mathcal{E} and $q \leq 2^{r-1}$ total construction queries with the total number of queried blocks not exceeding σ and the number of queried blocks for each nonce not exceeding \mathcal{B} , we can find three PRP-adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ each making at most q queries to its oracle and a PRP-adversary \mathcal{B}_4 making at most $q(\ell + 1)$ queries to its oracle such that

$$\mathbf{Adv}_{Pencil-DK-CAU[\mathbf{U},E,\mathcal{H}]}^{AEAD}(\mathcal{A}) \leq \frac{13\ell^2 q}{2^{n-\lambda}} + \frac{n\ell^2 q}{2^n} + \sum_{i=1}^4 \mathbf{Adv}_E^{PRP}(\mathcal{B}_i) + \frac{4(p+q)}{2^{\kappa}} + \frac{q}{2^n} + \frac{n(p+q) + n(p+q+\sigma)}{2^{\kappa}} + \frac{\sigma(2B+cn+3)}{2^n} + \frac{2q+1}{2^{2n}} + \frac{\sigma(\sigma+cn^2) + 2pq}{2^{\kappa+n}}.$$
 (55)

Proof (of Theorem 6). We prove the claimed bound with a sequence of game hops. In game \mathcal{G}_0 , \mathcal{A} plays against Pencil-DK-CAU[U, E, \mathcal{H}], which is the real world in the AEAD game.

In game \mathcal{G}_1 , the construction queries of \mathcal{A} are answered by Pencil-DK-CAU[$\mathbf{U}, E'/E, \mathcal{H}$], where two independent ideal ciphers E' and E are used in the \sharp Pencil portion and the CAU portion respectively (see Fig. 8), while the ideal cipher queries continue to be answered by E. This game is identical to the game against Pencil-DK-CAU[$\mathbf{U}, E, \mathcal{H}$] unless one of the p ideal cipher query keys or q encryption keys passed to CAU collide with one of the four keys in \sharp Pencil's root key. Since this involves a collision between at most p + q keys on one side and 4 keys on the other, we have

$$\left| \Pr[\mathcal{A}^{\mathcal{G}_0} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_1} \Rightarrow 1] \right| \le \frac{4(p+q)}{2^{\kappa}}.$$
(56)

Pen	$cil\text{-}DK\text{-}CAU[\mathbf{U},E'/E,\mathcal{H}].Enc(\mathrm{rK},\mathbf{N},\mathrm{AD},M)$
1:	$(\mathrm{EK}, \tilde{N}) \leftarrow msb_{\kappa+r}(\sharpPencil[\mathbf{U}, E'](\mathrm{rK}, \mathbf{N}, 0^{\lambda}))$
2:	return $CAU[E, \mathcal{H}].Enc(\mathrm{EK}, \tilde{N}, \mathrm{AD}, M)$
Pen	cil-DK-CAU[U $E'/E \mathcal{H}$] Dec(rK N AD $C \mathcal{T}$)
1:	$\frac{(\mathrm{EK}, \tilde{N}) \leftarrow msb_{\kappa+r}(\sharpPencil[\mathbf{U}, E'](\mathrm{rK}, \mathbf{N}, 0^{\lambda}))}{(\mathrm{EK}, \tilde{N}) \leftarrow msb_{\kappa+r}(\sharpPencil[\mathbf{U}, E'](\mathrm{rK}, \mathbf{N}, 0^{\lambda}))}$

Figure 8: The hybrid Pencil-DK-CAU $[\mathbf{U}, E'/E, \mathcal{H}]$ game.

In game \mathcal{G}_2 , the \sharp Pencil layer is dropped, and instead, for each unique nonce \mathbf{R} , an ℓ -block random string is directly sampled as $\mathbf{Z} \leftarrow \{0,1\}^{\ell n}$. CAU is called with $(\mathrm{EK}, \tilde{N}) \leftarrow \mathsf{msb}_{\kappa+r}(\mathbf{Z})$. Consider a PRF adversary \mathcal{B} against \sharp Pencil $[\mathbf{U}, E']$, which simulates \mathcal{A} , defined as follows: on receiving an encryption query $(\mathbf{N}, \mathrm{AD}, M)$ from \mathcal{A} , \mathcal{B} queries its own oracle with $(\mathbf{N}, 0^{\lambda})$, and receives a response \mathbf{Z} ; it then sets $(\mathrm{EK}, \tilde{N}) \leftarrow \mathsf{msb}_{\kappa+r}(\mathbf{Z})$, and returns $\mathsf{CAU}[E, \mathcal{H}].\mathsf{Enc}(\mathrm{EK}, \tilde{N}, \mathrm{AD}, M)$ to \mathcal{A} ; on receiving an decryption query $(\mathbf{N}, \mathrm{AD}, C, T)$ from \mathcal{A} , \mathcal{B} again queries its own oracle with $(\mathbf{N}, 0^{\lambda})$, and receives a response \mathbf{Z} ; it then sets $(\mathrm{EK}, \tilde{N}) \leftarrow \mathsf{msb}_{\kappa+r}(\mathbf{Z})$, and returns $\mathsf{CAU}[E, \mathcal{H}].\mathsf{Dec}(\mathrm{EK}, \tilde{N}, \mathrm{AD}, C, T)$ to \mathcal{A} . Then we have

$$\left| \Pr[\mathcal{A}^{\mathcal{G}_1} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_2} \Rightarrow 1] \right| \le \mathbf{Adv}_{\sharp\mathsf{Pencil}[\mathbf{U}, E']}^{\mathsf{PRF}}(\mathcal{B}).$$
(57)

In game \mathcal{G}_3 , (EK, \tilde{N}) is directly sampled as (EK, \tilde{N}) \leftarrow $\{0, 1\}^{\kappa+r}$, instead of first sampling a full chunk **Z**. Since the distribution of (EK, \tilde{N}) is identical here to that in \mathcal{G}_2 , we have

$$\left| \Pr[\mathcal{A}^{\mathcal{G}_2} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_3} \Rightarrow 1] \right| = 0.$$
(58)

In game \mathcal{G}_4 , the CAU layer is dropped; the encryption queries are answered uniform random strings of the requested length, and decryption queries are always answered with \perp . Consider an mu-AEAD adversary \mathcal{A}'' against CAU[E, \mathcal{H}]. \mathcal{A}'' simulates \mathcal{A} , and associates a unique user number $i(\mathbf{N})$ with each unique nonce \mathbf{N} queried by \mathcal{A} (e.g., by storing the nonces in a table and assigning the corresponding row number to i). Further, for each user number i, \mathcal{A}'' samples a uniform random r-bit nonce $\tilde{N}_i \leftarrow \{0, 1\}^r$. On receiving an encryption query ($\mathbf{N}, \mathrm{AD}, \mathcal{M}$) from $\mathcal{A}, \mathcal{A}''$ queries its own encryption oracle with ($i(\mathbf{N}), \tilde{N}_{i(\mathbf{N})}, \mathrm{AD}, \mathcal{M}$), and passes on the response to \mathcal{A} ; on receiving a decryption query ($\mathbf{N}, \mathrm{AD}, \mathcal{C}, \mathcal{T}$) from \mathcal{A}, \mathcal{A} queries its own decryption oracle with ($i(\mathbf{N}), \tilde{N}_{i(\mathbf{N})}, \mathrm{AD}, \mathcal{C}, \mathcal{T}$), and passes on the response to \mathcal{A} . It is clear that as long as \mathcal{A} 's encryption queries are nonce-respecting, \mathcal{A}'' 's encryption queries are also nonce-respecting. At the end of the game, \mathcal{A}'' copies the final output bit of \mathcal{A} . Then we have

$$\left| \Pr[\mathcal{A}^{\mathcal{G}_3} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_4} \Rightarrow 1] \right| \leq \mathbf{Adv}_{\mathsf{CAU}[E,\mathcal{H}]}^{\mathsf{mu-AEAD}}(\mathcal{A}'').$$
(59)

Next consider an adversary \mathcal{A}' which behaves identically to the adversary \mathcal{A}'' , except after sampling each \tilde{N}_i , it counts the number $\nu(\tilde{N}_i)$ of previous users i' with $\tilde{N}_{i'} = \tilde{N}_i$; if $\nu(\tilde{N}_i) \leq n$, it sets \tilde{N}_i to the lexicographically smallest $\tilde{N} \in \{0, 1\}^r$ such that $\nu(\tilde{N}) \leq n$, and continues as \mathcal{A}'' does. Let \mathcal{E} be the event that there is an (n + 1)-multicollision on the r-bit nonces. As long as $q \leq 2^{r-1}$, we have

$$\Pr[\mathcal{E}] \le {\binom{q}{n+1}} \left(\frac{1}{2^r}\right)^n \le q \left(\frac{q}{2^r}\right)^n \le \frac{q}{2^n}.$$
(60)

We observe that \mathcal{A}' and \mathcal{A}'' are identical unless \mathcal{E} happens. Thus, from Eqn. (60), we have

$$\mathbf{Adv}_{\mathsf{CAU}[E,\mathcal{H}]}^{\mathsf{mu-AEAD}}(\mathcal{A}'') \leq \mathbf{Adv}_{\mathsf{CAU}[E,\mathcal{H}]}^{\mathsf{mu-AEAD}}(\mathcal{A}') + \frac{q}{2^n}.$$
(61)

Plugging Eqn. (61) in Eqn. (59) yields

$$\left|\Pr[\mathcal{A}^{\mathcal{G}_3} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_4} \Rightarrow 1]\right| \le \mathbf{Adv}_{\mathsf{CAU}[E,\mathcal{H}]}^{\mathsf{mu-AEAD}}(\mathcal{A}') + \frac{q}{2^n}.$$
(62)

The game \mathcal{G}_4 is identical to the ideal world of the AEAD game. Thus, we have

$$\mathbf{Adv}_{\mathsf{Pencil-DK-CAU}[\mathbf{U}, E, \mathcal{H}]}^{\mathsf{AEAD}}(\mathcal{A}) = \left| \Pr[\mathcal{A}^{\mathcal{G}_0} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_4} \Rightarrow 1] \right| \\ \leq \left| \Pr[\mathcal{A}^{\mathcal{G}_0} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_1} \Rightarrow 1] \right| \\ + \left| \Pr[\mathcal{A}^{\mathcal{G}_1} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_2} \Rightarrow 1] \right| \\ + \left| \Pr[\mathcal{A}^{\mathcal{G}_2} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_3} \Rightarrow 1] \right| \\ + \left| \Pr[\mathcal{A}^{\mathcal{G}_3} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{G}_4} \Rightarrow 1] \right|.$$
(63)

Plugging in the bounds from Eqns. (56), (57), (58), and (62) in Eqn. (63) completes the proof. \Box

