Noname manuscript No.
(will be inserted by the editor)

On Tweakable Correlation Robust Hashing against Key Leakages

Chun Guo · Xiao Wang · Kang Yang · Yu Yu

Received: date / Accepted: date

Abstract We continue the study of blockcipher-based (tweakable) correlation robust hash functions, which are central building blocks of circuit garbling and oblivious-transfer extension schemes. Motivated by Roy (CRYPTO 2022), we first enhance the multi-user tweakable correlation robust notion of Guo et al. (CRYPTO 2020) with a *key leaking oracle* that tells the adversary whether a certain user key satisfies the adversarially-chosen predicate. We then investigate the state-of-the-art hash construction of Guo et al. with respect to our new security definition, providing security proof as well as matching attacks. As an application, we exhibit an OT extension protocol with non-trivial multi-user security.

Keywords Correlation robust hashing · key leakage · oblivious-transfer extension

Mathematics Subject Classification (2000) 94A60 · 68P25

Chun Guo
School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China
Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
Shandong Research Institute of Industrial Technology, Jinan, Shandong, 250102, China,
E-mail: chun.guo@sdu.edu.cn

Xiao Wang
Northwestern University, Evanston, USA
E-mail: wangxiao@northwestern.edu

Kang Yang
State Key Laboratory of Cryptology, Beijing, China
E-mail: yangk@sklc.org

Yu Yu
Shanghai Jiao Tong University, Shanghai, China
Shanghai Qi Zhi Institute, Shanghai, China
E-mail: yuyu@yuyu.hk

1 Introduction

(Tweakable) Correlation robust hashing. Garbling [31, 2] and oblivious-transfer (OT) extension [16] are two important building blocks of secure computation protocols. A huge proportion of the proposed schemes were built upon the so-called *correlation robust hash functions*. This notion was first proposed by Ishai et al. [16] for the purpose of OT extension. Roughly, a hash function H is correlation robust, if the function $f_R(x) := H(x \oplus R)$ keyed by R is pseudorandom. This notion was soon adopted by garbling with "free-XOR" technique [19]. However, Choi et al. [8] pointed out that a form of "circularity" is needed in order to support security proofs for the "free-XOR" garbling. They proposed *circular correlation robustness*, which requires $f_R(x, b) := H(x \oplus R) \oplus b \cdot R$ to be pseudorandom (provided that the input x is never repeated).

Bellare et al. [1] proposed to use fixed-key AES in circuit garbling, which results in substantially reduced CPU time costs. This has motivated many subsequent works to use fixed-key AES in secure computations. Concretely, many of them built their protocols over some variants of correlation robust hashing (e.g., the half-gate garbling scheme [32] used a variant termed *circular correlation robustness for naturally derived keys*), and then instantiated the hashing using fixed-key AES. To have a solid foundation, Guo et al. [12] provided a systematic study of the correlation robustness notions. They provided detailed security proofs for the correlation robustness of the folklore construction $\mathsf{MMO}^\pi(x) = \pi(x) \oplus x$ and circular correlation robustness of $\widehat{\mathsf{MMO}}^\pi_\sigma(x) = \pi(\sigma(x)) \oplus \sigma(x)$ using a linear orthomorphism σ.[1] They proposed a further enhanced notion named *tweakable circular correlation robustness* (TCCR), which is necessary for the malicious security of some protocols. Roughly, $H : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ is TCCR, if $f_R(w, b, i) := H(w \oplus R, i) \oplus b \cdot R$ is pseudorandom. Guo et al. [12] also gave a provably secure construction $\mathsf{TMMO}^\pi(x, i) = \pi(\pi(x) \oplus i) \oplus \pi(x)$ using two fixed-key AES calls. Subsequently, Chen and Tessaro [7] proposed two new TCCR hash designs from permutations, including a one-call construction using a field multiplication and a two-call construction with better security against a limited class of distinguishers.

To address security issues due to en mass deployment, Guo et al. [11] initiated the study of *multi-user security* of TCCR (miTCCR) hash functions. They also leveraged the "birthday-bound" issue in the MMO^π and TMMO^π constructions to attack certain instantiations of half-gate garbling. To remedy, Guo et al. reverted to the "full-fledged" blockcipher $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and proposed $\widehat{\mathsf{MMO}}^E(x, i) := E(i, \sigma(x)) \oplus \sigma(x)$, where σ is a linear orthomorphism. They proved good miTCCR security bounds: if the distinguisher makes at most μ queries per tweak (across multiple users), then secu-

[1] σ is *linear* if $\sigma(x \oplus y) = \sigma(x) \oplus \sigma(y)$ for all $x, y \in \{0,1\}^k$; σ is an *orthomorphism* [4] if it is a permutation, and the function σ' given by $\sigma'(x) := \sigma(x) \oplus x$ is also a permutation. It has been known [4, 11] that σ can be efficiently instantiated as $\sigma(x_L \| x_R) = x_R \oplus x_L \| x_L$ where x_L and x_R are the left and right halves of the input.

rity is ensured up to roughly $2^n/\mu$ queries to E and $2^n/\mu$ queries to f_R. In practical applications μ can be limited to $o(n)$ by using random initialization vectors [11], and the security is thus nearly optimal. Due to this, $\widehat{\mathsf{MMO}}^E$ has been adopted by some [6], even if its key schedule invocations slightly decrease performance.

