New Bounds for Keyed Sponges with Extendable Output: Independence between Capacity and Message Length

Yusuke Naito[1] and Kan Yasuda[2]

[1] Mitsubishi Electric Corporation
Naito.Yusuke@ce.MitsubishiElectric.co.jp
[2] NTT Secure Platform Laboratories
yasuda.kan@lab.ntt.co.jp

Abstract. We provide new bounds for the pseudo-random function security of keyed sponge constructions. For the case $c \leq b/2$ (c the capacity and b the permutation size), our result improves over all previously-known bounds. A remarkable aspect of our bound is that dependence between capacity and message length is removed, partially solving the open problem posed by Gaži et al. at CRYPTO 2015. Our bound is essentially tight, matching the two types of attacks pointed out by Gaži et al. For the case $c > b/2$, Gaži et al.'s bound remains the best for the case of single-block output, but for keyed sponges with extendable outputs, our result partly (when query complexity is relatively large) provides better security than Mennink et al.'s bound presented at ASIACRYPT 2015.

Keyword: PRF, XOF, game playing, coefficient H technique, lazy sampling, multi-collision, Stirling's approximation.

1 Introduction

The sponge construction today, though being originally introduced as a mode for keyless hash functions [7], is drawing more and more attention in the secret-key setting. The primary reason seems to lie in the flexibility: the *keyed* sponge construction has been modified in a variety of ways such as duplexing [6], parallelism [3] and full-state (i.e. the rate being equal to the permutation size) absorption [9, 19]. However, one of the reasons why the sponge construction was so attractive in the first place was that it inherently possessed the capability of *extendable* output.

FIPS 202 [17] standardizes two sorts of extendable output functions (XOFs): SHAKE128 and SHAKE256, which have a permutation size of $b = 1600$ bits and capacity values of $c = 256, 512$ bits, respectively. FIPS 202 states:

> *XOFs are a powerful new kind of cryptographic primitive that offers the flexibility to produce outputs with any desired length. ... In practice, the use of an XOF as a key derivation function (KDF) could preclude the possibility of related outputs, by incorporating the length and/or type of*

the derived key into the message input to the KDF. In that case, a disagreement or misunderstanding between two users of the KDF about the type or length of the key they are deriving would almost certainly not lead to related outputs.

To confirm the above statement in a more formal way, we need to investigate the security of the KDF as a pseudo-random function (PRF).

Previous PRF Bounds. Several different types of PRF bounds are known for keyed sponges. Security parameters of keyed sponges include the permutation size b, the capacity c, the rate $r := b - c$, and the key length k. The main focus remains on the capacity value c, because usually it is this parameter that defines a dominant term in a bound. Nevertheless, none of the previous bounds has been shown to be strictly tight in relation to parameter c, as explained below.

The PRF security of keyed sponges can be derived from the indifferentiability of the sponge construction. The indifferentiability of the sponge construction [7] crucially depends on the capacity c, and hence so does the derived PRF bound. Roughly, the indifferentiability-based PRF bound has a dominant term of the form $(\ell q + Q)^2/2^c$, where parameter ℓ is the maximum length of an adversarial query, parameter q the maximum number of construction (online) queries to the keyed sponge $\mathcal{C}$, and parameter Q the maximum number of primitive (offline) queries to the underlying permutation P.

Note that we are working in the ideal model [1, 13, 16] where the underlying permutation P is regarded as a random permutation. In practice, P is a fixed permutation; hence Q corresponds to the time complexity of the adversary, measuring how many times the adversary could perform offline computation of P.

The above indifferentiability-based PRF bound is rather loose, and the actual PRF security of keyed sponges should be much higher, as first noticed by Bertoni et al. [8]. Later, Andreeva et al. [1] successfully removed the term $Q^2/2^c$ and obtained a bound which was basically $\big((\ell q)^2 + \mu Q\big)/2^c$. Here, μ is an adversarial parameter called "multiplicity" and lies somewhere between $2\ell q/2^r$ and $2\ell q$.

Concurrently, Gaži et al. [13] provided a "nearly tight" bound [16] which was roughly of the form $(q^2 + \ell q + qQ)/2^c$. Gaži et al. also pointed out two attacks matching $q^2/2^c$ and $qQ/2^c$, respectively. They observed that their bound "only mildly depends on the length" when ℓ is sufficiently small [13] but left it open whether their bound was tight for all cases, especially when ℓ is large. It should be noted that Gaži et al. [13] only treated the case of single-block output, and their method did not seem to be easily extendable to the case of multiple-block output [16].

For the case of extendable output, recently Mennink et al. [16] has provided another bound which is essentially $(\ell q^2 + \mu Q)/2^c$. While definitely improving Andreeva et al.'s $\big((\ell q)^2 + \mu Q\big)/2^c$, Mennink et al.'s bound does not come close to Gaži et al.'s $(q^2 + \ell q + qQ)/2^c$, at least for the case of single-block output.

Table 1. Comparison of target keyed sponge constructions

	Key		Extendable
	Inner	Outer	output
Bertoni et al. [8]	—	✓	✓
Chang et al. [11]	✓	✓	✓
Andreeva et al. [1]	✓	✓	✓
Gaži et al. [13][a]	—	✓	—
Mennink et al. [16][b]	✓	—	✓
This paper	✓	✓	✓

[a] Gaži et al. [13] treat the case where the rate values are different between absorbing and squeezing phases. Only the rate r for the squeezing phase appears in the bound; the rate for absorbing phase does not affect security in their analysis.

[b] Mennink et al. [16] study the case of full-state absorption, i.e. the rate for absorbing phase is equal to the permutation size except for the first call of the underlying permutation.

Consequently, it seems that there is still room for improvement. It might be possible to come up with a tighter PRF bound for keyed sponges, especially for the case of extendable output.

Inner- and Outer-Keying. There are two ways of keying the sponge construction. The difference between the two methods is analogous to the one between NMAC and HMAC [4]. The first method, which is like NMAC, is called the *inner-keyed* sponge [1]. This replaces (part of) the inner IV with a secret key $K \in \{0,1\}^k$, so that $k \le c$. The inner-keyed sponge was proposed by Chang et al. [11] who showed that it has a certain advantage in the standard-model security.

The second method, which is like HMAC, is called the *outer-keyed* sponge [1]. This is nothing but the sponge construction itself that processes the input $K\|M$ (i.e. a message prefixed by a secret key K) and hence does not have a limitation on the key size k. A first analysis of the outer-keyed sponge was given by Bertoni et al. [8]. The obvious advantage of this method, besides key length, is that we can make use of existing sponge constructions that have been already implemented as hash functions.

Our Contributions. We provide new PRF bounds for keyed sponges with extendable output, under the condition that the rate and capacity remain the same for absorbing and squeezing phases. We treat both inner- and outer-keyed sponges (cf. Table 1). Previous PRF bounds and our results are summarized in Table 2.

- **Case $c \le b/2$.** This case includes SHAKE128 and SHAKE256. In this case, our bound improves over all previously-known PRF bounds. For the inner-keyed sponge, our bound is qualitatively better than the previous two bounds by Andreeva et al. [1] and by Mennink et al. [16]. For example, if $k = c$ (which is the case that provides the highest security for the inner-keyed sponge), then the previous bounds contained $(\ell q^2 + \mu Q)/2^c$, whereas our bound only contains $(\ell q + q^2 + qQ)/2^c$. On the other hand, for the outer-keyed sponge, observe that the term related to capacity in our bound becomes roughly $(q^2 + qQ)/2^c$, which is dominant in many scenarios. Note the absence of ℓq here; we remove the dependence between capacity c and message length ℓ, partially answering the open question posed by Gaži et al. [13]. Together with the two attacks pointed out by Gaži et al. [13] whose complexities were roughly $q^2/2^c$ and $qQ/2^c$, we see that our bound is strictly tight in terms of parameters q and Q. Furthermore, for the outer-keyed sponge, the remaining parameter ℓ is restricted only by the term $\ell^2 q^2/2^b$, whereas previous bounds contained $\ell q/2^c$ or $\ell^2 q^2/2^c$. Hence, our bound has a qualitatively weaker restriction on ℓ, under the condition $c \leq b/2$.

- **Case $c > b/2$.** This is the case for lightweight hash functions, such as Quark [2], SPONGENT [10] and PHOTON [14]. In this case, our contribution is more subtle. For single-block output, Gaži et al.'s bound [13] remains the best, beating our bound as well as Mennink et al.'s [16]. However, for multiple-block output, our result improves over Mennink et al.'s [16] which has been the best known bound for extendable output. The two bounds are incomparable due to the parameter μ, but roughly speaking, we see that our bound becomes better when query complexity is relatively large. For simplicity, assume $k = c$ and put $\mu = 2\ell q$. Then Mennink et al.'s bound becomes roughly $(\ell q^2 + \ell q Q)/2^c$, whereas our bound has a dominant term of $\left((\ell q^2 + \ell q Q)/2^b\right)^{1/2}$. By comparison, our bound becomes smaller when $\ell q^2 + \ell q Q > 2^{c-r}$.

For our proofs we take an approach different from previous work. We first make use of the game-playing technique, introducing just one intermediate game between the real and ideal worlds. Our transition between the games heavily relies on the coefficient H technique of Patarin [18]. To evaluate probabilities of "bad" events, we make extensive use of lazy sampling. As pointed out by Bellare and Rogaway [5], the lazy sampling of random functions with many constraints can be tricky. We show how to carefully lazy-sample input/output points for underlying permutations with certain restrictions. Lastly, we adopt techniques developed by Jovanovic et al. [15] for bounding the size of multi-collisions and for finally optimizing the bound (or "balancing" the terms).

2 Preliminaries

Notation. Let $\{0,1\}^*$ be the set of all bit strings, and for an integer $d \geq 0$, let $\{0,1\}^d$ be a set of d-bit strings. Let 0^d denotes the bit string of d-bit zeroes. For a bit string $x \in \{0,1\}^d$, let $x[i,j]$ be the substring of x from i-th bit to j-th bit, where $1 \leq i \leq j \leq d$. For a finite set X, $x \xleftarrow{\$} X$ means that an element is randomly drawn from X and is set to x. For a set X, $\mathsf{Perm}(X)$ is the set of all

Table 2. Comparison of PRF bounds for keyed sponges. In the bounds, parameter κ is key length in blocks, i.e. $\kappa := k/r$; parameter μ is the multiplicity, i.e. $2\ell q/2^r \le \mu \le 2\ell q$; parameter $t \ge 1$ can be arbitrary; the number e is Napier's constant $2.71828\cdots$; the function λ is defined as $\lambda(x) := x/2^k$ if $\kappa = 1$ and $\lambda(x) := \min\{\epsilon_1, \epsilon_2\}$ if $\kappa \ge 2$, where $\epsilon_1 := (x^2/2^{c+1}) + (x/2^k)$ and $\epsilon_2 := (1/2^b) + x(12b/2^r)^{\kappa/2}$.