References

- [AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, November 2001. (Cited on p. 3.)
- [BBN22] Arghya Bhattacharjee, Ritam Bhaumik, and Mridul Nandi. Offset-based BBB-secure tweakable block-ciphers with updatable caches. In Takanori Isobe and Santanu Sarkar, editors, *INDOCRYPT 2022*, volume 13774 of *LNCS*, pages 171–194. Springer, Cham, December 2022. (Cited on pp. 5 and 10.)
- [BCF⁺24] Ritam Bhaumik, André Chailloux, Paul Frixons, Bart Mennink, and María Naya-Plasencia. Block cipher doubling for a post-quantum world. *IACR Communications in Cryptology*, 1(3), 2024. (Cited on p. 10.)
- [BGK99] Mihir Bellare, Oded Goldreich, and Hugo Krawczyk. Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier. In Michael J. Wiener, editor, CRYPTO'99, volume 1666 of LNCS, pages 270–287. Springer, Berlin, Heidelberg, August 1999. (Cited on pp. 3 and 4.)
- [BHI⁺23] Zhenzhen Bao, Seongha Hwang, Akiko Inoue, ByeongHak Lee, Jooyoung Lee, and Kazuhiko Minematsu. XOCB: Beyond-birthday-bound secure authenticated encryption mode with rateone computation. In Carmit Hazay and Martijn Stam, editors, EUROCRYPT 2023, Part IV, volume 14007 of LNCS, pages 532–561. Springer, Cham, April 2023. (Cited on p. 5.)
- [BKR98] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. In Kaisa Nyberg, editor, EUROCRYPT'98, volume 1403 of LNCS, pages 266–280. Springer, Berlin, Heidelberg, May / June 1998. (Cited on p. 3.)
- [BR17] Andrej Bogdanov and Alon Rosen. Pseudorandom functions: Three decades later. Cryptology ePrint Archive, Report 2017/652, 2017. (Cited on p. 3.)
- [BT16] Mihir Bellare and Björn Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part I, volume 9814 of LNCS, pages 247–276. Springer, Berlin, Heidelberg, August 2016. (Cited on p. 5.)
- [CDN⁺23] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha. Proof of mirror theory for a wide range of ξ_{max} . In Carmit Hazay and Martijn Stam, editors, *EURO-CRYPT 2023, Part IV*, volume 14007 of *LNCS*, pages 470–501. Springer, Cham, April 2023. (*Cited on pp. 10 and 11.*)
- [CLL19] Wonseok Choi, ByeongHak Lee, and Jooyoung Lee. Indifferentiability of truncated random permutations. In Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Part I, volume 11921 of LNCS, pages 175–195. Springer, Cham, December 2019. (Cited on p. 3.)
- [CLL24] Wonseok Choi, Jooyoung Lee, and Yeongmin Lee. Toward full n-bit security and nonce misuse resistance of block cipher-based macs. In Kai-Min Chung and Yu Sasaki, editors, Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IX, volume 15492 of Lecture Notes in Computer Science, pages 251–279. Springer, 2024. (Cited on p. 10.)

- [CLLL21] Wonseok Choi, ByeongHak Lee, Jooyoung Lee, and Yeongmin Lee. Toward a fully secure authenticated encryption scheme from a pseudorandom permutation. In Mehdi Tibouchi and Huaxiong Wang, editors, ASIACRYPT 2021, Part III, volume 13092 of LNCS, pages 407–434. Springer, Cham, December 2021. (Cited on p. 5.)
- [CLP15] Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin. The indistinguishability of the XOR of k permutations. In Carlos Cid and Christian Rechberger, editors, FSE 2014, volume 8540 of LNCS, pages 285–302. Springer, Berlin, Heidelberg, March 2015. (Cited on p. 10.)
- [CS14] Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, Berlin, Heidelberg, May 2014. (*Cited on p. 9.*)
- [CS16] Benoît Cogliati and Yannick Seurin. EWCDM: An efficient, beyond-birthday secure, noncemisuse resistant MAC. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part I, volume 9814 of LNCS, pages 121–149. Springer, Berlin, Heidelberg, August 2016. (Cited on p. 3.)
- [DHT17] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In Jonathan Katz and Hovav Shacham, editors, CRYPTO 2017, Part III, volume 10403 of LNCS, pages 497–523. Springer, Cham, August 2017. (Cited on p. 3.)
- [DNS22] Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of Mirror Theory for $\xi_{\text{max}} = 2$. *IEEE Trans. Inf. Theory*, 68(9):6218–6232, 2022. (Cited on p. 10.)
- [GBJ⁺23] Aldo Gunsing, Ritam Bhaumik, Ashwin Jha, Bart Mennink, and Yaobin Shen. Revisiting the indifferentiability of the sum of permutations. In Helena Handschuh and Anna Lysyanskaya, editors, CRYPTO 2023, Part III, volume 14083 of LNCS, pages 628–660. Springer, Cham, August 2023. (Cited on p. 3.)
- [GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In 25th FOCS, pages 464–479. IEEE Computer Society Press, October 1984. (Cited on p. 3.)
- [GL17] Shay Gueron and Yehuda Lindell. Better bounds for block cipher modes of operation via noncebased key derivation. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, ACM CCS 2017, pages 1019–1036. ACM Press, October / November 2017. (Cited on pp. 3 and 23.)
- [GM20] Aldo Gunsing and Bart Mennink. The summation-truncation hybrid: Reusing discarded bits for free. In Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO 2020, Part I, volume 12170 of LNCS, pages 187–217. Springer, Cham, August 2020. (Cited on p. 3.)
- [GM22] Lorenzo Grassi and Bart Mennink. Security of truncated permutation without initial value. In Shweta Agrawal and Dongdai Lin, editors, ASIACRYPT 2022, Part II, volume 13792 of LNCS, pages 620–650. Springer, Cham, December 2022. (Cited on p. 3.)
- [Gue24a] Shay Gueron. Double Nonce Derive Key AES-GCM (DNDK-GCM). Internet-Draft draftgueron-cfrg-dndkgcm-00, Internet Engineering Task Force, April 2024. Work in Progress. (Cited on pp. 3, 4, 6, and 22.)
- [Gue24b] Shay Gueron. Double-nonce-derive-key-gcm (dndk-gcm), 2024. Presented at the IACR Real World Crypto Symposium 2024. (Cited on pp. 3 and 22.)

- [HTT18] Viet Tung Hoang, Stefano Tessaro, and Aishwarya Thiruvengadam. The multi-user security of GCM, revisited: Tight bounds for nonce randomization. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, ACM CCS 2018, pages 1429–1440. ACM Press, October 2018. (Cited on pp. 6 and 23.)
- [IMV16] Tetsu Iwata, Bart Mennink, and Damian Vizár. CENC is optimally secure. Cryptology ePrint Archive, Report 2016/1087, 2016. (Cited on pp. 3, 4, and 10.)
- [Iwa06] Tetsu Iwata. New blockcipher modes of operation with beyond the birthday bound security. In Matthew J. B. Robshaw, editor, FSE 2006, volume 4047 of LNCS, pages 310–327. Springer, Berlin, Heidelberg, March 2006. (Cited on pp. 3 and 4.)
- [JN22] Ashwin Jha and Mridul Nandi. A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF. *Entropy*, 24(4):462, 2022. (*Cited on p. 9.*)
- [KCC⁺23] Panos Kampanakis, Matt Campagna, Eric Crocket, Adam Petcher, and Shay Gueron. Practical challenges with aes-gcm and the need for a new cipher. In *Third NIST Workshop on Block Cipher Modes of Operation*, 2023. (Cited on p. 3.)
- [MN17] Bart Mennink and Samuel Neves. Encrypted Davies-Meyer and its dual: Towards optimal security using mirror theory. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017*, *Part III*, volume 10403 of *LNCS*, pages 556–583. Springer, Cham, August 2017. (*Cited on pp. 3 and 10.*)
- [Nat25] National Institute of Standards and Technology. Pre-draft call for comments: GCM and GMAC block cipher modes of operation, Jan 2025. (*Cited on pp. 4 and 5.*)
- [Pat03] Jacques Patarin. Luby-Rackoff: 7 rounds are enough for 2n(1-epsilon)security. In Dan Boneh, editor, CRYPTO 2003, volume 2729 of LNCS, pages 513–529. Springer, Berlin, Heidelberg, August 2003. (Cited on p. 9.)
- [Pat06] Jacques Patarin. On linear systems of equations with distinct variables and small block size.
 In Dongho Won and Seungjoo Kim, editors, *ICISC 05*, volume 3935 of *LNCS*, pages 299–321.
 Springer, Berlin, Heidelberg, December 2006. (Cited on p. 9.)
- [Pat08] Jacques Patarin. A proof of security in O(2n) for the xor of two random permutations. In Reihaneh Safavi-Naini, editor, *ICITS 08*, volume 5155 of *LNCS*, pages 232–248. Springer, Berlin, Heidelberg, August 2008. (Cited on p. 10.)
- [Pat09] Jacques Patarin. The "coefficients H" technique (invited talk). In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, SAC 2008, volume 5381 of LNCS, pages 328–345. Springer, Berlin, Heidelberg, August 2009. (Cited on p. 9.)
- [Pat10a] Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. Cryptology ePrint Archive, Report 2010/287, 2010. (Cited on p. 10.)
- [Pat10b] Jacques Patarin. Transfinite cryptography. Cryptology ePrint Archive, Report 2010/001, 2010. (Cited on p. 9.)
- [ZHY18] Ping Zhang, Honggang Hu, and Qian Yuan. Close to Optimally Secure Variants of GCM. Secur. Commun. Networks, 2018:9715947:1–9715947:12, 2018. (Cited on p. 10.)

Appendix

A Deferred Proofs of Lemmas from Sec. 3

A.1 Proof of Lemma 1

The adversary \mathcal{A}' simulates \mathcal{A} , and simply passes the queries of \mathcal{A} to its own oracle and passes the oracles responses back to \mathcal{A} , and eventually replicates the output bit of \mathcal{A} .

The adversary \mathcal{B} also simulates \mathcal{A} . It first initialises an empty table In. On receiving a query $(h_{\text{in}}^{(i)}, h_{\text{out}}^{(i)})$ from \mathcal{A} , \mathcal{B} checks whether $h_{\text{in}}^{(i)} \in \text{In}$; if yes, it sets $\mathbf{R}^{(i)} \leftarrow \text{In}[h_{\text{in}}^{(i)}]$; otherwise, it samples $\mathbf{R}^{(i)} \leftarrow \mathbb{GF}(2^{2n-2\lambda})$, and sets $\ln[h_{\text{in}}^{(i)}] \leftarrow \mathbf{R}^{(i)}$. Next, \mathcal{B} computes $\tilde{\mathbf{X}}^{(i)} \leftarrow \mathbf{U} \cdot \mathbf{R}^{(i)}$, and sends the $(\ell + 1)$ queries $\tilde{X}_{0}^{(i)} || \langle h_{\text{out}}^{(i)} \rangle_{\lambda}$, $\dots, \tilde{X}_{\ell}^{(i)} || \langle h_{\text{out}}^{(i)} \rangle_{\lambda}$ to its own oracle, to receive the respective responses $Y_{0}^{(i)}, \dots, Y_{\ell}^{(i)}$; then it computes $Z_{j}^{(i)} \leftarrow Y_{0}^{(i)} \oplus Y_{j}^{(i)}$ for each $j \in [0..\ell]$ and returns $(\mathbf{R}^{(i)}, \mathbf{Z}^{(i)})$ to \mathcal{A} ; at the end of the game \mathcal{B} also replicates the output bit of \mathcal{A} .