Selective-failure leakage on keys. In the active setting where an adversary can arbitrarily deviate from the protocol, almost all existing OT-extension protocols (e.g., [18,21,25,3,30,28,24,9]), to generate correlated OT correlations (modeled as an ideal functionality $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}$), allow the adversary to perform selective-failure attacks on a key R. Specifically, the adversary can choose a set L, and then the protocol aborts if $R \notin L$, or nothing happens otherwise. In other words, $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}$ allows the adversary to choose a predicate P and learn $P(R)$, where the functionality aborts if $P(R) = 0$.

When applying $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}$ to design standard OT protocols via a generic transformation, a tweakable correlation robust (TCR) hash function will be used to protect the privacy of OT messages. If the key R suffers from selective-failure attacks, then the TCR hash function suffers from the selective-failure leakage on R. Besides, when applying $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}$ to construct constant-round secure multi-party computation (MPC) protocols (e.g., [26,27,14,17,33,29,10, 13]), the TCCR hash function will be used in the construction of distributed garbled circuits. In this case, the TCCR hash function also suffers from the selective-failure leakage on R.

Recently, Roy [24] incorporated the key-leakage oracle into the security definition of TCR, where the oracle takes an affine set L as input and aborts if $R \notin L$. Roy proved that two instantiations satisfy the new security notion in the single-user setting, where one is proved in the random oracle model; the other is similar to the aforementioned $\widehat{\mathsf{MMO}}^E$ construction but works in the ideal cipher model. The proven bounds are comparable with Guo et al. [11, Theorems 6 and 2], and are not tight. It is unknown whether the TCCR hash function (having the stronger security than TCR) has a tight security proof in the multi-user setting, when the adversary is allowed to have access to the general key-leakage oracle that returns $P(R)$.

1.1 Our contribution

We continue with the above line of work and extend [11,7,24] w.r.t. security definitions, feasibility results and applications.

Multi-user TCCR with key leakages. We augment the notion miTCCR of Guo et al. [11] with a key leaking oracle, and formalize the obtained security definition as *multi-user TCCR with key leakages* (muTCCRL). Concretely, our key leaking oracle takes a user index id and a predicate P as input and answers if the id-th user's key R_{id} has $P(R_{\mathsf{id}}) = 1$. Compared with Roy [24], our notion

muTCCRL allows for multiple users, multiple key leaking queries[2] and a much wider class of queried predicates.

Security of $\widehat{\mathsf{MMO}}^E$. We then investigate the aforementioned hash construction $\widehat{\mathsf{MMO}}^E$ of Guo et al. with respect to our new security definition.

On the positive side, we prove security for $\widehat{\mathsf{MMO}}^E$. Assume that: (i) the u user keys $R_1, ..., R_{\mathsf{id}}$ are independently and uniformly sampled from an (oracle-independent) set $\mathcal{R}$, (ii) the adversary asks key leaking queries to at most M distinct users, and for each of them, the adversary asks at most $q_{L,max}$ leaking queries, and (iii) the adversary asks at most μ construction queries per tweak (across multiple users), then security of $\widehat{\mathsf{MMO}}^E$ is ensured up to roughly $|\mathcal{R}|/(\mu M q_{L,max})$ ideal cipher queries and $|\mathcal{R}|/(\mu M q_{L,max})$ construction queries. Our proof relies on a somewhat novel application of the H-coefficient method, which may be of some independent interest. On the practical side, NIST [20] has recently launched its standardization process of multi-party threshold cryptographic schemes. Our positive results thus provide promising building blocks to this end.

As mentioned before, practical applications could limit μ to $O(n)$ by using random initialization vectors (see our application below), and the $\log_2 \mu$ bits security loss is rather small. The parameter $q_{L,max}$ could be limited to $O(n)$ as well. On the other hand, M may be large in the multi-user setting (e.g., in our application below, it equals the number of corrupted receivers across the u OT extension instances), and the corresponding security loss is of $\log_2 M$ bits. Unfortunately, the bound is tight, and an anonymous reviewer has given a matching attack (we include the attack in Appendix B: we do not claim it as our contribution). By this, to have sufficient multi-user security in relevant settings, one may need moderately large security parameters.