Inner-keyed ($k \le c$)	
Andreeva et al. [1]	$\frac{(\ell q)^2}{2^c} + \frac{\mu Q}{2^k}$
Mennink et al. [16]	$\frac{2\ell q^2}{2^c} + \frac{\mu Q}{2^k} + \frac{2(\ell q)^2}{2^b}$
This paper ($c \le b/2$)	$\frac{3q^2 + qQ + 2r(q+Q)}{2^c} + \frac{\ell q + Q}{2^k} + \frac{(3 + 32e^2 r^{-2})\ell^2 q^2}{2^b}$
This paper ($c > b/2$)	$\left(\frac{18e\ell q(q+Q)}{2^b}\right)^{1/2} + \frac{3q^2 + qQ + 2r(q+Q)}{2^c}$ $+ \frac{\ell q + Q}{2^k} + \frac{3\ell^2 q^2}{2^b}$
Outer-keyed	
Indifferentiability [7]	$\frac{2(\kappa + \ell q + Q)^2}{2^c} + \frac{Q}{2^k}$
Andreeva et al. [1]	$\frac{(\ell q)^2 + 2\mu Q}{2^c} + \frac{2\kappa Q}{2^b} + \lambda(Q)$
Gaži et al. [13]	$\frac{6bq^2 + 8\ell q + qQ}{2^c} + \frac{(6t+17)\ell q^2 + 7\ell qQ + 2q}{2^b}$ $+ \frac{136\ell^4 q^2}{2^{2b}} + \frac{2(\ell q)^{t+1}}{2^{bt}} + \lambda(\ell q + Q)$
This paper ($c \le b/2$)	$\frac{3q^2 + 2qQ + 2r(q+Q)}{2^c}$ $+ \frac{(3.5 + 32e^2 r^{-2})\ell^2 q^2 + 2qQ + 2\kappa Q}{2^b} + \lambda(Q)$
This paper ($c > b/2$)	$\left(\frac{18e\ell q(q+Q)}{2^b}\right)^{1/2} + \frac{3q^2 + 2qQ + 2r(q+Q)}{2^c}$ $+ \frac{3.5\ell^2 q^2 + 2qQ + 2\kappa Q}{2^b} + \lambda(Q)$

permutations on X. For sets X and Y, $\mathsf{Func}(X, Y)$ is the set of all functions: $X \to Y$. We denote by $\emptyset$ an empty set. For sets X and Y, $X \leftarrow Y$ means that set Y is assigned to set X, and $X \overset{\cup}{\leftarrow} Y$ means $X \leftarrow X \cup Y$.

PRF-Security. Through this paper, a distinguisher $\mathbf{D}$ is a computationally unbounded probabilistic algorithm. It is given query access to one or more oracles $\mathcal{O}$, denoted $\mathbf{D}^{\mathcal{O}}$. Its complexity is solely measured by the number of queries made to its oracles. For integers $k > 0$ and $\tau > 0$, let $\mathcal{F}_K : \{0,1\}^* \to \{0,1\}^\tau$ be a keyed hash function based on a permutation having keys $K \in \{0,1\}^k$. The security proof will be done in the ideal model, regarding the underlying permutation as

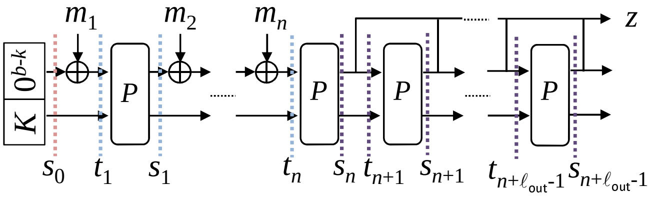

Fig. 1. IKSponge Construction

a random permutation $\mathcal{P} \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^b)$ for an integer $b > 0$. We denote by $\mathcal{P}^{-1}$ its inverse.

The PRF-security of $\mathcal{F}_K$ is defined in terms of indistinguishability between the real world and the ideal world. In the real world, $\mathbf{D}$ has query access to $\mathcal{F}_K$, $\mathcal{P}$, and $\mathcal{P}^{-1}$ for a key $K \xleftarrow{\$} \{0,1\}^k$ and $\mathcal{P} \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^b)$. In the ideal world, it has query access to a random function $\mathcal{R}$, $\mathcal{P}$, and $\mathcal{P}^{-1}$, for $\mathcal{R} \xleftarrow{\$} \mathsf{Func}(\{0,1\}^*, \{0,1\}^\tau)$ and $\mathcal{P} \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^b)$. After $\mathbf{D}$'s interaction, it outputs $y \in \{0,1\}$. The event is denoted by $\mathbf{D} \Rightarrow y$. Then the advantage function is defined as

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathcal{F}}(\mathbf{D}) = \Pr[\mathbf{D}^{\mathcal{F}_K,\mathcal{P},\mathcal{P}^{-1}} \Rightarrow 1] - \Pr[\mathbf{D}^{\mathcal{R},\mathcal{P},\mathcal{P}^{-1}} \Rightarrow 1].$$

We call queries to $\mathcal{F}_K/\mathcal{R}$ "online queries" and queries to $(\mathcal{P},\mathcal{P}^{-1})$ "offline queries." Though this paper, without loss of generality, assume that $\mathbf{D}$ is deterministic and makes no repeated query.

3 Inner Keyed Sponge and the PRF-Security

3.1 Inner Keyed Sponge Construction

The inner keyed sponge construction uses the sponge function as the underlying function. By IKSponge we denote the construction.

First we explain the sponge function. The sponge function is a permutation-based one. For an integer $b > 0$, let $P \in \mathsf{Perm}(\{0,1\}^b)$ be the underlying permutation. By $\mathtt{Sponge}^P$, we denote the sponge function using P. For integers $r > 0$ and $c \geq 0$ with $r + c = b$, r is a bit length so-called rate and c is a bit length so-called capacity. For an input $m \in \{0,1\}^*$, the output $\mathtt{Sponge}^P(m) = z$ is calculated as follows. Firstly, a bit string $\mathsf{pad}(|m|)$ is appended to the suffix of m such that the bit length of $m\|\mathsf{pad}(|m|)$ becomes a multiple of r and the last r-bit block is not 0^r. The example of the padded string is $m\|\mathsf{pad}(|m|) = m\|1\|0^*$, which means that 1 and the minimum number of zeroes so that the bit length becomes a multiple of r. Secondly, the padded bit string is partitioned into r-bit blocks $m_1, \ldots, m_l$, where $m_l \neq 0^r$. Thirdly, b-bit internal state s is updated by the following procedure.

$$s \leftarrow 0^b;\ \text{for } i = 1, \ldots l \text{ do } s \leftarrow P(m_i\|0^c \oplus s)$$

Finally, the $\ell_{\mathrm{out}} \times r$-bit string z is produced by the following procedure.

$$z \leftarrow s[1,r];\ \text{for } i = 1, \dots \ell_{\mathrm{out}} - 1 \text{ do } s \leftarrow P(s); z \leftarrow z \| s[1,r]$$

Next we explain the `IKSponge` construction. For an integer k with $0 < k \leq c$, let $K \in \{0,1\}^k$ be a secret key. By $\mathtt{IKSponge}_K^P$, we denote `IKSponge` with P having K. `IKSponge` equals `Sponge` with the initial value $0^{b-k} \| K$. Concretely, for a message m, the response $\mathtt{IKSponge}_K^P(m) = z$ is denoted as follows, and the figure 1 shows the procedure.

1. Partition $m \| \mathsf{pad}(|m|)$ into r-bit blocks $m_1, \dots, m_n$
2. $s_0 \leftarrow 0^{b-k} \| K$
3. For $i = 1, \dots, n$ do $t_i \leftarrow m_i \| 0^c \oplus s_{i-1}$; $s_i \leftarrow P(t_i)$
4. $z \leftarrow s_n[1,r]$
5. For $i = 1, \dots, \ell_{\mathrm{out}} - 1$ do $t_{n+i} \leftarrow s_{n+i-1}$; $s_{n+i} \leftarrow P(t_{n+i})$; $z \leftarrow z \| s_{n+i}[1,r]$
6. Return z

3.2 PRF-Security of the `IKSponge` Construction

We show the PRF-security of `IKSponge` in the ideal permutation model.

Theorem 1. *Let* $\mathbf{D}$ *be a distinguisher which makes* q *online queries of* r*-bit block length at most* ℓ_{in} *and* Q *offline queries. Then, for any parameter* ρ*, we have* $\mathbf{Adv}^{\mathsf{prf}}_{\mathtt{IKSponge}}(\mathbf{D}) \leq \frac{\ell q + Q}{2^k} + \frac{3q^2 + qQ + 2\rho(q+Q)}{2^c} + \frac{3\ell^2 q^2}{2^b} + 2^{r+1} \times \left(\frac{2e\ell q}{\rho 2^r}\right)^{\rho}$*, where* $\ell = \ell_{\mathrm{in}} + \ell_{\mathrm{out}} - 1$ *and* $e = 2.71828\cdots$ *is Napier's constant.*

Corollary 1. *We assume* $c \leq b/2$*. Then, we put* $\rho = r$*, and without loss of generality, assume* $r \geq 2$ *(otherwise* $r = c = 1$ *and* b*=2). Since* $r \geq b/2$*, we have* $\mathbf{Adv}^{\mathsf{prf}}_{\mathtt{IKSponge}}(\mathbf{D}) \leq \frac{3q^2 + qQ + 2r(q+Q)}{2^c} + \frac{(3 + 32e^2 r^{-2})\ell^2 q^2}{2^b} + \frac{\ell q + Q}{2^k}$.

We assume $c > b/2$*, and put* $\rho = \max\left\{r, \left(\frac{2e \times \ell q}{2^{r-c}(q+Q)}\right)^{1/2}\right\}$*. Then we have* $\mathbf{Adv}^{\mathsf{prf}}_{\mathtt{IKSponge}}(\mathbf{D}) \leq \left(\frac{32e\ell q(q+Q)}{2^b}\right)^{1/2} + \frac{3q^2 + qQ + 2r(q+Q)}{2^c} + \frac{3\ell^2 q^2}{2^b} + \frac{\ell q + Q}{2^k}$.