It is easy to verify that \mathcal{A}' makes q queries and \mathcal{B} makes $(\ell + 1)q$ queries, so it remains to show the bound in Eqn. (11). Let $F^* : \{0,1\}^{2n-\lambda} \to \{0,1\}^{\ell n}$ be a uniform random function. Then from Eqn. (1) we have

$$\begin{aligned} \mathbf{Adv}_{\mathsf{Pencil}[\mathbf{U},E]}^{\mathsf{wPRF}}(\mathcal{A}) &= \left| \Pr[\mathcal{A}^{\mathsf{Pencil}[\mathbf{U},E]} \Rightarrow 1] - \Pr[\mathcal{A}^{F^*} \Rightarrow 1] \right| \\ &= \left| \Pr[\mathcal{A}^{\mathsf{Pencil}[\mathbf{U},\pi^*]} \Rightarrow 1] - \Pr[\mathcal{A}^{F^*} \Rightarrow 1] \right| \\ &+ \Pr[\mathcal{A}^{\mathsf{Pencil}[\mathbf{U},E]} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathsf{Pencil}[\mathbf{U},\pi^*]} \Rightarrow 1] \right| \\ &= \left| \Pr[\mathcal{A}'^{\mathsf{Pencil}[\mathbf{U},\pi^*]} \Rightarrow 1] - \Pr[\mathcal{A}'^{F^*} \Rightarrow 1] \right| \\ &+ \Pr[\mathcal{B}^E \Rightarrow 1] - \Pr[\mathcal{B}^{\pi^*} \Rightarrow 1] \right| \\ &\leq \left| \Pr[\mathcal{A}'^{\mathsf{Pencil}[\mathbf{U},\pi^*]} \Rightarrow 1] - \Pr[\mathcal{A}'^{F^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}^E \Rightarrow 1] - \Pr[\mathcal{B}^{\pi^*} \Rightarrow 1] \right| \\ &= \left| \operatorname{Adv}_{\mathsf{Pencil}[\mathbf{U},\pi^*]}^{\mathsf{wPRF}}(\mathcal{A}') + \operatorname{Adv}_{E}^{\mathsf{PRP}}(\mathcal{B}), \end{aligned}$$

which establishes Eqn. (11), thus completing the proof.

A.2 Proof of Lemma 4

Fix a $tr = (\mathbf{R}, \mathbf{Z}, \mathbf{Y}) \in \mathcal{T}_{good}$. By definition of \mathcal{T}_{bad} , we know that $\Phi_{tr} := \Phi[\mathbf{A}_{r \times \ell q}, \mathbf{Z}]$ is a consistent mirror system and $\xi_{max}(tr) \leq n\ell$. First we observe that since the random nonce generation step doesn't depend on the oracle, we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};1\right)=\mathbf{R}\right]=\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};1\right)=\mathbf{R}\right]=\frac{1}{2^{2(n-\lambda)q}}.$$
(64)

For the rest of the transcript, we examine the real world and the ideal world separately. Since **A** has r rows, there must be r distinct values of $X_j^{(i)}$ in **X**. Since the corresponding outputs are sampled uniformly without replacement by π^* in the real world, we have

$$\Pr\left[\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};3\right)=\mathbf{Y}\mid\operatorname{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};1\right)=\mathbf{R}\right]=\frac{1}{(2^{n})_{r}}.$$
(65)

-	-	-	1

Finally, in the real world, \mathbf{Z} is determined from \mathbf{Y} , we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};2\right)=\mathbf{Z} \mid \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};1\right)=\mathbf{R}, \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};3\right)=\mathbf{Y}\right]=1.$$
(66)

From Eqns. (64), (65), and (66) we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = \mathsf{tr}\right] = \frac{1}{2^{2(n-\lambda)q}(2^{n})_{r}}.$$
(67)

Next we turn our attention to the ideal world. Here, $(\mathcal{A}^{\mathcal{O}_0}; 2)$ is sampled first, and independently of $(\mathcal{A}^{\mathcal{O}_0}; 1)$, so we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};2\right)=\mathbf{Y} \mid \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};1\right)=\mathbf{R}\right]=\frac{1}{2^{n\ell q}}.$$
(68)

In the final step, sampling $(\mathcal{A}^{\mathcal{O}_0}; 3)$ is equivalent to a uniform sampling from $\Gamma(\Phi_{\mathsf{tr}})$, so we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};3\right)=\mathbf{Y}\mid\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};1\right)=\mathbf{R},\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};2\right)=\mathbf{Y}\right]=\frac{1}{|\Gamma(\Phi_{\mathsf{tr}})|}.$$
(69)

From Eqns. (64), (68), and (69) we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = \mathsf{tr}\right] = \frac{1}{2^{2(n-\lambda)q+n\ell q}|\Gamma(\Phi_{\mathsf{tr}})|}.$$
(70)

To complete the proof, we need to find an appropriate bound for the ratio of $\Pr[\operatorname{Trs} (\mathcal{A}^{\mathcal{O}_1}) = \operatorname{tr}]$ and $\Pr[\operatorname{Trs} (\mathcal{A}^{\mathcal{O}_0}) = \operatorname{tr}]$. From Eqns. (67) and (70) we have

$$\frac{\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = \mathsf{tr}\right]}{\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = \mathsf{tr}\right]} = \frac{2^{n\ell q} |\Gamma(\Phi_{\mathsf{tr}})|}{(2^{n})_{r}}.$$
(71)

As the final step in the proof, we want to bound $|\Gamma(\Phi_{tr})|$ by applying Theorem 2. We already know that Φ_{tr} is a consistent mirror system, so we just need to verify the conditions on $\xi_{\max}(tr)$. Using the bound $\xi_{\max}(tr) \leq n\ell$ and the assumptions $n^3\ell^2 + n\ell \leq 2^{n/2}$ and $n\ell^2q \leq 2^{n-4}$, we have

$$n\xi_{\max}(tr)^2 + \xi_{\max}(tr) \le n^3 \ell^2 + n\ell \le 2^{n/2},$$
(72)

and

$$12\ell q\xi_{\max}(\mathsf{tr}) \le 12n\ell^2 q \le 2^n.$$
(73)

Thus, all the conditions for Theorem 2 are satisfied, and applying this theorem gives

$$|\Gamma(\Phi_{\mathsf{tr}})| \ge \frac{(2^n)_r}{2^{n\ell q}}.\tag{74}$$

Substituting Eqn. (74) in Eqn. (71) completes the proof of Lemma 4.

A.3 Proof of Lemma 5

Eqn. (15) is equivalent to $\tilde{X}_{j'}^{(i)} = \tilde{X}_{j}^{(i)}$, which we can rewrite as

$$\mathbf{U}_{j'*}^{\mathsf{T}} \cdot \mathbf{R}^{(i)} = \mathbf{U}_{j*}^{\mathsf{T}} \cdot \mathbf{R}^{(i)}, \quad \text{or} \quad (\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}}) \cdot \mathbf{R}^{(i)} = 0.$$

Since **U** is locally non-degenerate, its rows are pairwise independent, which means in particular that $\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}} \neq 0$. Thus, $(\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}}) \cdot \mathbf{R}^{(i)}$ is distributed uniformly over $\mathbb{GF}(2^{n-\lambda})$, so that

$$\Pr\left[\left(\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}}\right) \cdot \mathbf{R}^{(i)} = 0\right] = \frac{1}{2^{n-\lambda}}.$$
(75)

There are q choices for i, and $\ell(\ell+1)/2$ choices for j, j', so applying union-bound to Eqn. (75) yields Eqn. (16).

A.4 Proof of Lemma 6

For Eqn. (17) to be satisfiable, we need $h_{\text{out}}^{(i_1)} = h_{\text{out}}^{(i_2)}$; then it reduces to $(\tilde{X}_{j_2}^{(i_2)}, \tilde{X}_{j'_2}^{(i_2)}) = (\tilde{X}_{j_1}^{(i_1)}, \tilde{X}_{j'_1}^{(i_1)})$, which we can rewrite as

$$(\mathbf{U}_{j_{2}*}, \mathbf{U}_{j_{2}'*})^{\mathsf{T}} \cdot \mathbf{R}^{(i_{2})} = (\mathbf{U}_{j_{1}*}, \mathbf{U}_{j_{1}'*})^{\mathsf{T}} \cdot \mathbf{R}^{(i_{1})}.$$
(76)

Since $\mathbf{U}_{j_{2*}}$ and $\mathbf{U}_{j'_{2*}}$ are independent, $(\mathbf{U}_{j_{2*}}, \mathbf{U}_{j'_{2*}})^{\intercal}$ is an invertible 2×2 matrix, so we can further rewrite Eqn. (76) as

$$\mathbf{R}^{(i_2)} = (\mathbf{U}_{j_2*}, \mathbf{U}_{j'_2*})^{\mathsf{T}-1} \cdot (\mathbf{U}_{j_1*}, \mathbf{U}_{j'_1*})^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)}.$$
(77)

Since $h_{\text{out}}^{(i_1)} = h_{\text{out}}^{(i_2)}$, $\mathbf{R}^{(i_2)}$ is sampled uniformly from $(\mathbb{GF}(2^{n-\lambda}))^2$, and independently of $\mathbf{R}^{(i_1)}$, we can write

$$\Pr[Eqn. (77)] = \frac{1}{2^{2n-2\lambda}}.$$
(78)

There are q(q-1)/2 choices for i_1, i_2 (since there's no restriction on how many times a suffix s can repeat), and $\ell^2(\ell+1)^2/4$ choices for j_1, j'_1, j_2, j'_2 , so applying union-bound to Eqn. (78) yields Eqn. (18).

A.5 Proof of Lemma 7

As before, for Eqn. (19) to hold, we must have $h_{out}^{(i_1)} = h_{out}^{(i_2)} = \cdots = h_{out}^{(i_{n+1})}$, so we can assume here that $\mathbf{R}^{(i_1)}, \mathbf{R}^{(i_2)}, \ldots, \mathbf{R}^{(i_{n+1})}$ are all independent and uniformly sampled from $\mathbb{GF}(2^{n-\lambda})$; then Eqn. (19) reduces to $(\tilde{X}_{j'_2}^{(i_2)}, \ldots, \tilde{X}_{j'_{n+1}}^{(i_{n+1})}) = (\tilde{X}_{j_1}^{(i_1)}, \ldots, \tilde{X}_{j_n}^{(i_n)})$, which we can rewrite as

$$(\mathbf{U}_{j_{2}^{\prime}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{2})}, \dots, \mathbf{U}_{j_{n+1}^{\prime}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{n+1})}) = (\mathbf{U}_{j_{1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{1})}, \dots, \mathbf{U}_{j_{n}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{n})}).$$
(79)

For any $k \in [1..n]$, let $\tilde{\mathcal{E}}[1, \ldots, k]$ denote the event $(\mathbf{U}_{j'_{2^*}}^{\mathsf{T}} \cdot \mathbf{R}^{(i_2)}, \ldots, \mathbf{U}_{j'_{k+1}^*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k+1})}) = (\mathbf{U}_{j_{1^*}}^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)}, \ldots, \mathbf{U}_{j'_{k+1}^*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_k)})$. Let us fix a $k \in [1..n]$. Since $\mathbf{U}_{j'_{k+1}^*}$ is not a 0 vector (by local non-degeneracy of \mathbf{U}), $\mathbf{U}_{j'_{k+1}^*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k+1})}$ is distributed uniformly on $\mathbb{GF}(2^{n-\lambda})$ and is independent of $\mathbf{R}^{(i_k)}$. Thus,

$$\Pr\left[\mathbf{U}_{j_{k+1}^{\prime}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k+1})} = \mathbf{U}_{j_{k}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k})} \mid \mathbf{R}^{(i_{k})}\right] = \frac{1}{2^{n-\lambda}}.$$
(80)

When $k \geq 2$, since the event $\mathbf{U}_{j'_{k+1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k+1})} = \mathbf{U}_{j_{k}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k})}$ is independent of $\mathbf{R}^{(i_{1})}, \ldots, \mathbf{R}^{(i_{k-1})}$, we can rewrite Eqn. (80) as

$$\Pr\left[\mathbf{U}_{j'_{k+1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k+1})} = \mathbf{U}_{j_{k}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k})} \mid \mathbf{R}^{(i_{1})}, \dots, \mathbf{R}^{(i_{k})}\right] = \frac{1}{2^{n-\lambda}}.$$

Moreover, since the above probability is not a function of $\mathbf{R}^{(i_1)}, \ldots, \mathbf{R}^{(i_k)}$, we also get the same probability when we condition on the event $\tilde{\mathcal{E}}[1, \ldots, k-1]$, so we have

$$\Pr\left[\mathbf{U}_{j_{k+1}^{\dagger}^{\star}}^{\dagger} \cdot \mathbf{R}^{(i_{k+1})} = \mathbf{U}_{j_{k}^{\star}}^{\dagger} \cdot \mathbf{R}^{(i_{k})} \mid \tilde{\mathcal{E}}[1, \dots, k-1]\right] = \frac{1}{2^{n-\lambda}}.$$
(81)

Since for any two events B_1 and B_2 , $\Pr[B_1 \cap B_2 | B_2] = \Pr[B_1 | B_2]$, we have from Eqn. (81) that

$$\Pr\left[\tilde{\mathcal{E}}[1,\ldots,k] \mid \tilde{\mathcal{E}}[1,\ldots,k-1]\right] = \frac{1}{2^{n-\lambda}}.$$
(82)

Writing out Eqn. (82) for each $k \in [1..n]$ and taking the product yields

$$\Pr\left[\tilde{\mathcal{E}}[1,\ldots,n]\right] = \frac{1}{2^{n(n-\lambda)}}.$$
(83)

The event $\tilde{\mathcal{E}}[1,\ldots,n]$ is exactly the event described in Eqns. (19) and (79). Since there are $(q)_{n+1}$ choices for i_1,\ldots,i_{n+1} (since they must all be distinct) and $(\ell+1)^{2n}$ choices for $j_1,\ldots,j_n,j'_2,\ldots,j'_{n+1}$, applying union-bound to Eqn. (83) gives

$$\Pr[\mathcal{E}_3] \le \frac{(q)_{n+1}(\ell+1)^{2n}}{2^{n(n-\lambda)}} \le \frac{q^{n+1}(\ell+1)^{2n}}{2^{n(n-\lambda)}} = q\left(\frac{(\ell+1)^2q}{2^{n-\lambda}}\right)^n \le \frac{q}{2^n}$$

where in the last inequality we use the assumption that $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$. This gives us the final bound of Eqn. (20).

A.6 Proof of Lemma 8

Again, for Eqn. (21) to hold, we must have $h_{out}^{(i_1)} = h_{out}^{(i_2)} = \cdots = h_{out}^{(i_k)}$, so we can assume that $\mathbf{R}^{(i_1)}, \mathbf{R}^{(i_2)}, \ldots, \mathbf{R}^{(i_k)}$ are all independent and uniformly sampled from $\mathbb{GF}(2^{n-\lambda})$; then Eqn. (21) reduces to

$$(\tilde{X}_{j'_2}^{(i_2)},\ldots,\tilde{X}_{j'_k}^{(i_k)},\tilde{X}_{j'_1}^{(i_1)}) = (\tilde{X}_{j_1}^{(i_1)},\ldots,\tilde{X}_{j_{k-1}}^{(i_{k-1})},\tilde{X}_{j_k}^{(i_k)}).$$

To bound the probability of this, we first focus on the last two indices, and swap the last term on either side to get the equation

$$(\tilde{X}_{j'_{k}}^{(i_{k})}, \tilde{X}_{j_{k}}^{(i_{k})}) = (\tilde{X}_{j_{k-1}}^{(i_{k-1})}, \tilde{X}_{j'_{1}}^{(i_{1})}).$$

$$(84)$$

We can rewrite Eqn. (84) as

$$(\mathbf{U}_{j'_{k}*},\mathbf{U}_{j_{k}*})^{\mathsf{T}}\cdot\mathbf{R}^{(i_{k})} = (\mathbf{U}_{j_{k-1}*}^{\mathsf{T}}\cdot\mathbf{R}^{(i_{k-1})},\mathbf{U}_{j'_{1}*}^{\mathsf{T}}\cdot\mathbf{R}^{(i_{1})})^{\mathsf{T}},$$

and since $(\mathbf{U}_{j'_k*}, \mathbf{U}_{j_k*})^{\mathsf{T}}$ is invertible, this becomes

$$\mathbf{R}^{(i_k)} = (\mathbf{U}_{j'_k*}, \mathbf{U}_{j_k*})^{\mathsf{T}-1} \cdot (\mathbf{U}_{j_{k-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k-1})}, \mathbf{U}_{j'_1*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)})^{\mathsf{T}}.$$

Let $(u, v)^{\mathsf{T}}$ denote $(\mathbf{U}_{j'_k*}, \mathbf{U}_{j_k*})^{\mathsf{T}-1} \cdot (\mathbf{U}_{j_{k-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k-1})}, \mathbf{U}_{j'_1*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)})^{\mathsf{T}}$. Since $\mathbf{R}^{(i_k)}$ is sampled uniformly from $(\mathbb{GF}(2^{n-\lambda}))^2$ and is independent of $\mathbf{R}^{(i_1)}, \ldots, \mathbf{R}^{(i_{k-1})}$, we have

$$\Pr\left[\mathbf{R}^{(i_k)} = (u, v)^{\mathsf{T}} \mid \mathbf{R}^{(i_1)}, \dots, \mathbf{R}^{(i_{k-1})}\right] = \frac{1}{2^{2n-2\lambda}}$$

Arguing as before Eqn. (81), we get

$$\Pr\left[\mathbf{R}^{(i_k)} = (u, v)^{\mathsf{T}} \mid \tilde{\mathcal{E}}[1, \dots, k-2]\right] = \frac{1}{2^{2n-2\lambda}}.$$
(85)

Taking k - 2 instead of n in the derivation of Eqn. (83) gives

$$\Pr\left[\tilde{\mathcal{E}}[1,...,k-2]\right] = \frac{1}{2^{(n-\lambda)(k-2)}}.$$
(86)

We observe that Eqn. (21) is exactly the conjunction of the events $\mathbf{R}^{(i_k)} = (u, v)^{\intercal}$ and $\tilde{\mathcal{E}}[1, \ldots, k-2]$. Thus, taking the product of Eqns. (85) and (86) gives

$$\Pr\left[Eqn.\ (21)\right] = \frac{1}{2^{(n-\lambda)k}}.$$
(87)

Since there are $(q)_k$ choices for i_1, \ldots, i_k and $(\ell+1)^{2k}$ choices for $j_1, \ldots, j_n, j'_1, \ldots, j'_n$, applying union-bound to Eqn. (87) gives

$$\Pr[\mathcal{E}_{4,k}] \le \frac{(q)_k (\ell+1)^{2k}}{2^{(n-\lambda)k}} \le \frac{q^k (\ell+1)^{2k}}{2^{(n-\lambda)k}} = \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^k.$$
(88)

We recall that \mathcal{E}_4 denotes the event $\mathcal{E}_{4,3} \lor \cdots \lor \mathcal{E}_{4,n}$. Then by Eqn. (88) and union-bound we have

$$\Pr[\mathcal{E}_4] \le \sum_{k=3}^n \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^k = \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^3 \cdot \sum_{k=0}^{n-3} \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^k.$$
(89)

Using the assumption that $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$, we can bound Eqn. (89) as

$$\Pr[\mathcal{E}_4] \le \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^3 \cdot \sum_{k=0}^{n-3} \left(\frac{1}{2}\right)^k \le 2\left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^3,$$

which establishes the bound in Eqn. (22).

B Deferred Proofs of Lemmas from Sec. 4

B.1 Proof of Lemma 9

The adversary \mathcal{A}' simulates \mathcal{A} , and simply passes the queries of \mathcal{A} to its own oracle and passes the oracles responses back to \mathcal{A} , and eventually replicates the output bit of \mathcal{A} .

The adversary \mathcal{B}_1 also simulates \mathcal{A} . It initially samples three random keys $K_2, K_3, K_4 \leftarrow \{0, 1\}^n$. On receiving a query $(\mathbf{N}^{(i)}, h_{\text{out}}^{(i)})$ from $\mathcal{A}, \mathcal{B}_1$ first queries $N_2^{(i)}$ to its own oracle to receive $J^{(i)}$ as response; it then computes $\tilde{\mathbf{X}}^{(i)}$ as follows: $\mathbf{W}^{(i)} := (W_1^{(i)}, W_2^{(i)})^{\intercal} \leftarrow (\frac{1}{1}\frac{1}{2}) \cdot (N_1^{(i)}, J^{(i)})^{\intercal}, R_1^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(E(K_2, W_1^{(i)})),$ $R_2^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(E(K_3, W_2^{(i)})), \tilde{\mathbf{X}}^{(i)} \leftarrow \mathbf{U} \cdot \mathbf{R}^{(i)}$. Next, for each $j \in [0..\ell], \mathcal{B}_1$ computes $Y_j^{(i)} \leftarrow E(K_4, \tilde{X}_j^{(i)})$ and $Z_j^{(i)} \leftarrow Y_0^{(i)} \oplus Y_j^{(i)}$, and returns $\mathbf{Z}^{(i)}$ to \mathcal{A} . At the end of the game \mathcal{B}_1 also replicates the output bit of \mathcal{A} .

The adversary \mathcal{B}_2 also simulates \mathcal{A} . It initially samples one random permutation $\pi_1^* \leftarrow S_{2^n}$, and two random keys $K_3, K_4 \leftarrow \{0,1\}^n$. On receiving a query $(\mathbf{N}^{(i)}, h_{out}^{(i)})$ from $\mathcal{A}, \mathcal{B}_2$ first computes $J^{(i)} \leftarrow \pi_1^*(N_2^{(i)})$, and $\mathbf{W}^{(i)} := (W_1^{(i)}, W_2^{(i)})^{\intercal} \leftarrow (\frac{1}{1}\frac{1}{2}) \cdot (N_1^{(i)}, J^{(i)})^{\intercal}$. It then queries $W_1^{(i)}$ to its own oracle and truncates the response to $n - \lambda$ bits to get $R_1^{(i)}$, and computes $R_2^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(E(K_3, W_2^{(i)}))$ and $\tilde{\mathbf{X}}^{(i)} \leftarrow \mathbf{U} \cdot \mathbf{R}^{(i)}$. Next, for each $j \in [0..\ell]$, \mathcal{B}_2 computes $Y_j^{(i)} \leftarrow E(K_4, \tilde{X}_j^{(i)})$ and $Z_j^{(i)} \leftarrow Y_0^{(i)} \oplus Y_j^{(i)}$, and returns $\mathbf{Z}^{(i)}$ to \mathcal{A} . At the end of the game \mathcal{B}_2 also replicates the output bit of \mathcal{A} .