4 Proof of Theorem 1

We prove the PRF-security of $\mathtt{IKSponge}_K^{\mathcal{P}}$ via three games. We denote these games by Game 1, Game 2, and Game 3. For $i \in \{1,2,3\}$, we let $G_i := (L_i, \mathcal{P}, \mathcal{P}^{-1})$ to which $\mathbf{D}$ has query access in Game i. Note that in each game, $\mathcal{P}$ is independently drawn as $\mathcal{P} \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^b)$. We let $L_1 := \mathtt{IKSponge}_K^{\mathcal{P}}$ and $L_3 := \mathcal{R}$. Hence we have

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathtt{IKSponge}}(\mathbf{D}) = \sum_{i=1}^{2} \left(\Pr[\mathbf{D}^{G_i} \Rightarrow 1] - \Pr[\mathbf{D}^{G_{i+1}} \Rightarrow 1]\right) \ . \qquad (1)$$

Hereafter, we upper-bound $\Pr[\mathbf{D}^{G_i} \Rightarrow 1] - \Pr[\mathbf{D}^{G_{i+1}} \Rightarrow 1]$ for $i \in \{1, 2\}$. Note that we define L_2 before $\Pr[\mathbf{D}^{G_1} \Rightarrow 1] - \Pr[\mathbf{D}^{G_2} \Rightarrow 1]$ is evaluated.

In the following proof, for $\alpha \in \{1, \ldots, Q\}$, we denote an α-th offline query by x^α or y^α, and the response by y^α or x^α, where $y^\alpha = \mathcal{P}(x^\alpha)$ or $x^\alpha = \mathcal{P}^{-1}(y^\alpha)$. For $\alpha \in \{1, \ldots, q\}$, we denote an α-th online query by m^α and the response by z^α. We also use superscripts for other values defined by online queries, e.g., $n^1, t_1^1, s_1^1, n^2, t_1^2, s_1^2$, etc.

4.1 Upper-Bound of $\Pr[\mathbf{D}^{G_1} \Rightarrow 1] - \Pr[\mathbf{D}^{G_2} \Rightarrow 1]$

We start by defining L_2. Let $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_\ell \xleftarrow{\$} \mathsf{Func}(\{0,1\}^b, \{0,1\}^b)$ be random functions. Let $K \xleftarrow{\$} \{0,1\}^k$ be a secret key. For an online query $m \in \{0,1\}^*$, the response $L_2(m) = z$ is defined as follows.

```
1. Partition $m \| \mathsf{pad}(|m|)$ into $r$-bit blocks $m_1, \ldots, m_n$
2. $s_0 \leftarrow 0^{b-k} \| K$
3. For $i = 1, \ldots, n$ do $t_i \leftarrow m_i \| 0^c \oplus s_{i-1}$; $s_i \leftarrow \mathcal{G}_i(t_i)$
4. $z \leftarrow s_n[1, r]$
5. For $i = 1, \ldots, \ell_{\mathrm{out}} - 1$ do $t_{n+i} \leftarrow s_{n+i-1}$; $s_{n+i} \leftarrow \mathcal{G}_{n+i}(t_{n+i})$; $z \leftarrow z \| s_{n+i}[1, r]$
6. Return $z$
```

Transcript. Let $\tau_L = \{(m^1, z^1), \ldots, (m^q, z^q)\}$ be the set of query-response pairs defined by online queries and $\tau_\mathcal{P} = \{(x^1, y^1), \ldots, (x^Q, y^Q)\}$ be the set of query-response pairs defined by offline queries. Additionally, we define sets $\tau_1, \ldots, \tau_\ell$. For $i \in \{1, \ldots, \ell\}$, let $\tau_i = \bigcup_{\alpha=1}^{q} \{(t_i^\alpha, s_i^\alpha)\}$ be the set of all input-output pairs at the i-th block defined by online queries. Note that for $\alpha \in \{1, \ldots, q\}, i \in \{1, \ldots, \ell\}$ if (t_i^α, s_i^α) is not defined then $\{(t_i^\alpha, s_i^\alpha)\}$ is an empty set.

This proof permits $\mathbf{D}$ to obtain these sets and a secret key K after $\mathbf{D}$'s interaction but before it outputs a result. We let $\tau_{1..\ell} = \bigcup_{i=1}^{\ell} \tau_i$. Then $\mathbf{D}$'s transcript is summarized as $\tau = \{\tau_L, \tau_\mathcal{P}, \tau_{1..\ell}, K\}$.

Let T_1 be the transcript in Game 1 obtained by sampling $K \xleftarrow{\$} \{0,1\}^k$ and $\mathcal{P} \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^b)$. Let T_2 be the transcript in Game 2 obtained by sampling $K \xleftarrow{\$} \{0,1\}^k$, $\mathcal{P} \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^b)$, $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_\ell \xleftarrow{\$} \mathsf{Func}(\{0,1\}^b, \{0,1\}^b)$. We call τ *valid* if an interaction with their oracles could render this transcript, namely, $\Pr[\mathsf{T}_i = \tau] > 0$ for $i \in \{1, 2\}$. Then $\Pr[\mathbf{D}^{G_1} \Rightarrow 1] - \Pr[\mathbf{D}^{G_2} \Rightarrow 1]$ is upper-bounded by the statistical distance of transcripts, i.e.,

$$\Pr[\mathbf{D}^{G_1} \Rightarrow 1] - \Pr[\mathbf{D}^{G_2} \Rightarrow 1] \leq \mathsf{SD}(\mathsf{T}_1, \mathsf{T}_2) = \frac{1}{2} \sum_{\tau} |\Pr[\mathsf{T}_1 = \tau] - \Pr[\mathsf{T}_2 = \tau]| \ ,$$

where the sum is over all valid transcripts.

Coefficient H Technique. We upper-bound the statistical distance by using the coefficient H technique [18, 12]. In this technique, firstly, we need to partition valid transcripts into good transcripts $\mathcal{T}_{\mathsf{good}}$ and bad transcripts $\mathcal{T}_{\mathsf{bad}}$. Then we can upper-bound the statistical distance $\mathsf{SD}(\mathsf{T}_1, \mathsf{T}_2)$ by the following lemma.

Lemma 1 (Coefficient H Technique). *Let* $0 \leq \varepsilon \leq 1$ *be such that for all* $\tau \in \mathcal{T}_{\mathsf{good}}$, $\frac{\Pr[\mathsf{T}_1=\tau]}{\Pr[\mathsf{T}_2=\tau]} \geq 1-\varepsilon$. *Then,* $\mathsf{SD}(\mathsf{T}_1, \mathsf{T}_2) \leq \varepsilon + \Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}]$.

The proof of the lemma is given in [12]. Hence, we can upper-bound $\Pr[\mathbf{D}^{G_1} \Rightarrow 1] - \Pr[\mathbf{D}^{G_2} \Rightarrow 1]$ by defining good and bad transcripts and by evaluating ε and $\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}]$.

Good and Bad Transcripts. We define $\mathcal{T}_{\mathsf{bad}}$ that satisfies one of the following conditions.

- $\mathsf{hit}_{\mathsf{tx,sy}} \Leftrightarrow \exists (t,s) \in \tau_{1..\ell}, (x,y) \in \tau_{\mathcal{P}}$ s.t. $t = x \vee s = y$
- $\mathsf{hit}_{\mathsf{tt}} \Leftrightarrow \exists i,j \in \{1,\ldots,\ell\}$ with $i \neq j$ s.t. $\exists (t_i,s_i) \in \tau_i, (t_j,s_j) \in \tau_j$ s.t. $t_i = t_j$
- $\mathsf{hit}_{\mathsf{ss}} \Leftrightarrow \exists (t,s),(t',s') \in \tau_{1..\ell}$ s.t. $t \neq t' \wedge s = s'$

$\mathcal{T}_{\mathsf{good}}$ is defined such that the above conditions are not satisfied.

Upper-Bound of $\mathbf{Pr[T_2 \in \mathcal{T}_{bad}]}$. We start by defining additional conditions mcoll_T, mcoll_S, and $\mathsf{coll}_{\mathsf{tt}}$. Firstly, we define mcoll_T and mcoll_S which are $(q+\rho)$- and ρ-multi-collision conditions for sets T and S, respectively. Here, T keeps all inputs to $\mathcal{G}_2, \ldots, \mathcal{G}_\ell$, and S keeps all outputs of $\mathcal{G}_1, \ldots, \mathcal{G}_\ell$, where $T := \bigcup_{\alpha=1}^{q} \bigcup_{i=2}^{n^\alpha+\ell_{\mathrm{out}}-1} \{t_i^\alpha\}$ and $S := \bigcup_{\alpha=1}^{q} \bigcup_{i=1}^{n^\alpha+\ell_{\mathrm{out}}-1} \{s_i^\alpha\}$. Note that sets T and S do not keep duplex elements, and T does not keep inputs to $\mathcal{G}_1$. Then the conditions are defined as

$$\mathsf{mcoll}_T \Leftrightarrow \exists t^{(1)}, t^{(2)}, \ldots, t^{(q+\rho)} \in T \text{ s.t. } t^{(1)}[1,r] = t^{(2)}[1,r] = \cdots = t^{(q+\rho)}[1,r]$$
$$\mathsf{mcoll}_S \Leftrightarrow \exists s^{(1)}, s^{(2)}, \ldots, s^{(\rho)} \in S \text{ s.t. } s^{(1)}[1,r] = s^{(2)}[1,r] = \cdots = s^{(\rho)}[1,r]$$

where ρ is a free parameter which was described in Theorem 1. We let $\mathsf{mcoll} := \mathsf{mcoll}_T \vee \mathsf{mcoll}_S$. Secondly, we define $\mathsf{coll}_{\mathsf{tt}}$ which is a collision condition for inputs to a random function in L_2. The condition is defined as follows.

$$\begin{aligned}\mathsf{coll}_{\mathsf{tt}} \Leftrightarrow & \exists \alpha, \beta \in \{1,\ldots,q\} \text{ with } \alpha \neq \beta, i \in \{2,\ldots,\min\{n^\alpha,n^\beta\}+\ell_{\mathrm{out}}-1\} \\ & \text{s.t. } t_{i-1}^\alpha \neq t_{i-1}^\beta \wedge t_i^\alpha = t_i^\beta .\end{aligned}$$

Then we have

$$\begin{aligned}\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}] \leq & \Pr[\mathsf{hit}_{\mathsf{tx,sy}} \vee \mathsf{hit}_{\mathsf{tt}} \vee \mathsf{hit}_{\mathsf{ss}}] \\ \leq & \Pr[\mathsf{hit}_{\mathsf{ss}}] + \Pr[\mathsf{coll}_{\mathsf{tt}}] + \Pr[\mathsf{mcoll}_S] + \Pr[\mathsf{mcoll}_T | \neg\mathsf{coll}_{\mathsf{tt}}] \\ & + \Pr[\mathsf{hit}_{\mathsf{tx,sy}} | \neg\mathsf{mcoll}] + \Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll})] \ . \qquad (2)\end{aligned}$$

►We upper-bound $\Pr[\mathsf{hit}_{\mathsf{ss}}]$. Note that $|\tau_{1..\ell}| \leq \ell q$ holds, and for all $(t,s) \in \tau_{1..\ell}$ s is randomly drawn from $\{0,1\}^b$. Hence we have $\Pr[\mathsf{hit}_{\mathsf{ss}}] \leq \binom{\ell q}{2} \times \frac{1}{2^b} = \frac{0.5\ell^2 q^2}{2^b}$.