The adversary \mathcal{B}_3 also simulates \mathcal{A} . It initially samples two random permutations $\pi_1^*, \pi_2^* \leftarrow S_{2^n}$, and one random key $K_4 \leftarrow \{0,1\}^n$. On receiving a query $(\mathbf{N}^{(i)}, h_{out}^{(i)})$ from $\mathcal{A}, \mathcal{B}_2$ first computes $J^{(i)} \leftarrow \pi_1^*(N_2^{(i)})$, and $\mathbf{W}^{(i)} := (W_1^{(i)}, W_2^{(i)})^{\mathsf{T}} \leftarrow (\frac{1}{1}\frac{1}{2}) \cdot (N_1^{(i)}, J^{(i)})^{\mathsf{T}}$. It then queries $W_2^{(i)}$ to its own oracle and truncates the response to $n - \lambda$ bits to get $R_2^{(i)}$, and computes $R_1^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(\pi_2^*(W_1^{(i)}))$ and $\tilde{\mathbf{X}}^{(i)} \leftarrow \mathbf{U} \cdot \mathbf{R}^{(i)}$. Next, for each $j \in [0..\ell]$, \mathcal{B}_3 computes $Y_j^{(i)} \leftarrow E(K_4, \tilde{X}_j^{(i)})$ and $Z_j^{(i)} \leftarrow Y_0^{(i)} \oplus Y_j^{(i)}$, and returns $\mathbf{Z}^{(i)}$ to \mathcal{A} . At the end of the game \mathcal{B}_3 also replicates the output bit of \mathcal{A} .

The adversary \mathcal{B}_4 also simulates \mathcal{A} . It first samples three random permutations $\pi_1^*, \pi_2^*, \pi_3^* \leftrightarrow S_{2^n}$. On receiving a query $(\mathbf{N}^{(i)}, h_{\text{out}}^{(i)})$ from $\mathcal{A}, \mathcal{B}_4$ first computes $\mathbf{R}^{(i)}$ as follows: $J^{(i)} \leftarrow \pi_1^*(N_2^{(i)}), \mathbf{W}^{(i)} := (W_1^{(i)}, W_2^{(i)})^{\mathsf{T}} \leftarrow (\frac{1}{1}\frac{1}{2}) \cdot (N_1^{(i)}, J^{(i)})^{\mathsf{T}}, R_1^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(\pi_2^*(W_1^{(i)})), R_2^{(i)} \leftarrow \mathsf{msb}_{n-\lambda}(\pi_3^*(W_2^{(i)}))$. Next, \mathcal{B}_4 computes $\tilde{\mathbf{X}}^{(i)} \leftarrow \mathbf{U} \cdot \mathbf{R}^{(i)}$, and sends the $(\ell + 1)$ queries $\tilde{X}_0^{(i)} ||\langle h_{\mathrm{out}}^{(i)} \rangle_{\lambda}, \ldots, \tilde{X}_{\ell}^{(i)} ||\langle h_{\mathrm{out}}^{(i)} \rangle_{\lambda}$ to its own oracle, to receive

the respective responses $Y_0^{(i)}, \ldots, Y_\ell^{(i)}$; then it computes $Z_j^{(i)} \leftarrow Y_0^{(i)} \oplus Y_j^{(i)}$ for each $j \in [0..\ell]$ and returns $\mathbf{Z}^{(i)}$ to \mathcal{A} ; at the end of the game \mathcal{B}_4 also replicates the output bit of \mathcal{A} .

It is easy to verify that \mathcal{A}' , \mathcal{B}_1 , \mathcal{B}_2 , and \mathcal{B}_3 make q queries each and \mathcal{B}_4 makes $(\ell + 1)q$ queries, so it remains to show the bound in Eqn. (30). For four random permutations $\pi_1^*, \ldots, \pi_4^* \leftarrow S_{2^n}$ and $\tilde{\pi}^* := (\pi_1^*, \ldots, \pi_4^*)$, define the following hybrids of \sharp Pencil:

- $\sharp \mathsf{Pencil}[\mathbf{U}, \tilde{\pi}^*/E : 1/3]$ uses three keys $K_2, K_3, K_4 \leftarrow \{0, 1\}^n$, and encrypts $N_2^{(i)}, W_1^{(i)}, W_2^{(i)}, W_1^{(i)}, W_2^{(i)}, M_1^{(i)}, W_2^{(i)}, M_1^{(i)}, W_2^{(i)}, M_1^{(i)}, W_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_2^{(i)}, M_1^{(i)}, M_2^{(i)}, M_$
- $\sharp \mathsf{Pencil}[\mathbf{U}, \tilde{\pi}^*/E : 2/2]$ uses two keys $K_3, K_4 \leftarrow \{0, 1\}^n$, and encrypts $N_2^{(i)}, W_1^{(i)}, W_2^{(i)}$, and $\{X_j^{(i)} \mid j \in [0, \ell]\}$ using $\pi_1^*, \pi_2^*, E(K_3, \cdot)$, and $E(K_4, \cdot)$ respectively;
- $\sharp \mathsf{Pencil}[\mathbf{U}, \tilde{\pi}^*/E : 3/1]$ uses one key $K_4 \leftarrow \{0, 1\}^n$, and encrypts $N_2^{(i)}, W_1^{(i)}, W_2^{(i)}$, and $\{X_j^{(i)} \mid j \in [0..\ell]\}$ using $\pi_1^*, \pi_2^*, \pi_1^*$, and $E(K_4, \cdot)$ respectively.

Let $F^*: \{0,1\}^{2n+\lambda} \to \{0,1\}^{\ell n}$ be a uniform random function. Then from Eqn. (1) we have

$$\begin{split} \mathbf{Adv}_{\sharp \text{Percil}[\mathbf{U},E]}^{\text{PRF}}(\mathcal{A}) &= \left| \Pr[\mathcal{A}^{\sharp \text{Pencil}[\mathbf{U},E]} \Rightarrow 1] - \Pr[\mathcal{A}^{F^*} \Rightarrow 1] \right| \\ &= \left| \Pr[\mathcal{A}^{\sharp \text{Pencil}[\mathbf{U},\bar{\pi}^*]} \Rightarrow 1] - \Pr[\mathcal{A}^{F^*} \Rightarrow 1] \\ &+ \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:3/1]} \Rightarrow 1] - \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*]} \Rightarrow 1] \\ &+ \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:2/2]} \Rightarrow 1] - \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:3/1]} \Rightarrow 1] \\ &+ \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:1/3]} \Rightarrow 1] - \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:2/2]} \Rightarrow \\ &+ \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:1/3]} \Rightarrow 1] - \Pr[\mathcal{A}^{\text{Pencil}[\mathbf{U},\bar{\pi}^*/E:1/3]} \Rightarrow 1] \right| \\ &= \left| \Pr[\mathcal{A}^{\prime\text{Pencil}[\mathbf{U},\bar{\pi}^*]} \Rightarrow 1] - \Pr[\mathcal{A}^{\prime F^*} \Rightarrow 1] \\ &+ \Pr[\mathcal{B}_{1}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{1}^{\pi^*} \Rightarrow 1] \\ &+ \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{2}^{\pi^*} \Rightarrow 1] \\ &+ \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \\ &+ \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{1}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{1}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{1}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{1}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{1}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{1}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{1}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{1}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{1}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{2}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{3}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow 1] - \Pr[\mathcal{B}_{4}^{\pi^*} \Rightarrow 1] \right| \\ &+ \left| \Pr[\mathcal{B}_{4}^{E} \Rightarrow$$

which establishes Eqn. (11), thus completing the proof.

1

B.2 Proof of Lemma 12

Fix a tr = $(\mathbf{N}, \mathbf{h}_{out}; \mathbf{Z}; \mathbf{J}, \mathbf{R}, \mathbf{Y}) \in \mathcal{T}_{good}$. By definition of \mathcal{T}_{bad} , we know that $\Phi_{tr} := \Phi[\mathbf{A}_{r \times \ell q}, \mathbf{Z}]$ is a consistent mirror system and $\xi_{max}(tr) \leq n\ell$. First we observe that since the preprocessing step is identical for both oracles, we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};1\right)=\mathbf{R}\right]=\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};1\right)=\mathbf{R}\right]=\rho(\mathbf{R}) \text{ (say)}.$$
(90)

For the rest of the transcript, we examine the real world and the ideal world separately. Since **A** has r rows, there must be r distinct values of $X_j^{(i)}$ in **X**. Since the corresponding outputs are sampled uniformly without replacement by π_4^* in the real world, we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};3\right)=\mathbf{Y}\mid\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};1\right)=\mathbf{R}\right]=\frac{1}{(2^{n})_{r}}.$$
(91)

Finally, in the real world, \mathbf{Z} is determined from \mathbf{Y} , so we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};2\right)=\mathbf{Z} \mid \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};1\right)=\mathbf{R}, \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}};3\right)=\mathbf{Y}\right]=1.$$
(92)

From Eqns. (90), (91), and (92) we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = \mathsf{tr}\right] = \frac{\rho(\mathbf{R})}{(2^{n})_{r}}.$$
(93)

Next we turn our attention to the ideal world. Here, $(\mathcal{A}^{\mathcal{O}_0}; 2)$ is sampled first, and independently of $(\mathcal{A}^{\mathcal{O}_0}; 1)$, so we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};2\right)=\mathbf{Y} \mid \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};1\right)=\mathbf{R}\right]=\frac{1}{2^{n\ell q}}.$$
(94)

In the final step, sampling $(\mathcal{A}^{\mathcal{O}_0}; 3)$ is equivalent to a uniform sampling from $\Gamma(\Phi_{\mathsf{tr}})$, so we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};3\right)=\mathbf{Y} \mid \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};1\right)=\mathbf{R}, \mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}};2\right)=\mathbf{Y}\right]=\frac{1}{\left|\Gamma(\Phi_{\mathsf{tr}})\right|}.$$
(95)

From Eqns. (90), (94), and (95) we have

$$\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = \mathsf{tr}\right] = \frac{\rho(\mathbf{R})}{2^{n\ell q} |\Gamma(\Phi_{\mathsf{tr}})|}.$$
(96)

To complete the proof, we need to find an appropriate bound for the ratio of $\Pr[\mathsf{Trs}(\mathcal{A}^{\mathcal{O}_1}) = \mathsf{tr}]$ and $\Pr[\mathsf{Trs}(\mathcal{A}^{\mathcal{O}_0}) = \mathsf{tr}]$. From Eqns. (93) and (96) we have

$$\frac{\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{1}}\right) = \mathsf{tr}\right]}{\Pr\left[\mathsf{Trs}\left(\mathcal{A}^{\mathcal{O}_{0}}\right) = \mathsf{tr}\right]} = \frac{2^{n\ell q} |\Gamma(\Phi_{\mathsf{tr}})|}{(2^{n})_{r}}.$$
(97)

As the final step in the proof, we want to bound $|\Gamma(\Phi_{tr})|$ by applying Theorem 2. We already know that Φ_{tr} is a consistent mirror system, so we just need to verify the conditions on $\xi_{max}(tr)$. Using the bound $\xi_{max}(tr) \leq n\ell$, we have

$$n\xi_{\max}(\operatorname{tr})^2 + \xi_{\max}(\operatorname{tr}) \le n^3 \ell^2 + n\ell \le 2^{n/2},$$
(98)

and

$$12\ell q\xi_{\max}(\mathsf{tr}) \le 12n\ell^2 q \le 2^n.$$
⁽⁹⁹⁾

Thus, all the conditions for Theorem 2 are satisfied, and applying this theorem gives

$$|\Gamma(\Phi_{\mathsf{tr}})| \ge \frac{(2^n)_r}{2^{n\ell q}}.$$
(100)

Substituting Eqn. (100) in Eqn. (97) completes the proof of Lemma 12.