►We upper-bound $\Pr[\mathsf{hit}_{\mathsf{tx,sy}} | \neg\mathsf{mcoll}]$. Note that $\mathsf{hit}_{\mathsf{tx,sy}}$ implies that

$$\exists \alpha \in \{1,\ldots,q\}, i \in \{1,\ldots,n^\alpha+\ell_{\mathrm{out}}-1\}, \beta \in \{1,\ldots,Q\} \text{ s.t. } t_i^\alpha = x^\beta \vee s_i^\alpha = y^\beta .$$

We then consider the following cases.

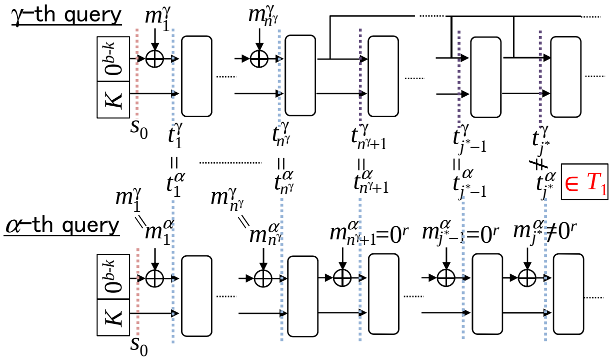

Fig. 2. Procedures for $\boxed{\text{set } T_1}$ and $\mathsf{prefix}^{=}_{m^\alpha}$

Case 1 $\Leftrightarrow \mathsf{hit}_{\mathsf{tx,sy}} \wedge t_i^\alpha = x^\beta \wedge i = 1$:
Note that t_1^α has the form $t_1^\alpha = m_1^\alpha \| 0^c \oplus 0^{b-k} \| K$. Since K is randomly drawn from $\{0,1\}^k$, the probability that Case 1 holds is at most $\frac{Q}{2^k}$.

Case 2 $\Leftrightarrow \mathsf{hit}_{\mathsf{tx,sy}} \wedge t_i^\alpha = x^\beta \wedge i \neq 1$:
By $\neg\mathsf{mcoll}_T$, the number of elements in T whose first r bits are equal to $x^\beta[1,r]$ is at most $q+\rho$. We note that for some r-bit block M^α, t_i^α has the form $t_i^\alpha = M^\alpha \| 0^c \oplus s_{i-1}^\alpha$, where M^α is 0^r or a message block. Since $s_{i-1}^\alpha[r+1,b]$ is randomly drawn from $\{0,1\}^c$, the probability that Case 2 holds is at most $\frac{(q+\rho)Q}{2^c}$.

Case 3 $\Leftrightarrow \mathsf{hit}_{\mathsf{tx,sy}} \wedge s_i^\alpha = y^\beta$:
By $\neg\mathsf{mcoll}_S$, the number of elements in S whose first r bits are equal to $y^\beta[1,r]$ is at most ρ. Since $s_i^\alpha[r+1,b]$ is randomly drawn from $\{0,1\}^c$, the probability that Case 3 holds is at most $\frac{\rho Q}{2^c}$.

Hence we have $\Pr[\mathsf{hit}_{\mathsf{tx,sy}} | \neg(\mathsf{hit}_{\mathsf{ux,wy}} \vee \mathsf{mcoll})] \leq \frac{Q}{2^k} + \frac{(q+2\rho)Q}{2^c}$.

►We upper-bound $\Pr[\mathsf{mcoll}_S]$. Fix $s \in \{0,1\}^r$ and $s^{(1)}, s^{(2)}, \ldots, s^{(\rho)} \in S$. Since they are randomly drawn from $\{0,1\}^b$, the probability that $s^{(1)}[1,r] = s^{(2)}[1,r] = \cdots = s^{(\rho)}[1,r] = s$ holds is at most $\left(\frac{1}{2^r}\right)^\rho$. By $s \in \{0,1\}^r$ and $|S| \leq \ell q$, we have $\Pr[\mathsf{mcoll}_S] \leq 2^r \times \binom{\ell q}{\rho} \times \left(\frac{1}{2^r}\right)^\rho \leq 2^r \times \left(\frac{e\ell q}{\rho} \times \frac{1}{2^r}\right)^\rho$, using Stirling's approximation $(x! \geq (x/e)^x$ for any $x)$.

► We upper-bound $\Pr[\mathsf{mcoll}_T | \neg\mathsf{coll}_{\mathsf{tt}}]$. First we partition set T into two sets T_1 and T_2. Roughly speaking, T_1 keeps all inputs to random functions whose first r bits can be controlled by message blocks. The figure 2 (with the boxed statement) depicts the procedure of L_2 corresponding with T_1, which considers γ-th and α-th online queries with $\gamma < \alpha$ and $n^\gamma < n^\alpha$ (n^γ and n^α are the query lengths in blocks at the γ-th and α-th online queries, respectively) such that these message blocks satisfy the condition: $\exists j^* \in \{n^\gamma+1, \ldots, n^\gamma + \ell_{\mathrm{out}} - 1\}$ s.t. $m_1^\alpha = m_1^\gamma, m_2^\alpha = m_1^\gamma, \ldots, m_{n^\gamma}^\alpha = m_{n^\gamma}^\gamma, m_{n^\gamma}^\alpha = 0^r, \ldots, m_{j^*-1}^\alpha = 0^r, m_{j^*}^\alpha \neq 0^r$. We call the condition between the α-th and γ-th online queries "prefix condition."

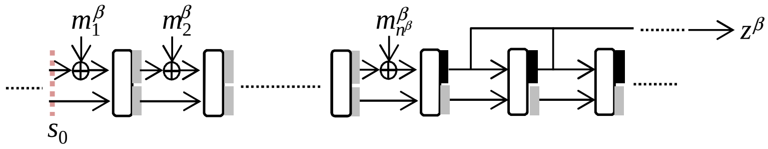

Fig. 3. Lazy sampling random functions in Case 2, where black boxes represent outputs defined at the β-th query and gray boxes represent outputs defined after **D**'s interaction.

In this case, $t_{j^*}^\alpha$ becomes an element of T_1. Since $s_{j^*-1}^\alpha = s_{j^*-1}^\gamma$ holds and before the α-th online query a distinguisher can find $s_{j^*-1}^\gamma[1,r]$ which is the part of output blocks at the γ-th online query, he can assign any value to $t_{j^*}^\alpha[1,r]$ by using the message block $m_{j^*}^\alpha$. We call the input $t_{j^*}^\alpha$ "controllable input," and T_1 keeps all controllable inputs. The definitions of these sets are given as follows.

$$\begin{aligned}T_1 :=\Big\{ t_{j^*}^\alpha \in T : (\alpha \in \{2,\dots,q\}) \wedge \Big(\exists \gamma \in \{1,\dots,\alpha-1\} \text{ s.t. } \big(n^\gamma < n^\alpha\big) \\ \wedge \big(\forall j \in \{1,\dots,n^\gamma\} : m_j^\alpha = m_j^\gamma\big) \wedge \big(\exists j^* \in \{n^\gamma+1,\dots,n^\gamma+\ell_{\text{out}}-1\} \text{ s.t.} \\ (\forall j \in \{n^\gamma+1,\dots,j^*-1\} : m_j^\alpha = 0^r) \wedge (m_{j^*}^\alpha \neq 0^r)\big)\Big)\Big\} \ ,\end{aligned}$$

and $T_2 := T \backslash T_1$. Note that for any $\alpha_1, \alpha_2, \dots, \alpha_i \in \{1,\dots,q\}$ with $\alpha_1 < \alpha_2 < \dots < \alpha_i$ and with the prefix relations, the number of controllable inputs is at most $i-1$, because set T_1 does not keep duplex elements. Hence, we have $|T_1| \leq q-1$, and thereby $\Pr[\mathsf{mcoll}_T | \neg\mathsf{coll}_{\mathsf{tt}}]$ is upper-bounded by the probability that a ρ-multi-collision occurs in T_2 under the condition $\neg\mathsf{coll}_{\mathsf{tt}}$, that is, $\exists t^{(1)}, t^{(2)}, \dots, t^{(\rho)} \in T_2$ s.t. $t^{(1)}[1,r] = t^{(2)}[1,r] = \dots = t^{(\rho)}[1,r]$. Hereafter, we upper-bound the ρ-multi-collision probability under the condition $\neg\mathsf{coll}_{\mathsf{tt}}$.

Fix $t \in \{0,1\}^r$ and $t_i^\alpha \in T_2$ with $\alpha \in \{1,\dots,q\}$ and $i \in \{2,\dots,n^\alpha+\ell_{\text{out}}-1\}$. We upper-bound the probability that $t_i^\alpha[1,r] = t$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}}$. We consider the following cases.

Case 1 $\Leftrightarrow (t_i^\alpha[1,r] = t) \wedge (n^\alpha + 1 \leq i)$:
By $n^\alpha + 1 \leq i$, $t_i^\alpha = s_{i-1}^\alpha$ holds, where $s_{i-1}^\alpha = \mathcal{G}_{i-1}(t_{i-1}^\alpha)$. By $\neg\mathsf{coll}_{\mathsf{tt}}$, s_{i-1}^α is randomly drawn from at least $2^b - q$ values. Thus, the probability that Case 1 holds is at most $\frac{2^c}{2^b-q}$.

Case 2 $\Leftrightarrow (t_i^\alpha[1,r] = t) \wedge (2 \leq i \leq n^\alpha)$:
In the evaluation, we lazy sample random functions $\mathcal{G}_1, \dots, \mathcal{G}_\ell$ that is consistent with the condition $\neg\mathsf{coll}_{\mathsf{tt}}$. The procedure is shown bellow.

- At the β-th online query with $\beta \in \{1,\dots,q\}$, the following procedure is performed.
  - For $j \in \{n^\beta, \dots, n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[1,r]$ is randomly drawn from $\{0,1\}^r$.
- After **D**'s interaction, the following procedure is performed.
  - For all $\beta \in \{1,\dots,q\}$ and $j \in \{1,\dots,n^\beta-1\}$, if t_j^β is a new input to $\mathcal{G}_j$ then s_j^β is randomly drawn from $\{0,1\}^b$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}$.

- For all $\beta \in \{1, \dots, q\}$ and $j \in \{n^\beta, \dots, n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[r+1, b]$ is randomly drawn from $\{0,1\}^c$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}$.

The figure 3 depicts the above procedure. Without loss of generality, assume that $q < 2^c$ (If $q \geq 2^c$ then the advantage of Theorem 1 becomes 1 or more). Note that for each random function, there are at most q inputs, and for $a \in \{0,1\}^r$, there are 2^c elements in $\{0,1\}^b$ whose first r bits are equal to a. Thus, for all $\beta \in \{1, \dots, q\}$ and $j \in \{n^\beta, \dots, n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[r+1, b]$ can be defined such that it is consistent with the condition $\neg\mathsf{coll}_{\mathsf{tt}}$. Thus, the above procedure realizes random functions $\mathcal{G}_1, \dots, \mathcal{G}_\ell$ that are consistent with the condition $\neg\mathsf{coll}_{\mathsf{tt}}$.

For $2 \leq i \leq n^\alpha$, t_i^α has the form $t_i^\alpha = m_i^\alpha \| 0^c \oplus s_{i-1}^\alpha$. By the above procedure, s_{i-1}^α is randomly drawn from at least $2^b - q$ values after $\mathbf{D}$'s interaction (i.e., after m_i^α is determined). Hence, the probability that $t_i^\alpha[1, r] = t$ holds is at most $\frac{2^c}{2^b - q}$.

We next fix $t^{(1)}, t^{(2)}, \dots, t^{(\rho)} \in T_2$ and $t \in \{0,1\}^r$. By the above evaluations, the probability that $t^{(1)}[1,r] = t^{(2)}[1,r] = \cdots = t^{(\rho)}[1,r] = t$ holds is at most $\left(\frac{2^c}{2^b - q}\right)^\rho \leq \left(\frac{2}{2^r}\right)^\rho$, assuming $q \leq 2^{b-1}$. By $t \in \{0,1\}^r$ and $|T_2| \leq \ell q$, we have $\Pr[\mathsf{mcoll}_T | \neg\mathsf{coll}_{\mathsf{tt}}] \leq 2^r \times \binom{\ell q}{\rho} \times \left(\frac{2}{2^r}\right)^\rho \leq 2^r \times \left(\frac{e\ell q}{\rho} \times \frac{2}{2^r}\right)^\rho$, using Stirling's approximation ($x! \geq (x/e)^x$ for any x).

►We upper-bound $\Pr[\mathsf{coll}_{\mathsf{tt}}]$. We denote by $\mathsf{coll}_{\mathsf{tt}}^\alpha$ the condition where at the α-th online query $\mathsf{coll}_{\mathsf{tt}}$ holds. Then we have
$\Pr[\mathsf{coll}_{\mathsf{tt}}] \leq \sum_{\alpha=2}^q \Pr[\mathsf{coll}_{\mathsf{tt}}^\alpha \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}] \leq \sum_{\alpha=2}^q \Pr[\mathsf{coll}_{\mathsf{tt}}^\alpha | \neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}]$.

Next we fix $\alpha \in \{2, \dots, q\}$, and upper-bound $\Pr[\mathsf{coll}_{\mathsf{tt}}^\alpha | \neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}]$, which is the probability that $\mathsf{coll}_{\mathsf{tt}}$ holds at the α-th online query when it does not hold up to the $(\alpha - 1)$-th online query. In order to upper-bound the probability, we consider two cases with respect to the following condition.

$$\begin{aligned}\mathsf{prefix}_{m^\alpha}^{=} \Leftrightarrow & \exists\gamma \in \{1, \dots, \alpha-1\} \text{ s.t. } \left(n^\gamma < n^\alpha\right) \wedge \left(\forall j \in \{1, \dots, n^\gamma\} : m_j^\gamma = m_j^\alpha\right) \\ & \wedge \big(\exists j^* \in \{n^\gamma + 1, \dots, n^\gamma + \ell_{\text{out}} - 1\} \text{ s.t.} \\ & \qquad m_{n^\gamma+1}^\alpha = 0^r, \dots, m_{j^*-1}^\alpha = 0^r, m_{j^*}^\alpha \neq 0^r\big).\end{aligned}$$

We call such γ-th online query "prefix online query" of the α-th query, and such j^* "distinct point." The figure 2 (without the boxed statement) depicts the procedures of L_2 corresponding with the condition. In this evaluation, similar to Case 2 of $\Pr[\mathsf{mcoll}_T | \neg\mathsf{coll}_{\mathsf{tt}}]$, we lazy sample random functions $\mathcal{G}_1, \dots, \mathcal{G}_\ell$ that are consistent with the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}$. The procedure is shown bellow.

- At the β-th online query with $\beta \in \{1, \dots, \alpha - 1\}$, the following procedure is performed.
  - For all $j \in \{n^\beta, \dots, n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[1, r]$ is randomly drawn from $\{0,1\}^r$.
- At the α-th online query, the following procedure is performed.
  - For all $\beta \in \{1, \dots, \alpha - 1\}$,

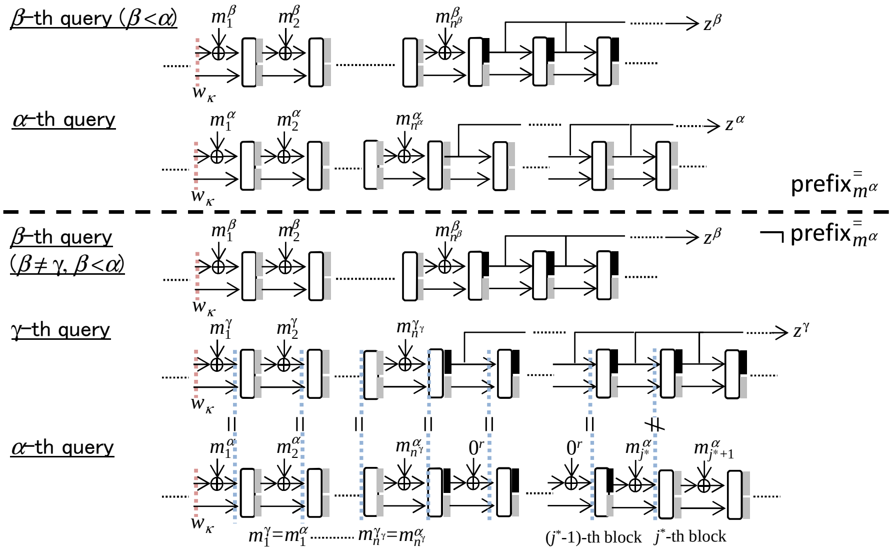

Fig. 4. Lazy sampling random functions in the evaluation of $\Pr[\mathsf{coll}_{\mathsf{tt}}^{\alpha} | \neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}]$, where black boxes represent outputs defined up to the $(\alpha-1)$-th query and gray boxes represent outputs defined at the α-th query.

  - $*$ for all $j \in \{1,\dots,n^\beta - 1\}$, if t_j^β is a new input to $\mathcal{G}_j$ then the response s_j^β is randomly drawn from $\{0,1\}^b$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}$,
  - $*$ for all $j \in \{n^\beta,\dots,n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[r+1,b]$ is randomly drawn from $\{0,1\}^c$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}$.
- For $j \in \{1,\dots,n^\alpha + \ell_{\text{out}} - 1\}$, if t_j^α is a new input to $\mathcal{G}_j$ then the response s_j^α is randomly drawn from $\{0,1\}^b$.

The top (resp., the bottom) of the figure 4 depicts the above procedure under the condition $\mathsf{prefix}_{m^\alpha}^{=}$ (resp., $\neg\mathsf{prefix}_{m^\alpha}^{=}$). Then we evaluate the probability $\Pr[\mathsf{coll}_{\mathsf{tt}}^{\alpha} | \neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1}]$ as follows.

Case 1 $\Leftrightarrow \mathsf{coll}_{\mathsf{tt}}^{\alpha}$ under the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=}$:
For $i \in \{2,\dots,n^\alpha + \ell_{\text{out}} - 1\}$, let $\mathsf{coll}_{\mathsf{tt}}^{\alpha,i}$ be the condition where $\mathsf{coll}_{\mathsf{tt}}^{\alpha}$ holds at the i-th block of the α-th online query, and let $\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1} := \mathsf{coll}_{\mathsf{tt}}^{\alpha,2} \vee \mathsf{coll}_{\mathsf{tt}}^{\alpha,3} \vee \cdots \vee \mathsf{coll}_{\mathsf{tt}}^{\alpha,i-1}$. Note that for $i \in \{2,\dots,n^\alpha + \ell_{\text{out}} - 1\}$, $\mathsf{coll}_{\mathsf{tt}}^{\alpha,i} \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$ is the condition where $\mathsf{coll}_{\mathsf{tt}}^{\alpha}$ holds at the i-th block of the α-th online query for the first time. (i.e., $\mathsf{coll}_{\mathsf{tt}}^{\alpha}$ does not hold up to the $(i-1)$-th block), and thus $\mathsf{coll}_{\mathsf{tt}}^{\alpha} \Leftrightarrow \bigvee_{i=2}^{n^\alpha+\ell_{\text{out}}-1} (\mathsf{coll}_{\mathsf{tt}}^{\alpha,i} \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1})$, where $\mathsf{coll}_{\mathsf{tt}}^{\alpha,2} \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,1} := \mathsf{coll}_{\mathsf{tt}}^{\alpha,2}$. In the following, for $i \in \{2,\dots,n^\alpha + \ell_{\text{out}} - 1\}$, we assume that $\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$ does not hold, and thus upper-bound the probability that $\mathsf{coll}_{\mathsf{tt}}^{\alpha,i}$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=}$. By $p_{1,i}$, we denote the probability. Note that for some r-bit string M^α t_i^α has the form $t_i^\alpha = M^\alpha \| 0^c \oplus s_{i-1}^\alpha$, where M^α is a message block or 0^r. By the condition

$\neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$, t_{i-1}^{α} is a new input to $\mathcal{G}_{i-1}$, and thereby s_{i-1}^{α} is randomly drawn from $\{0,1\}^b$ after M^α is determined. Hence, we have $p_{1,i} \leq (\alpha-1) \times \frac{1}{2^b}$, and thereby $\Pr[\textbf{Case 1}] \leq \ell \times (\alpha-1) \times \frac{1}{2^b}$.