B.3 Proof of Lemma 13

For each pair $(i_1, i_2) \in [1..q]^2$, let I_{i_1,i_2} be the indicator random variable for membership in \mathcal{S}_{ar} , defined as

$$\begin{split} I_{i_1,i_2} &= 1, & \text{if } (i_1,i_2) \in \mathcal{S}_{\mathsf{ar}} \\ &= 0, & \text{otherwise.} \end{split}$$

If $N_2^{(i_1)} = N_2^{(i_2)}$, then $W_1^{(i_1)} \neq W_1^{(i_2)}$ and $W_2^{(i_1)} \neq W_2^{(i_2)}$, so (i_1, i_2) can only form an arm if $N_2^{(i_1)} = N_2^{(i_2)}$, so that $J^{(i_1)}$ and $J^{(i_2)}$ are outputs of π_1^* on two different inputs. We observe that

$$\Pr\left[W_1^{(i_1)} = W_1^{(i_2)}\right] = \Pr\left[N_1^{(i_1)} \oplus J^{(i_1)} = N_1^{(i_2)} \oplus J^{(i_2)}\right] = \frac{1}{2^n - 1},$$

$$\Pr\left[W_2^{(i_1)} = W_2^{(i_2)}\right] = \Pr\left[N_1^{(i_1)} \oplus 2 \cdot J^{(i_1)} = N_1^{(i_2)} \oplus 2 \cdot J^{(i_2)}\right] = \frac{1}{2^n - 1}.$$

By union-bound, we have

$$\mathbb{E}\left[I_{i_1,i_2}\right] = \Pr\left[(i_1,i_2) \in \mathcal{S}_{\mathsf{ar}}\right]$$

$$\leq \Pr\left[W_1^{(i_1)} = W_1^{(i_2)}\right] + \Pr\left[W_2^{(i_1)} = W_2^{(i_2)}\right] \leq \frac{2}{2^n - 1}.$$

Since $|S_{ar}| = \sum_{(i_1, i_2) \in [1..q]^2} I_{i_1, i_2}$, we have

$$\mathbb{E}[|\mathcal{S}_{\mathsf{ar}}|] = \sum_{(i_1, i_2) \in [1..q]^2} \mathbb{E}[I_{i_1, i_2}] \le \frac{2q(q-1)}{2^n - 1} \le \frac{2q^2}{2^n}.$$

By applying Markov's Inequality, we get

$$\Pr[\mathcal{E}_{\mathsf{ar}}] = \Pr[|\mathcal{S}_{\mathsf{ar}}| > q] \le \frac{\mathbb{E}[|\mathcal{S}_{\mathsf{ar}}|]}{q} \le \frac{2q}{2^n}$$

which establishes the bound in Eqn. (34).

B.4 Proof of Lemma 14

For each triple $(i_1, i_2, i_3) \in [1..q]^3$, let I_{i_1, i_2, i_3} be the indicator random variable for membership in S_{el} , defined as

$$\begin{split} I_{i_1,i_2,i_3} &= 1, & \text{if } (i_1,i_2,i_3) \in \mathcal{S}_{\mathsf{el}}, \\ &= 0, & \text{otherwise.} \end{split}$$

If $N_2^{(i_1)} = N_2^{(i_2)}$, then $W_1^{(i_1)} \neq W_1^{(i_2)}$, and if $N_2^{(i_2)} = N_2^{(i_3)}$, then $W_2^{(i_2)} \neq W_2^{(i_3)}$. Thus, the event $W_1^{(i_1)} = W_1^{(i_2)}, W_2^{(i_2)} = W_2^{(i_3)}$ can have non-zero probability only when $N_2^{(i_2)} \notin \{N_2^{(i_1)}, N_2^{(i_3)}\}$. In this case, we can write this event as

$$N_1^{(i_1)} \oplus J^{(i_1)} = N_1^{(i_2)} \oplus J^{(i_2)}, \tag{101}$$

$$N_1^{(i_2)} \oplus 2 \cdot J^{(i_2)} = N_1^{(i_3)} \oplus 2 \cdot J^{(i_3)}.$$
(102)

Since $N_2^{(i_1)} \neq N_2^{(i_2)}$, $J^{(i_1)}$ and $J^{(i_2)}$ are outputs of π_1^* on two different inputs. Thus,

$$\Pr\left[Eqn.\ (101)\right] = \frac{1}{2^n - 1}.\tag{103}$$

	-	-	٦
	_	-	J

If in addition $N_2^{(i_1)} \neq N_2^{(i_3)}$, then $J^{(i_3)}$ is the output of π_1^* on yet another different input, so that

$$\Pr\left[Eqn.\ (102) \mid Eqn.\ (101)\right] = \frac{1}{2^n - 2}.$$
(104)

From Eqns. (103) and (104), we get

$$\Pr\left[W_1^{(i_1)} = W_1^{(i_2)}, W_2^{(i_2)} = W_2^{(i_3)}\right] = \Pr\left[Eqns. \ (101), \ (102)\right]$$
$$= \Pr\left[Eqn. \ (101)\right] \Pr\left[Eqn. \ (102) \mid Eqn. \ (101)\right]$$
$$= \frac{1}{(2^n - 1)(2^n - 2)}.$$
(105)

This leaves the case $N_2^{(i_1)} = N_2^{(i_3)} \implies J^{(i_1)} = J^{(i_3)}$. Multiplying Eqn. (101) by 2, adding to Eqn. (102), setting $J^{(i_1)} = J^{(i_3)}$, and rearranging the terms gives

$$N_1^{(i_3)} = 3 \cdot N_1^{(i_2)} \oplus 2 \cdot N_1^{(i_1)}.$$
(106)

Define the set $\mathcal{S}^* \subseteq [1..q]^3$ as

$$\mathcal{S}^* := \left\{ (i_1, i_2, i_3) \mid N_1^{(i_3)} = 3 \cdot N_1^{(i_2)} \oplus 2 \cdot N_1^{(i_1)}, N_2^{(i_3)} = N_2^{(i_1)} \right\}$$

For $(i_1, i_2, i_3) \in \mathcal{S}^*$, Eqn. (101) implies Eqn. (102), so we have

$$\Pr\left[W_1^{(i_1)} = W_1^{(i_2)}, W_2^{(i_2)} = W_2^{(i_3)}\right] = \Pr\left[Eqn. \ (101)\right] = \frac{1}{2^n - 1}.$$
(107)

If $(i_1, i_2, i_3) \notin S^*$ and yet $N_2^{(i_3)} = N_2^{(i_1)}$, $\Pr[W_1^{(i_1)} = W_1^{(i_2)}, W_2^{(i_2)} = W_2^{(i_3)}] = 0$, because Eqn. (106) does not hold. From Eqns. (105) and (107), we can conclude that

$$\mathbb{E}[I_{i_1,i_2,i_3}] = \Pr[(i_1,i_2,i_3) \in \mathcal{S}_{\mathsf{el}}] \le \begin{cases} \frac{1}{2^n - 1}, & \text{if } (i_1,i_2,i_3) \in \mathcal{S}^*, \\ \frac{1}{(2^n - 1)(2^n - 2)}, & \text{otherwise.} \end{cases}$$

Since $|S_{\sf el}| = \sum_{(i_1, i_2, i_3) \in [1..q]^3} I_{i_1, i_2, i_3}$, we have

$$\mathbb{E}[|\mathcal{S}_{\mathsf{el}}|] = \sum_{(i_1, i_2, i_3) \in [1..q]^3} \mathbb{E}[I_{i_1, i_2, i_3}]$$

$$= \sum_{(i_1, i_2, i_3) \in \mathcal{S}^*} \mathbb{E}[I_{i_1, i_2, i_3}] + \sum_{(i_1, i_2, i_3) \notin \mathcal{S}^*} \mathbb{E}[I_{i_1, i_2, i_3}]$$

$$\leq \sum_{(i_1, i_2, i_3) \in \mathcal{S}^*} \frac{1}{2^n - 1} + \sum_{(i_1, i_2, i_3) \notin \mathcal{S}^*} \frac{1}{(2^n - 1)(2^n - 2)}$$

$$= \frac{|\mathcal{S}^*|}{2^n - 1} + \frac{q(q - 1)(q - 2) - |\mathcal{S}^*|}{(2^n - 1)(2^n - 2)}$$

$$\leq \frac{|\mathcal{S}^*|}{2^n - 1} + \frac{q(q - 1)(q - 2)}{(2^n - 1)(2^n - 2)}.$$
(108)

To bound $|\mathcal{S}^*|$, we observe that for each $(i_1, i_2, i_3) \in \mathcal{S}^*$, fixing i_1 and i_2 completely determines i_3 . Thus, $|\mathcal{S}^*| \leq q(q-1)$. Substituting this bound in Eqn. (108) gives

$$\mathbb{E}[|\mathcal{S}_{\mathsf{el}}|] \le \frac{q(q-1)}{2^n - 1} + \frac{q(q-1)(q-2)}{(2^n - 1)(2^n - 2)} \le \frac{q^2}{2^n} + \frac{q^3}{2^{2n}}$$

By applying Markov's Inequality, we get

$$\Pr[\mathcal{E}_{\mathsf{el}}] = \Pr[|\mathcal{S}_{\mathsf{el}}| > q] \le \frac{\mathbb{E}[|\mathcal{S}_{\mathsf{el}}|]}{q} \le \frac{q}{2^n} + \frac{q^2}{2^{2n}},$$

which establishes the bound in Eqn. (35).

B.5 Proof of Lemma 15

For Eqn. (36) to hold, we must have $h_{\text{out}}^{(i_1)} = h_{\text{out}}^{(i_2)} = \cdots = h_{\text{out}}^{(i_k)}$, so we can assume here that $\mathbf{N}^{(i_1)}, \mathbf{N}^{(i_2)}, \ldots, \mathbf{N}^{(i_k)}$ are all distinct; then Eqn. (36) reduces to $(\tilde{X}_{j'_2}^{(i_2)}, \ldots, \tilde{X}_{j'_k}^{(i_k)}) = (\tilde{X}_{j_1}^{(i_1)}, \ldots, \tilde{X}_{j_{k-1}}^{(i_{k-1})})$, which we can rewrite as

$$(\mathbf{U}_{j_{2}^{\prime}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{2})}, \dots, \mathbf{U}_{j_{k}^{\prime}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k})}) = (\mathbf{U}_{j_{1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{1})}, \dots, \mathbf{U}_{j_{k-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k-1})})$$

A chain ζ can be treated interchangeably with the event of the chain forming, i.e., the conjunction of all the collisions necessary for ζ to satisfy the definition of a chain. In this way we can make sense of an expression like $\Pr[\zeta]$. For $2 < d \leq k$ and a k-chain ζ , let $\zeta_{<d}$ denote the (d-1)-chain (i_1, \ldots, i_{d-1}) (or, equivalently, the conjunction of the d-2 collisions required for this chain), and let ζ_d denote the collision required to link i_{d-1} to i_d , i.e., the event that for some $j_{d-1}, j'_d \in [0..\ell]$, $\mathbf{U}_{j_d*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_d)} = \mathbf{U}_{j_{d-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{d-1})}$. Note that by this notation,

$$\zeta = \bigwedge_{d=2}^{k} \zeta_d.$$

We observe that if $W_1^{(i_d)} \notin \{W_1^{(i_a)} \mid 1 \leq a < d\}$, $R_1^{(i_d)}$ will be the truncated output of π_2^* on an input that did not appear earlier in the chain, and similarly, if $W_2^{(i_d)} \notin \{W_1^{(i_a)} \mid 1 \leq a < d\}$, $R_2^{(i_d)}$ will be the truncated output of π_3^* on an input that did not appear earlier in the chain. Thus, if i_d is fresh, at least one of $R_1^{(i_d)}$ and $R_2^{(i_d)}$ will be a source of fresh randomness after conditioning on $\zeta_{<d}$. This is a key feature of fresh nodes that we will repeatedly invoke.