Case 2 $\Leftrightarrow \mathsf{coll}_{\mathsf{tt}}^{\alpha}$ under the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1} \wedge \mathsf{prefix}_{m^\alpha}^{=}$:

In this analysis, we use the conditions $\mathsf{coll}_{\mathsf{tt}}^{\alpha,i}$ and $\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$ defined above. For $i \in \{2,\ldots,n^\alpha+\ell_{\mathrm{out}}-1\}$, we assume that $\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$ does not hold, and thus upper-bound the probability that $\mathsf{coll}_{\mathsf{tt}}^{\alpha,i}$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1} \wedge \mathsf{prefix}_{m^\alpha}^{=}$. By $p_{2,i}$, we denote the probability. We assume that the γ-th online query ($\gamma \in \{1,\ldots,\alpha-1\}$) is the prefix online query of the α-th online query, and j^* is the distinct point. If there are two or more prefix online queries of the α-th online query then we consider the prefix online query such that the distinct point is maximum.

- Firstly, we consider the case of $i \in \{2,\ldots,j^*-1\}$. By $\mathsf{prefix}_{m^\alpha}^{=}$, $t_i^\alpha = t_i^\gamma$ holds. By the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$, we have $p_{2,i}=0$.
- Secondly, we consider the case of $i=j^*$. Note that $t_{j^*}^{\alpha}[r+1,b] = s_{j^*-1}^{\alpha}[r+1,b]$ holds, and by the lazy sampled random functions, $s_{j^*-1}^{\alpha}$ is randomly drawn from at least 2^b-q values. Thus we have $p_{2,i} \leq (\alpha-1) \times \frac{2^r}{2^b-q}$.
- Finally, we consider the case of $i \in \{j^*+1,\ldots,n^\alpha+\ell_{\mathrm{out}}-1\}$. In this case, for some r-bit string M^α, t_i^α has the form $t_i^\alpha = M^\alpha \| 0^c \oplus s_{i-1}^\alpha$, where M^α is a message block or 0^r. Since j^* is maximum and by the condition $\neg\mathsf{coll}_{\mathsf{tt}}^{\leq\alpha,i-1}$ t_{i-1}^{α} is a new input to $\mathcal{G}_{i-1}$, s_{i-1}^α is randomly drawn from $\{0,1\}^b$ after M^α is determined. Hence, we have $p_{2,i} \leq (\alpha-1) \times \frac{1}{2^b}$.

Hence, we have $\Pr[\textbf{Case 2}] \leq (\alpha-1) \times \left(\frac{2^r}{2^b-q} + \frac{\ell_{\mathrm{out}}}{2^b}\right)$.

Finally, we assume that $q \leq 2^{b-1}$. We then have $\Pr[\mathsf{coll}_{\mathsf{tt}}] \leq \sum_{\alpha=2}^{q}(\alpha-1) \times \max\left\{\frac{\ell}{2^b}, \left(\frac{2^r}{2^b-q} + \frac{\ell_{\mathrm{out}}}{2^b}\right)\right\} \leq \frac{q^2}{2^c} + \frac{0.5\ell q^2}{2^b}$.

►We upper-bound $\Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll})]$. We start by defining the following condition.

$$\mathsf{hit}_K \Leftrightarrow \exists\alpha \in \{1,\ldots,q\}, i \in \{2,\ldots,n^\alpha+\ell_{\mathrm{out}}-1\} \text{ s.t. } t_i^\alpha[r+1,b] = 0^{c-k}\|K$$

Then we have

$$\Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll})] \leq \Pr[\mathsf{hit}_K] + \Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll}) \wedge \neg\mathsf{hit}_K]\ .$$

Since K is randomly drawn from $\{0,1\}^k$, we have $\Pr[\mathsf{hit}_K] \leq \frac{\ell q}{2^k}$.

Next, we upper-bound $\Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll}) \wedge \neg\mathsf{hit}_K]$. Note that $\mathsf{hit}_{\mathsf{tt}}$ implies that

$$\begin{aligned}&\exists\alpha,\beta \in \{1,\ldots,q\}, i \in \{1,\ldots,n^\alpha+\ell_{\mathrm{out}}-1\}, j \in \{1,\ldots,n^\beta+\ell_{\mathrm{out}}-1\}\\ &\quad \text{s.t. } i \neq j \wedge t_i^\alpha = t_j^\beta.\end{aligned}$$

For $\alpha \in \{1,\ldots,q\}$, we define a condition where $\mathsf{hit}_{\mathsf{tt}}$ holds up to the α-th online query. The concrete definition is given bellow.

$$\begin{aligned}\mathsf{hit}_{\mathsf{tt}}^{\alpha} \Leftrightarrow &\exists\beta,\gamma \in \{1,\ldots,\alpha\}, i \in \{1,\ldots,n^\beta+\ell_{\mathrm{out}}-1\}, j \in \{1,\ldots,n^\gamma+\ell_{\mathrm{out}}-1\}\\ &\text{s.t. } i \neq j \wedge t_i^\beta = t_j^\gamma.\end{aligned}$$

Then the following inequation holds.

$$\begin{aligned}&\Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll}) \wedge \mathsf{hit}_K]\\ &\le \sum_{\alpha=1}^{q} \Pr[\mathsf{hit}_{\mathsf{tt}}^{\alpha} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg(\mathsf{mcoll} \vee \mathsf{coll}_{\mathsf{tt}}) \wedge \neg\mathsf{hit}_K]\\ &\le \sum_{\alpha=1}^{q} \Pr[\mathsf{hit}_{\mathsf{tt}}^{\alpha} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll} \wedge \neg\mathsf{hit}_K | \neg\mathsf{coll}_{\mathsf{tt}}] \enspace .\end{aligned}$$

First fix $\alpha \in \{1, \ldots, q\}$, and upper-bound the probability $\Pr[\mathsf{hit}_{\mathsf{tt}}^{\alpha} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll} \wedge \neg\mathsf{hit}_K | \neg\mathsf{coll}_{\mathsf{tt}}]$. In this evaluation, we lazy sample random functions $\mathcal{G}_1, \ldots, \mathcal{G}_\ell$ by the similar way to the evaluation of $\Pr[\mathsf{coll}_{\mathsf{tt}}]$. The procedure is shown bellow, and the figure 4 depicts the procedure.

- At the β-th online query with $\beta \in \{1, \ldots, \alpha-1\}$, the following procedure is performed.
  - For all $j \in \{n^\beta, \ldots, n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[1, r]$ is randomly drawn from $\{0,1\}^r$.
- At the α-th online query, the following procedure is performed.
  - For all $\beta \in \{1, \ldots, \alpha-1\}$,
    - for all $j \in \{1, \ldots, n^\beta - 1\}$, if t_j^β is a new input to $\mathcal{G}_j$ then the response s_j^β is randomly drawn from $\{0,1\}^b$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}$,
    - for all $j \in \{n^\beta, \ldots, n^\beta + \ell_{\text{out}} - 1\}$, $s_j^\beta[r+1, b]$ is randomly drawn from $\{0,1\}^c$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}$.
  - For $j \in \{1, \ldots, n^\alpha + \ell_{\text{out}} - 1\}$, if t_j^α is a new input to $\mathcal{G}_j$ then the response s_j^α is randomly drawn from $\{0,1\}^b$, keeping the condition $\neg\mathsf{coll}_{\mathsf{tt}}$.

In this evaluation, we consider two cases with respect to the condition $\mathsf{prefix}_{m^\alpha}^{=}$ which was defined in the analysis of $\Pr[\mathsf{coll}_{\mathsf{tt}}]$. In addition, the following analyses use the terms "prefix online query" and "distinct point."

Case 1 $\Leftrightarrow$ $\mathsf{hit}_{\mathsf{tt}}^{\alpha} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll} \wedge \neg\mathsf{hit}_K$ under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=}$: For $i \in \{1, \ldots, n^\alpha + \ell_{\text{out}} - 1\}$, let $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i}$ be the condition where $\mathsf{hit}_{\mathsf{tt}}^{\alpha}$ holds at the i-th block of the α-th online query, that is,

$$\begin{aligned}\mathsf{hit}_{\mathsf{tt}}^{\alpha,i} \Leftrightarrow &(\exists \beta \in \{1, \ldots, \alpha-1\}, j \in \{1, \ldots, n^\beta + \ell_{\text{out}} - 1\} \text{ s.t. } i \neq j \wedge t_i^\alpha = t_j^\beta)\\ &\wedge (\exists j \in \{1, \ldots, i-1\} \text{ s.t. } t_i^\alpha = t_j^\alpha).\end{aligned}$$

Then $\mathsf{hit}_{\mathsf{tt}}^{\alpha} \Rightarrow \bigvee_{i=1}^{n^\alpha + \ell_{\text{out}} - 1} \mathsf{hit}_{\mathsf{tt}}^{\alpha,i}$. In the following, for $i \in \{1, \ldots, n^\alpha + \ell_{\text{out}} - 1\}$, we upper-bound the probability that $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll} \wedge \neg\mathsf{hit}_K$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=}$. By $p_{1,i}$, we denote the probability.

- Firstly, we consider the case of $i = 1$. In addition to the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=}$, we assume that hit_K does not hold, and don't consider the condition $\neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll}$. Since t_1^α has the form $t_1^\alpha = (m_1^\alpha \| 0^c) \oplus (0^{b-k} \| K)$, the probability that $\mathsf{hit}_{\mathsf{tt}}^{\alpha,1}$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=} \wedge \neg\mathsf{hit}_K$ is 0 and thus we have $p_{1,1} = 0$.

- Secondly, we consider the case of $i \geq 2$. In this case, we don't consider the condition $\neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll} \wedge \neg\mathsf{hit}_K$. Note that for an r-bit string M^α, t_i^α has the form $t_i^\alpha = M^\alpha \| 0^c \oplus s_{i-1}^\alpha$, where M^α is a message block or 0^r. Since s_{i-1}^α is randomly drawn from at least $2^b - q$ values after M^α is defined, the probability that $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i}$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \neg\mathsf{prefix}_{m^\alpha}^{=}$ is at most $\frac{(\ell-1)(\alpha-1)+(i-1)}{2^b-q} \leq \frac{(\ell-1)\alpha}{2^b-q}$, and thus we have $p_{1,i} \leq \frac{(\ell-1)\alpha}{2^b-q}$.

Hence, we have $\Pr[\textbf{Case 1}] \leq (\ell-1) \times \frac{(\ell-1)\alpha}{2^b-q}$.

Case 2 $\Leftrightarrow \mathsf{hit}_{\mathsf{tt}}^{\alpha} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \wedge \neg\mathsf{mcoll} \wedge \neg\mathsf{hit}_K$ under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \mathsf{prefix}_{m^\alpha}^{=}$: In this analysis, we use the condition $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i}$ for $i \in \{1, \ldots, n^\alpha + \ell_{\mathrm{out}} - 1\}$, defined in Case 1. We let $\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1} := \mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \vee \mathsf{hit}_{\mathsf{tt}}^{\alpha,1} \vee \cdots \vee \mathsf{hit}_{\mathsf{tt}}^{\alpha,i-1}$, where $\mathsf{hit}_{\mathsf{tt}}^{\alpha,0} := \mathsf{hit}_{\mathsf{tt}}^{\alpha-1}$. Then the following holds: $\mathsf{hit}_{\mathsf{tt}}^{\alpha} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\alpha-1} \Rightarrow \bigvee_{i=1}^{n^\alpha+\ell_{\mathrm{out}}-1} (\mathsf{hit}_{\mathsf{tt}}^{\alpha,i} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1})$. In this evaluation, we don't consider the condition $\neg\mathsf{hit}_K$, and thus for $i \in \{1, \ldots, n^\alpha + \ell_{\mathrm{out}} - 1\}$, upper-bound the probability that $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i} \wedge \neg\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1} \wedge \neg\mathsf{mcoll}$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \mathsf{prefix}_{m^\alpha}^{=}$. By $p_{2,i}$, we denote the probability. We assume that the γ-th online query ($\gamma \in \{1, \ldots, \alpha-1\}$) is the prefix online query of the α-th online query, and j^* is the distinct point. If there are two or more prefix online queries of the α-th online query then we consider the prefix online query such that the distinct point is maximum.

- Firstly, we consider the case of $i < j^*$. In this case, we don't consider the condition $\neg\mathsf{mcoll}$, and assume that $\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1}$ does not hold in addition to the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \mathsf{prefix}_{m^\alpha}^{=}$. By $\mathsf{prefix}_{m^\alpha}^{=}$, $t_i^\alpha = t_i^\gamma$ holds, and by $\neg\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1}$, $\mathsf{hit}_{\mathsf{tt}}^{\gamma}$ does not hold. Hence, $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i}$ does not hold under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \mathsf{prefix}_{m^\alpha}^{=} \wedge \mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1}$, and thus we have $p_{2,i} = 0$.
- Secondly, we consider the case of $i = j^*$. In this analysis, we don't consider the condition $\neg\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1}$, and assume that mcoll does not hold in addition to the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \mathsf{prefix}_{m^\alpha}^{=}$. Note that since j^* is the maximum distinct point, $t_{j^*}^\alpha$ is a new input to $\mathcal{G}_{j^*}$. By $\neg\mathsf{mcoll}_T$, the number of inputs to random functions whose first r bits are equal to $t_{j^*}^\alpha[1,r]$ is at most $(q+\rho)$. Note that $t_{j^*}^\alpha[r+1,b] = s_{j^*-1}^\alpha[r+1,b]$, and $s_{j^*-1}^\alpha[r+1,b]$ is randomly drawn from at least $2^c - q$ values. Hence, the probability that $\mathsf{hit}_{\mathsf{tt}}^{\alpha,i}$ holds under the condition $\neg\mathsf{coll}_{\mathsf{tt}} \wedge \mathsf{prefix}_{m^\alpha}^{=} \wedge \neg\mathsf{mcoll}$ is at most $\frac{q+\rho}{2^c-q}$, and thus we have $p_{2,i} \leq \frac{q+\rho}{2^c-q}$.
- Finally, we consider the case of $i > j^*$. In this analysis, we don't consider the conditions $\neg\mathsf{hit}_{\mathsf{tt}}^{\leq\alpha,i-1}$ and $\neg\mathsf{mcoll}_T$. Note that for an r-bit string M^α, t_i^α has the form $t_i^\alpha = M^\alpha \| 0^c \oplus s_{i-1}^\alpha$, where M^α is a message block or 0^r. By $\neg\mathsf{coll}_{\mathsf{tt}}$, s_{i-1}^α is randomly drawn from at least $2^b - q$ values after M^α is defined. We thus have $p_{2,i} \leq \frac{(\ell-2)\alpha}{2^b-q}$.

Hence, we have $\Pr[\textbf{Case 2}] \leq \frac{q+\rho}{2^c-q} + (\ell-2) \times \frac{(\ell-2)\alpha}{2^b-q}$.

Hence, we have

$$\begin{aligned}\Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll}) \wedge \neg\mathsf{hit}_K] &\le \sum_{\alpha=1}^{q} \max\left\{\frac{(\ell-1)^2\alpha}{2^b-q}, \frac{q+\rho}{2^c-q} + \frac{(\ell-2)^2\alpha}{2^b-q}\right\}\\ &\le \frac{2(q+\rho)q}{2^c} + \frac{\ell^2q^2}{2^b}\ \text{, assuming } q \le 2^{c-1}.\end{aligned}$$

Finally, we have $\Pr[\mathsf{hit}_{\mathsf{tt}} \wedge \neg(\mathsf{coll}_{\mathsf{tt}} \vee \mathsf{mcoll})] \le \frac{\ell q}{2^k} + \frac{2(q+\rho)q}{2^c} + \frac{\ell^2q^2}{2^b}$.

►We put the above bounds to the inequation (2). Then we have

$$\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}] \le \frac{\ell q + Q}{2^k} + \frac{2q^2 + qQ + 2\rho(q+Q)}{2^c} + \frac{2\ell^2q^2}{2^b} + 2^{r+1} \times \left(\frac{2e\ell q}{\rho 2^r}\right)^{\rho}.$$

Upper-Bound of $\boldsymbol{\varepsilon}$*.* Let $\tau \in \mathcal{T}_{\mathsf{good}}$. Let all_i be the set of all oracles in Game i for $i = 1, 2$. Let $\mathrm{comp}_i(\tau)$ be the set of oracles compatible with τ in Game i for $i = 1, 2$. Then $\Pr[\mathsf{T}_1 = \tau] = \frac{|\mathrm{comp}_1(\tau)|}{|\mathrm{all}_1|}$ and $\Pr[\mathsf{T}_2 = \tau] = \frac{|\mathrm{comp}_2(\tau)|}{|\mathrm{all}_2|}$.

Firstly, we evaluate $|\mathrm{all}_1|$. Since $K \in \{0,1\}^k$ and $\mathcal{P} \in \mathsf{Perm}(\{0,1\}^b)$, we have $|\mathrm{all}_1| = 2^k \cdot 2^b!$.

Secondly, we evaluate $|\mathrm{all}_2|$. Since $K \in \{0,1\}^k$, $\mathcal{P} \in \mathsf{Perm}(\{0,1\}^b)$, and $\mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_\ell \in \mathsf{Func}(\{0,1\}^b, \{0,1\}^b)$, we have $|\mathrm{all}_2| = 2^k \cdot (2^b!) \cdot \left((2^b)^{2^b}\right)^{\ell}$.

Thirdly, we evaluate $|\mathrm{comp}_1(\tau)|$. For $i \in \{1, \dots, \ell\}$, let γ_i be the number of pairs in τ_i. Let $\gamma_{\mathcal{P}}$ be the numbers of pairs in $\tau_{\mathcal{P}}$. Let $\gamma = \gamma_{\mathcal{P}} + \sum_{i=1}^{\ell} \gamma_i$. Since $\tau_1, \dots, \tau_\ell$ and $\tau_{\mathcal{P}}$ are defined so that they do not overlap each other, we have $|\mathrm{comp}_1(\tau)| = (2^b - \gamma)!$.

Fourthly, we evaluate $|\mathrm{comp}_2(\tau)|$. Here, $\gamma_1, \dots \gamma_\ell$, and $\gamma_{\mathcal{P}}$ are analogously defined. Then we have $|\mathrm{comp}_2(\tau)| = (2^b - \gamma_{\mathcal{P}})! \cdot \prod_{i=1}^{\ell} (2^b)^{2^b - \gamma_i} = (2^b - \gamma_{\mathcal{P}})! \cdot (2^b)^{\ell 2^b - \gamma + \gamma_{\mathcal{P}}}$.

Finally, we have

$$\begin{aligned}\frac{\Pr[\mathsf{T}_1 = \tau]}{\Pr[\mathsf{T}_2 = \tau]} &= \frac{|\mathrm{comp}_1(\tau)|}{|\mathrm{all}_1|} \times \frac{|\mathrm{all}_2|}{|\mathrm{comp}_2(\tau)|} = \frac{(2^b - \gamma)!}{2^k \cdot (2^b!)} \times \frac{2^k \cdot (2^b!) \cdot (2^b)^{\ell 2^b}}{(2^b - \gamma_{\mathcal{P}})! \cdot (2^b)^{\ell 2^b - \gamma + \gamma_{\mathcal{P}}}}\\ &= \frac{(2^b)^{\gamma} \cdot (2^b - \gamma)!}{(2^b)^{\gamma_{\mathcal{P}}} \cdot (2^b - \gamma_{\mathcal{P}})!} \ge 1\ ,\end{aligned}$$

and thus $\varepsilon = 0$.

Upper-Bound of $\mathbf{Pr}[\mathbf{D}^{\boldsymbol{G_1}} \Rightarrow \mathbf{1}] - \mathbf{Pr}[\mathbf{D}^{\boldsymbol{G_2}} \Rightarrow \mathbf{1}]$. Finally, by Lemma 1, the upper-bound of $\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}]$ and ε yield the following bound.

$$\begin{aligned}&\Pr[\mathbf{D}^{G_1} \Rightarrow 1] - \Pr[\mathbf{D}^{G_2} \Rightarrow 1]\\ &\le \frac{\ell q + Q}{2^k} + \frac{2q^2 + qQ + 2\rho(q+Q)}{2^c} + \frac{2\ell^2q^2}{2^b} + 2^{r+1} \times \left(\frac{2e\ell q}{\rho 2^r}\right)^{\rho}.\end{aligned} \tag{3}$$

4.2 Upper-Bound of $\mathbf{Pr}[\mathbf{D}^{G_2} \Rightarrow 1] - \mathbf{Pr}[\mathbf{D}^{G_3} \Rightarrow 1]$

Firstly, we prove the following lemma.

Lemma 2. *G_2 and G_3 are indistinguishable unless the following condition holds in Game 2.*[3]

$$\begin{aligned}\mathsf{coll} \Leftrightarrow & \exists \alpha, \beta \in \{1, \ldots, q\}, i \in \{\max\{n^\alpha, n^\beta\}, \ldots, \min\{n^\alpha, n^\beta\} + \ell_{\mathrm{out}} - 1\} \\ & \text{s.t. } \alpha \neq \beta \wedge t_i^\alpha = t_i^\beta .\end{aligned}$$

Proof. If coll does not hold then all blocks in outputs of L_2 are independently drawn by random functions. Hence the above lemma holds. □

By the above lemma, $\Pr[\mathbf{D}^{G_2} \Rightarrow 1 | \neg\mathsf{coll}] = \Pr[\mathbf{D}^{G_3} \Rightarrow 1]$ holds. Then we have

$$\Pr[\mathbf{D}^{G_2} \Rightarrow 1] - \Pr[\mathbf{D}^{G_3} \Rightarrow 1] \leq \Pr[\mathsf{coll}] \ .$$

Hereafter, we upper-bound $\Pr[\mathsf{coll}]$. In this evaluation, we use the condition $\mathsf{coll}_{\mathsf{tt}}$ given in Subsection 4.1. Then we have $\Pr[\mathsf{coll}] \leq \Pr[\mathsf{coll}_{\mathsf{tt}}] + \Pr[\mathsf{coll} | \neg\mathsf{coll}_{\mathsf{tt}}]$ where the upper-bound of $\Pr[\mathsf{coll}_{\mathsf{tt}}]$ is given in Subsection 4.1: $\Pr[\mathsf{coll}_{\mathsf{tt}}] \leq \frac{q^2}{2^c} + \frac{0.5\ell q^2}{2^b}$.