With the above in mind, we can start analysing the probability of \mathcal{E}_{ch} . We first look at the probability of $\mathcal{E}_{ch,2}$. In a 2-chain (i_1, i_2) , the only candidate for a stale node is i_2 , and the only way for i_2 to be stale if to have both $W_1^{(i_2)} = W_1^{(i_1)}$ and $W_2^{(i_2)} = W_2^{(i_1)}$, which is impossible because $\mathbf{R}^{(i_1)} \neq \mathbf{R}^{(i_2)}$, and the mapping $\mathbf{R}^{(i)} \mapsto \mathbf{W}^{(i)}$ is injective. Thus,

$$\Pr[\mathcal{E}_{\mathsf{ch},2}] = 0.$$

Next, for k > 2, define

$$\mathcal{E}_{\mathsf{ch},< k} := \bigvee_{2 \leq k' < k} \mathcal{E}_{\mathsf{ch},k'}$$

We want to examine the probability of $\mathcal{E}_{ch,k}$ conditioned on $\neg \mathcal{E}_{ch,<k}$. So suppose $\mathcal{E}_{ch,<k}$ has not occurred. Consider a k-chain $\zeta = (i_1, \ldots, i_k)$ with one or more stale nodes, and let i_d be its first stale node from the left. We observe that if d < k, (i_1, \ldots, i_d) is a d-chain with i_d as a stale node, which contradicts the assumption that $\mathcal{E}_{ch,<k}$ (and thus in particular $\mathcal{E}_{ch,d}$) has not occurred. Thus, the only candidate for a stale node in ζ is i_k .

Now, since i_2 is fresh (it cannot be otherwise, as we saw earlier), for any fixed $j'_2, j_1 \in [0, \ell]$ we have

$$\Pr\left[\mathbf{U}_{j_{2*}}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{2})} = \mathbf{U}_{j_{1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{1})}\right] \le \frac{2^{\lambda}}{2^{n} - 1}$$

by the randomness of $R_1^{(i_2)}$ or $R_2^{(i_2)}$, whichever lends freshness to i_2 . Since there are $\ell + 1$ choices each for j_1 and j'_2 , we have

$$\Pr[\zeta_2] \le \frac{2^{\lambda} (\ell+1)^2}{2^n - 1}.$$
(109)

Further, if $k \ge 4$, for any d with 2 < d < k, since i_d is fresh (by the above discussion), for any fixed $j'_d, j_{d-1} \in [0, \ell]$ we have

$$\Pr\left[\mathbf{U}_{j_d*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_d)} = \mathbf{U}_{j_{d-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{d-1})} \mid \zeta_{< d}\right] \le \frac{2^{\lambda}}{2^n - d + 1},$$

and counting the choices for j'_d and j_{d-1} gives

$$\Pr\left[\zeta_d \mid \zeta_{\leq d}\right] \le \frac{2^{\lambda} (\ell+1)^2}{2^n - d + 1}.$$
(110)

By induction, we can show that

$$\Pr[\zeta_{< d+1}] \le \frac{2^{\lambda(d-1)}(\ell+1)^{2(d-1)}}{(2^n-1)_{d-1}}.$$
(111)

For the proof of this bound, Eqn. (109) serves as base case; for the induction step we use the identity $\Pr[\zeta_{< d+1}] = \Pr[\zeta_d \land \zeta_{< d}] = \Pr[\zeta_d \mid \zeta_{< d}] \Pr[\zeta_{< d}]$ and plug in the bound from Eqn. (110).

Taking d = k - 1 in Eqn. (111) gives

$$\Pr[\zeta_{< k}] \le \frac{2^{\lambda(k-2)}(\ell+1)^{2(k-2)}}{(2^n - 1)_{k-2}}$$

Since $\zeta_k \implies \zeta_{< k}$, we have

$$\Pr[\zeta_k \wedge i_k \text{ is stale}] \le \Pr[\zeta_k] \le \Pr[\zeta_{< k}] \le \frac{2^{\lambda(k-2)}(\ell+1)^{2(k-2)}}{(2^n-1)_{k-2}}.$$

Since i_k is stale and $\mathcal{E}_{ch,<k}$ did not occur, i_k must be fresh in the chain (i_2,\ldots,i_k) . Thus, either $W_1^{(i_k)} \notin \{W_1^{(i_a)} \mid 2 \leq a < k\}$ or $W_2^{(i_d)} \notin \{W_2^{(i_a)} \mid 2 \leq a < k\}$. First suppose $W_1^{(i_k)} \notin \{W_1^{(i_a)} \mid 2 \leq a < k\}$. Since i_k is stale in ζ , we must have $W_1^{(i_k)} = W_1^{(i_1)}$. This in turn implies that $W_2^{(i_k)} \neq W_2^{(i_1)}$, so again by staleness of i_k , we must have $W_2^{(i_k)} \neq W_2^{(i_a)}$ for some $a \in [2..k - 1]$. Thus, (i_1, i_k, i_a) must be an elbow. Similarly, if instead $W_2^{(i_d)} \notin \{W_2^{(i_a)} \mid 2 \leq a < k\}$, we can show that (i_a, i_k, i_1) must be an elbow.

In either case, the number of choices for i_1, i_a, i_k is bounded by $|S_{el}|$, which is bounded by q if \mathcal{E}_{el} has not occurred. Then the other k-3 indices in ζ can be picked in $(q-3)_{k-3}$ ways. Thus, by union-bound, we have

$$\Pr[\mathcal{E}_{\mathsf{ch},k} \mid \neg \mathcal{E}_{\mathsf{ch},
(112)$$

To simplify this bound, we observe that since $q - 3 < 2^n - 1$,

$$\frac{q-3-i}{2^n-2-i} \le \frac{q-3}{2^n-2} \le \frac{q-1}{2^n}$$

for any $i \in [0..k - 4]$. Thus,

$$\frac{q(q-3)_{k-3}}{(2^n-1)_{k-2}} = \frac{q}{2^n-1} \prod_{i=0}^{k-4} \frac{q-3-i}{2^n-2-i} \le \frac{q(q-1)^{k-3}}{(2^n-1)2^{n(k-3)}}.$$
(113)

Substituting Eqn. (113) in Eqn. (112) gives

$$\Pr[\mathcal{E}_{\mathsf{ch},k} \mid \neg \mathcal{E}_{\mathsf{ch},$$

Recall that \mathcal{E}_{ch} denotes the event $\mathcal{E}_{ch,3} \vee \cdots \vee \mathcal{E}_{ch,n+1}$. Then by union-bound we have

$$\Pr[\mathcal{E}_{\mathsf{ch}} \mid \neg \mathcal{E}_{\mathsf{el}}] \le \sum_{k=3}^{n+1} \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^{k-2} = \frac{(\ell+1)^2 q}{2^{n-\lambda}} \cdot \sum_{k=0}^{n-2} \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^k.$$
(114)

Using the assumption that $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$, we can bound Eqn. (114) as

$$\Pr[\mathcal{E}_{\mathsf{ch}} \mid \neg \mathcal{E}_{\mathsf{el}}] \le \frac{(\ell+1)^2 q}{2^{n-\lambda}} \cdot \sum_{k=0}^{n-2} \left(\frac{1}{2}\right)^k \le \frac{(\ell+1)^2 q}{2^{n-\lambda-1}}.$$
(115)

From Eqns. (35) (Lemma 14) and (115) we get

$$\begin{aligned} \Pr[\mathcal{E}_{\mathsf{ch}}] &= \Pr[\mathcal{E}_{\mathsf{ch}} \wedge \mathcal{E}_{\mathsf{el}}] + \Pr[\mathcal{E}_{\mathsf{ch}} \wedge \neg \mathcal{E}_{\mathsf{el}}] \\ &\leq \Pr[\mathcal{E}_{\mathsf{el}}] + \Pr[\mathcal{E}_{\mathsf{ch}} \mid \neg \mathcal{E}_{\mathsf{el}}] \leq \frac{q}{2^n} + \frac{q^2}{2^{2n}} + \frac{(\ell+1)^2 q}{2^{n-\lambda-1}}, \end{aligned}$$

which establishes the bound in Eqn. (37).

B.6 Proof of Lemma 16

Eqn. (38) is equivalent to $\tilde{X}_{j'}^{(i)} = \tilde{X}_{j}^{(i)}$, which we can rewrite as

$$\mathbf{U}_{j'*}^{\mathsf{T}} \cdot \mathbf{R}^{(i)} = \mathbf{U}_{j*}^{\mathsf{T}} \cdot \mathbf{R}^{(i)}, \quad \text{or} \quad (\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}}) \cdot \mathbf{R}^{(i)} = 0.$$

Since **U** is locally non-degenerate, its rows are pairwise independent, which means in particular that $\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}} \neq 0$. Without loss of generality, assume its first element is non-zero, i.e., $U_{j'1} \oplus U_{j1} \neq 0$. Then $(U_{j'1} \oplus U_{j1}) \cdot R_1^{(i)}$ is distributed uniformly over $\mathbb{GF}(2^{n-\lambda})$. Moreover, since $R_1^{(i)}$ and $R_2^{(i)}$ are independent (being the truncated outputs of the independent random permutations π_2^* and π_3^* respectively), it follows that $(\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}}) \cdot \mathbf{R}^{(i)}$ is distributed uniformly over $\mathbb{GF}(2^{n-\lambda})$, so that

$$\Pr\left[\left(\mathbf{U}_{j'*}^{\mathsf{T}} \oplus \mathbf{U}_{j*}^{\mathsf{T}}\right) \cdot \mathbf{R}^{(i)} = 0\right] = \frac{1}{2^{n-\lambda}}.$$
(116)

There are q choices for i, and $\ell(\ell+1)/2$ choices for j, j', so applying union-bound to Eqn. (116) yields the bound in Eqn. (39).