We thus upper-bound $\Pr[\mathsf{coll} | \neg\mathsf{coll}_{\mathsf{tt}}]$. First fix $\alpha, \beta \in \{1, \ldots, q\}$ with $\alpha \neq \beta$, and upper-bound the probability that by the α-th and β-th online queries, coll holds. We consider the following cases.

Case 1 $\Leftrightarrow n^\alpha = n^\beta$: Since $m^\alpha \neq m^\beta$, there exists $j^* \in \{1, \ldots, n^\alpha\}$ such that $t_{j^*}^\alpha \neq t_{j^*}^\beta$. By $\neg\mathsf{coll}_{\mathsf{tt}}$, for all $j \in \{j^*+1, \ldots, n^\alpha + \ell - 1\}$, $t_j^\alpha \neq t_j^\beta$ holds. Hence, in this case, coll does not hold.

Case 2 $\Leftrightarrow n^\alpha \neq n^\beta$: Without loss of generality, assume that $n^\alpha > n^\beta$. By $m_{n^\alpha}^\alpha \neq 0^r$ and $m^\alpha \neq m^\beta$, there exists $j^* \in \{1, \ldots, n^\beta\}$ such that $t_{j^*}^\alpha \neq t_{j^*}^\beta$ holds. By $\neg\mathsf{coll}_{\mathsf{tt}}$, for all $j \in \{j^* + 1, \ldots, n^\alpha + \ell - 1\}$, $t_j^\alpha \neq t_j^\beta$ holds. Hence, in this case, coll does not hold.

By the above evaluations, we have $\Pr[\mathsf{coll} | \neg\mathsf{coll}_{\mathsf{tt}}] = 0$.

Finally, we have

$$\Pr[\mathbf{D}^{G_2} \Rightarrow 1] - \Pr[\mathbf{D}^{G_3} \Rightarrow 1] \leq \Pr[\mathsf{coll}] \leq \frac{q^2}{2^c} + \frac{0.5\ell q^2}{2^b} \ . \tag{4}$$

4.3 Upper-Bound of the Advantage

We put the upper-bounds (3) and (4) into the inequation (1). Then we have

$$\mathbf{Adv}_{\mathtt{IKSponge}}^{\mathsf{prf}}(\mathbf{D}) \leq \frac{\ell q + Q}{2^k} + \frac{3q^2 + qQ + 2\rho(q+Q)}{2^c} + \frac{3\ell^2 q^2}{2^b} + 2^{r+1} \times \left(\frac{2e\ell q}{\rho 2^r}\right)^\rho .$$

[3] Note that in this condition we consider a collision at the same position for two online queries, where in the position the outputs of the queries are produced. Hence, the first point of i is $\max\{n^\alpha, n^\beta\}$ and the last point is $\min\{n^\alpha, n^\beta\} + \ell_{\mathrm{out}} - 1$.

5 Outer Keyed Sponge and the PRF-Security

By $\texttt{OKSponge}$ we denote the outer keyed sponge construction, and by $\texttt{OKSponge}_K^P$, denote $\texttt{OKSponge}$ with P having K. For a message $m \in \{0,1\}^*$, the response is defined as $\texttt{OKSponge}_K^P(m) := \texttt{Sponge}^P(K^* \| m)$, where K^* is defined by appending some bit string to the suffix of K such that the bit length is a multiple of r, e.g., a zero string is appended. So the difference between $\texttt{OKSponge}$ and $\texttt{IKSponge}$ is the procedure to define the value s_0. In $\texttt{OKSponge}_K^P$, s_0 is defined as follows, where $\kappa := |K^*|/r$.

1. Partition K^* into r-bit blocks $K_1, \ldots, K_\kappa$;
   Partition $m \| \mathsf{pad}(|K^* \| m|)$ into r-bit blocks $m_1, \ldots, m_n$
2. $w_0 \leftarrow 0^b$; For $i = 1, \ldots, \kappa$ do $u_i \leftarrow K_i \| 0^c \oplus w_{i-1}$; $w_i \leftarrow P(u_i)$
3. $s_0 \leftarrow w_\kappa$

Basically, we can prove the PRF-security of $\texttt{OKSponge}$ by the similar proof but need to consider the structural difference: $s_0 = 0^{b-k} \| K$ in $\texttt{IKSponge}$ and $s_0 = w_\kappa$ in $\texttt{OKSponge}$. If $\mathbf{D}$ does not know w_κ, that is, $\mathbf{D}$ does not make an offline query $\mathcal{P}(u_\kappa)$ and $\mathcal{P}^{-1}(w_\kappa)$ then w_κ becomes a secret random value of b bits. Therefore, the upper-bound of the PRF-security of $\texttt{OKSponge}$ can be obtained from that of $\texttt{IKSponge}$, where the probability for K, $\frac{\ell q + Q}{2^k}$, is replaced with the probability for the "bad" event where $\mathbf{D}$ knows w_κ. The probability for the bad event was considered in [13, 1], and we use their bound. The concrete upper-bound is given as follows, where the probability for the bad event is $\lambda(Q) + \frac{2\kappa Q}{2^b}$.

Theorem 2. *Let $\mathbf{D}$ be a distinguisher which makes q online queries of r-bit block length at most ℓ_{in} and Q offline queries. Then for any ρ, we have $\mathbf{Adv}^{\mathsf{prf}}_{\texttt{OKSponge}}(\mathbf{D}) \le \lambda(Q) + \frac{2\kappa Q}{2^b} + \frac{2qQ + 3.5\ell^2 q^2}{2^b} + \frac{3q^2 + 2qQ + 2\rho(q+Q)}{2^c} + 2^{r+1} \times \left(\frac{2e\ell q}{\rho 2^r}\right)^\rho$, where $\ell = \ell_{\mathrm{in}} + \ell_{\mathrm{out}} - 1$, $e = 2.71828\cdots$ is Napier's constant, and $\lambda(Q) = \frac{Q}{2^k}$ if $k \le r$, and $\lambda(Q) = \min\left\{\frac{Q^2}{2^{c+1}} + \frac{Q}{2^k}, \frac{1}{2^b} + \frac{Q}{2^{\left(\frac{1}{2} - \frac{\log_2(3b)}{2r} - \frac{1}{r}\right)k}}\right\}$ otherwise.*

Corollary 2. *We assume $c \le b/2$. Then, we put $\rho = r$, and without loss of generality, assume $r \ge 2$ (otherwise $r = c = 1$ and b=2). Since $r \ge b/2$, we have $\mathbf{Adv}^{\mathsf{prf}}_{\texttt{OKSponge}}(\mathbf{D}) \le \frac{3q^2 + 2qQ + 2r(q+Q)}{2^c} + \frac{(3.5 + 32e^2 r^{-2})\ell^2 q^2 + 2qQ + 2\kappa Q}{2^b} + \lambda(Q)$.*

We assume $c > b/2$ and put $\rho = \max\left\{r, \left(\frac{2e \times \ell q}{2^{r-c}(q+Q)}\right)^{1/2}\right\}$. Then we have $\mathbf{Adv}^{\mathsf{prf}}_{\texttt{OKSponge}}(\mathbf{D}) \le \left(\frac{18e\ell q(q+Q)}{2^b}\right)^{1/2} + \frac{3q^2 + 2qQ + 2r(q+Q)}{2^c} + \frac{3.5\ell^2 q^2 + 2qQ + 2\kappa Q}{2^b} + \lambda(Q)$.

References

1. Elena Andreeva, Joan Daemen, Bart Mennink, and Gilles Van Assche. Security of keyed sponge constructions using a modular proof approach. In *FSE 2015*, LNCS 9054, Springer, pages 364–384.

2. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A lightweight hash. In *CHES 2010*, LNCS 6225, Springer, pages 1–15.
3. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. NORX: parallel and scalable AEAD. In *ESORICS 2014 II*, LNCS 8713, Springer, pages 19–36.
4. Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *CRYPTO '96*, LNCS 1109, Springer, pages 1–15.
5. Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 409–426, 2006.
6. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In *SAC 2011*, LNCS 7118, Springer, pages 320–337.
7. Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In *EUROCRYPT 2008*, LNCS 4965, Springer, pages 181–197.
8. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the security of the keyed sponge construction. SKEW 2011, 2011.
9. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Permutation-based encryption, authentication and authenticated encryption. DIAC 2012, 2012.
10. Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. spongent: A lightweight hash function. In *CHES 2011*, LNCS 6917, Springer, pages 312–325.
11. Donghoon Chang, Morris Dworkin, Seokhie Hong, John Kelsey, and Mridul Nandi. A keyed sponge construction with pseudorandomness in the standard model. Third SHA-3 Candidate Conference, 2012.
12. Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In *EUROCRYPT 2014*, LNCS 8441, Springer, pages 327–350.
13. Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro. The exact PRF security of truncation: Tight bounds for keyed sponges and truncated CBC. In *CRYPTO 2015, Part I*, LNCS 9215, Springer, pages 368–387.
14. Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In *CRYPTO 2011*, LNCS 6841, Springer, pages 222–239.
15. Philipp Jovanovic, Atul Luykx, and Bart Mennink. Beyond $2^{c/2}$ security in sponge-based authenticated encryption modes. In *ASIACRYPT 2014*, LNCS 8873, Springer, pages 85–104. Springer.
16. Bart Mennink, Reza Reyhanitabar, and Damian Vizár. Security of full-state keyed sponge and duplex: Applications to authenticated encryption. In *ASIACRYPT 2015*, LNCS 6225, pages 465–489. Springer.
17. NIST. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. In *FIPS PUB 202*, 2015.
18. Jacques Patarin. The "coefficients H" technique. In *SAC 2008*, LNCS 5381, Springer, pages 328–345.
19. Yu Sasaki and Kan Yasuda. How to incorporate associated data in sponge-based authenticated encryption. In *CT-RSA 2015*, LNCS 9048, Springer, pages 353–370.