B.7 Proof of Lemma 17

For Eqn. (40) to be satisfiable, we need $h_{\text{out}}^{(i_1)} = h_{\text{out}}^{(i_2)}$; then it reduces to $(\tilde{X}_{j_2}^{(i_2)}, \tilde{X}_{j'_2}^{(i_2)}) = (\tilde{X}_{j_1}^{(i_1)}, \tilde{X}_{j'_1}^{(i_1)})$, which we can rewrite as

$$(\mathbf{U}_{j_{2}*}, \mathbf{U}_{j'_{2}*})^{\mathsf{T}} \cdot \mathbf{R}^{(i_{2})} = (\mathbf{U}_{j_{1}*}, \mathbf{U}_{j'_{1}*})^{\mathsf{T}} \cdot \mathbf{R}^{(i_{1})}.$$
(117)

Since $\mathbf{U}_{j_{2}*}$ and $\mathbf{U}_{j'_{2}*}$ are linearly independent, $(\mathbf{U}_{j_{2}*}, \mathbf{U}_{j'_{2}*})^{\mathsf{T}}$ is an invertible 2×2 matrix, so we can further rewrite Eqn. (117) as

$$\mathbf{R}^{(i_2)} = (\mathbf{U}_{j_2*}, \mathbf{U}_{j'_2*})^{\mathsf{T}-1} \cdot (\mathbf{U}_{j_1*}, \mathbf{U}_{j'_1*})^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)}.$$
(118)

If $(i_1, i_2) \notin S_{ar}$, $W_1^{(i_1)} \neq W_1^{(i_2)}$, so $R_1^{(i_1)}$ and $R_1^{(i_2)}$ are truncated outputs of π_2^* on different inputs, and similarly $W_2^{(i_1)} \neq W_2^{(i_2)}$, so $R_2^{(i_1)}$ and $R_2^{(i_2)}$ are truncated outputs of π_3^* on different inputs. So we can write

$$\Pr\left[Eqn. \ (118)\right] = \frac{2^{2\lambda}}{(2^n - 1)^2}.$$

In this case, there will be $\ell^2(\ell+1)^2/4$ choices for j_1, j'_1, j_2, j'_2 . If $(i_1, i_2) \in \mathcal{S}_{ar}$, the two equations in Eqn. (40) may be reduced to one equation. But one of $W_1^{(i_1)} \neq W_1^{(i_2)}$ and $W_2^{(i_1)} \neq W_2^{(i_2)}$ must still hold, so we must still have

$$\Pr\left[Eqn. \ (118)\right] \le \frac{2^{\lambda}}{2^n - 1}.\tag{119}$$

Moreover, this case fixes the choices of j_2 and j'_2 , so there are $\ell(\ell+1)/2$ choices for j_1, j'_1, j_2, j'_2 . Let $\mathcal{E}_2^{i_1, i_2}$ denote the event that for some $j_1, j'_1, j_2, j'_2 \in [0, \ell]$ with $j_1 < j'_1, j_2 < j'_2, (X_{j_2}^{(i_2)}, X_{j'_2}^{(i_2)}) = (X_{j_1}^{(i_1)}, X_{j'_1}^{(i_1)})$. Then we have

$$\Pr[\mathcal{E}_{2}^{i_{1},i_{2}} \mid \neg \mathcal{E}_{ar}] \leq \begin{cases} \frac{2^{\lambda}\ell(\ell+1)}{2(2^{n}-1)}, & \text{if } (i_{1},i_{2}) \in \mathcal{S}_{ar}, \\ \frac{2^{2\lambda}\ell^{2}(\ell+1)^{2}}{4(2^{n}-1)^{2}}, & \text{otherwise.} \end{cases}$$

Recalling that $|\mathcal{S}_{ar}| \leq q$ as long as \mathcal{E}_{ar} has not occurred, we get

$$\begin{split} \Pr[\mathcal{E}_{2}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{ar}}] &= \sum_{(i_{1},i_{2})\in[1..q]^{2}} \Pr[\mathcal{E}_{2}^{i_{1},i_{2}} \mid \neg \mathcal{E}_{\mathsf{ar}}] \\ &= \sum_{(i_{1},i_{2})\in\mathcal{S}_{\mathsf{ar}}} \Pr[\mathcal{E}_{2}^{i_{1},i_{2}} \mid \neg \mathcal{E}_{\mathsf{ar}}] + \sum_{(i_{1},i_{2})\notin\mathcal{S}_{\mathsf{ar}}} \Pr[\mathcal{E}_{2}^{i_{1},i_{2}} \mid \neg \mathcal{E}_{\mathsf{ar}}] \\ &\leq |\mathcal{S}_{\mathsf{ar}}| \frac{2^{\lambda}\ell(\ell+1)}{2(2^{n}-1)} + \frac{q(q-1)}{2} \frac{2^{2\lambda}\ell^{2}(\ell+1)^{2}}{4(2^{n}-1)^{2}} \\ &\leq \frac{\ell(\ell+1)q}{2^{n-\lambda}} + \frac{\ell^{2}(\ell+1)^{2}q^{2}}{2^{2n-2\lambda+4}}, \end{split}$$

which establishes the bound in Eqn. (41).

B.8 Proof of Lemma 18

Eqn. (42) is equivalent to an (n + 1)-chain ζ . If \mathcal{E}_{ch} has not happened, each node in this chain must be fresh, so arguing as in the bounding of $\Pr[\zeta_{\leq d+1}]$, we have

$$\Pr[\zeta \mid \neg \mathcal{E}_{\mathsf{ch}}] \le \frac{2^{\lambda n} (\ell+1)^{2n}}{(2^n - 1)_n}.$$
(120)

Since there are $(q)_{n+1}$ choices for the indices in ζ , by union-bound we have

$$\Pr[\mathcal{E}_3 \mid \neg \mathcal{E}_{ch}] \le \frac{2^{\lambda n} (\ell+1)^{2n} (q)_{n+1}}{(2^n-1)_n} \le q \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}}\right)^n \le \frac{q}{2^n},$$

using the assumption that $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$. This establishes the bound in Eqn. (43).

B.9 Proof of Lemma 19

Eqn. (44) is equivalent to (i_1, \ldots, i_{k-1}) forming a (k-1)-chain $\zeta_{\langle k}$, and i_k satisfying the condition

$$(X_{j'_k}^{(i_k)}, X_{j_k}^{(i_k)}) = (X_{j_{k-1}}^{(i_{k-1})}, X_{j'_1}^{(i_1)}).$$
(121)

For this to hold we need $h_{\text{out}}^{(i_k)} = h_{\text{out}}^{(i_1)}$ (which in turn is already equal to $h_{\text{out}}^{(i_d)}$ for each other $d \in [2..k-1]$); then we can rewrite Eqn. (121) as

$$(\mathbf{U}_{j'_{k}*},\mathbf{U}_{j_{k}*})^{\mathsf{T}}\cdot\mathbf{R}^{(i_{k})} = (\mathbf{U}_{j_{k-1}*}^{\mathsf{T}}\cdot\mathbf{R}^{(i_{k-1})},\mathbf{U}_{j'_{1}*}^{\mathsf{T}}\cdot\mathbf{R}^{(i_{1})})^{\mathsf{T}},$$

п		1
L		
L		
L		

and since $(\mathbf{U}_{j'_k*}, \mathbf{U}_{j_k*})^{\mathsf{T}}$ is invertible, this becomes

$$\mathbf{R}^{(i_k)} = (\mathbf{U}_{j'_k*}, \mathbf{U}_{j_k*})^{\mathsf{T}-1} \cdot (\mathbf{U}_{j_{k-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k-1})}, \mathbf{U}_{j'_1*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)})^{\mathsf{T}}.$$

Let $(u, v)_{j'_k, j_k, j'_{k-1}, j_1}^{\mathsf{T}}$ denote $(\mathbf{U}_{j'_k*}, \mathbf{U}_{j_k*})^{\mathsf{T}-1} \cdot (\mathbf{U}_{j_{k-1}*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_{k-1})}, \mathbf{U}_{j'_1*}^{\mathsf{T}} \cdot \mathbf{R}^{(i_1)})^{\mathsf{T}}$. Since $\zeta := (i_1, \ldots, i_k)$ is a chain, i_k will be fresh in ζ unless $\mathcal{E}_{\mathsf{ch}}$ has occurred. If both $W_1^{(i_d)} \notin \{W_1^{(i_a)} \mid 1 \leq a < d\}$ and $W_2^{(i_d)} \notin \{W_2^{(i_a)} \mid 1 \leq a < d\}$, then we can use the randomness of both $R_1^{(i_k)}$ and $R_2^{(i_k)}$ after conditioning on $\zeta_{<k}$, to get

$$\Pr\left[\mathbf{R}^{(i_k)} = (u, v)_{j'_k, j_{k-1}, j_1}^{\mathsf{T}} \mid \zeta_{< k}, \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \le \frac{2^{2\lambda}}{(2^n - k + 1)^2}.$$
(122)

Like in Eqn. (120), taking k - 2 instead of n, we get

$$\Pr[\zeta_{
(123)$$

Let ζ^{\bigcirc} denote the *cyclic closure* of ζ , i.e., the chain ζ together with the event that we can find $j'_k, j_k, j'_{k-1}, j_1 \in [0..\ell]$ such that Eqn. (121) holds. Then we have

$$\Pr\left[\zeta^{\bigcirc} \mid \zeta_{$$

by applying union-bound to Eqn. (122). Recalling that $\zeta^{\bigcirc} \wedge \zeta_{\langle k} = \zeta^{\bigcirc}$, from Eqns. (123) and (124) we get

$$\Pr\left[\zeta^{\circlearrowright} \mid \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \leq \Pr\left[\zeta^{\circlearrowright} \mid \zeta_{\langle k}, \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \Pr\left[\zeta_{\langle k} \mid \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \\ \leq \frac{2^{\lambda k} (\ell+1)^{2k}}{(2^n-1)_{k-2} (2^n-k+1)^2} \leq \frac{2^{\lambda k} (\ell+1)^{2k}}{(2^n-1)_k}.$$
(125)

If for some $d \in [1..k-1]$ either $W_1^{(i_d)} \in \{W_1^{(i_a)} \mid 1 \le a < d\}$ or $W_2^{(i_d)} \in \{W_2^{(i_a)} \mid 1 \le a < d\}$ holds, then $(i_d, i_k) \in \mathcal{S}_{ar}$, and we can argue as before Eqn. (119) that

$$\Pr\left[\mathbf{R}^{(i_k)} = (u, v)_{j'_k, j_k, j'_{k-1}, j_1}^{\mathsf{T}} \mid \zeta_{\langle k}, \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \leq \frac{2^{\lambda}}{2^n - k + 1},$$

and that this fixes j_k and j'_k , so that

$$\Pr\left[\zeta^{\circlearrowright} \mid \zeta_{< k}, \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \leq \frac{2^{\lambda} (\ell + 1)^2}{2^n - k + 1},$$

and hence

$$\Pr\left[\zeta^{\circlearrowright} \mid \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}\right] \le \frac{2^{\lambda(k-1)}(\ell+1)^{2(k-1)}}{(2^n-1)_{k-1}}.$$
(126)

Since \mathcal{E}_{ar} did not occur, (i_d, i_k) can be chosen in at most q ways, and the rest of the queries in at most $(q-2)_{k-2}$ ways. Thus, combining the two cases from Eqns. (125) and (126), we have

$$\Pr[\mathcal{E}_{4,k}^{\dagger} \mid \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}] \leq \frac{2^{\lambda k} (\ell+1)^{2k} (q)_k}{(2^n - 1)_k} + \frac{2^{\lambda (k-1)} (\ell+1)^{2(k-1)} q(q-2)_{k-2}}{(2^n - 1)_{k-1}} \\ \leq 2 \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^k + 2 \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^{k-1} \leq 3 \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^{k-1}, \quad (127)$$

where in the last inequality we use the assumption that $(\ell + 1)^2 q \leq 2^{n-\lambda-1}$, and in the one before we use the inequality

$$\frac{2^{nk}}{(2^n-1)^k} = \left(1 + \frac{1}{2^n-1}\right)^k \le e^{k/(2^n-1)} \le 2.$$

Recall that \mathcal{E}_4^{\dagger} denotes the event $\mathcal{E}_{4,3}^{\dagger} \lor \cdots \lor \mathcal{E}_{4,n}^{\dagger}$. Then by Eqn. (127) and union-bound we have

$$\begin{aligned} \Pr[\mathcal{E}_4^{\dagger} \mid \neg \mathcal{E}_{\mathsf{ch}}, \neg \mathcal{E}_{\mathsf{ar}}] &\leq \sum_{k=3}^n \left[3 \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^{k-1} \right] \\ &= 3 \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^2 \cdot \sum_{k=0}^{n-3} \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^k \\ &\leq 3 \left(\frac{(\ell+1)^2 q}{2^{n-\lambda}} \right)^2 \cdot \sum_{k=0}^{n-3} \left(\frac{1}{2} \right)^k \leq \frac{6(\ell+1)^4 q^2}{2^{2n-2\lambda}}, \end{aligned}$$

which establishes the bound in Eqn. (45).

- 1