Application to OT extension. Our new hashing result implies OT extension with non-trivial multi-user security. In detail, we present an OT extension protocol modified from the random-OT-to-standard-OT transformation of Guo et al. [12, Fig. 3]. Our protocol uses a random IV to control the number of collisions among tweak inputs of distinct hash calls, which borrows the idea of Guo et al. [11] on garbling. Compared with Chen and Tessaro [7, Fig. 3], our protocol does not invoke AXU hash functions. On the downside, we rely on our muTCCRL hash function $\widehat{\mathsf{MMO}}^E$ using $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, which is less efficient than Chen and Tessaro's two-call hash construction. Importantly, our protocol avoids the trivial $\log_2 u$ bits multi-user security degradation: assume that the adversary corrupts M receivers, then u (independently initiated) instances of our new OT extension protocol are indistinguishable

[2] Roy's security definition allows multiple key leaking queries, but from the results [24, Propositions 2.6, 2.7] and security proofs [23, Appendix A] it seems only a single key leaking query is allowed.

from u independent instances of the ideal standard-OT functionality, and security is of roughly $k - \log_2 n - \log_2 M$ bits (k is the size of the secret shift). We refer to Sect. 5.2 for details. To our knowledge, this is the first non-trivial multi-user treatment of OT extension protocols.

Organizations. We provide necessary preliminaries in Sect. 2. Then, in Sect. 3, we provide our multi-user TCCR definition; in Sect. 4, we discuss security of $\widehat{\mathsf{MMO}}^E$—both proven bounds and relevant attacks. We then present our application to multi-user security of OT extension in Sect. 5. Finally, we conclude in Sect. 6.

2 Preliminary

For any integer $j \in \{0, ..., m-1\}$, denote by $[j]_m$ the m-bit encoding of j. For any set or list $\mathcal{S}$, we denote by $|\mathcal{S}|$ its size or "length", i.e., the number of elements in $\mathcal{S}$. The union of two sets $\mathcal{S}_1$ and $\mathcal{S}_2$ is denoted $\mathcal{S}_1 \cup \mathcal{S}_2$. When $\mathcal{S}_1$ and $\mathcal{S}_2$ are disjoint, we denote their disjoint union as $\mathcal{S}_1 \sqcup \mathcal{S}_2$.

We will rely on a slightly generalized version of [11, Lemma 1], which is stated as follows.

Lemma 1 *Fix integers n, q and $u \le q$, a bijective function $\gamma : [2^n - 1] \mapsto \{0,1\}^n$ and a sequence of positive integers $(q_1, \ldots, q_u)$ with $\sum_{i=1}^{u} q_i = q$. Consider the following experiment involving a set of 2^n bins and q balls: for each $i \in [u]$, q_i balls are placed in the bins of indices $\gamma(1)\oplus IV_i, \gamma(2)\oplus IV_i, ..., \gamma(q_i)\oplus IV_i$, where $IV_i \xleftarrow{\$} \{0,1\}^n$ is uniformly picked. If μ^* is the random variable denoting the maximum number of balls in any bin, then*

$$\Pr\left[\mu^* > \mu\right] \le \frac{q^{\mu+1}}{(\mu+1)! \cdot 2^{\mu n}} .$$

Its proof, which essentially follows [11, Lemma 1], is given in Appendix A.

3 Multi-user TCCR with Key Leakages

Our definition of muTCCRL is an extension of Roy [23] to the multi-user setting. It may also be viewed as the miTCCR notion of Guo et al. [11] enhanced with a *key leaking oracle*. In detail, given a function $H : \mathcal{W} \times \mathcal{T} \to \mathcal{W}$ (that depends on an ideal cipher E) and a vector of secrets $\mathbf{R} = (R_1, ..., R_u)$, define

$$\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}, w, i, b) := H(w \oplus R_{\mathsf{id}}, i) \oplus b \cdot R_{\mathsf{id}}, \tag{1}$$

and define $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$, $P \in \mathcal{P}$, as the oracle that *aborts the session of the id-th user if and only if $P(R_{id}) \neq 1$*. This means if the adversary keeps querying $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$ with $P(R_{\mathsf{id}}) = 1$ then nothing happens (by this, it gains information about R_{id} by knowing $P(R_{\mathsf{id}}) = 1$); once it queries $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$ with $P(R_{\mathsf{id}}) = 0$

then $\mathcal{L}_{\mathbf{R}}$ never replies queries of the form $(\mathsf{id}, \star)$ and $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}$ never replies queries of the form $(\mathsf{id}, \star, \star, \star)$. (On the other hand, it is always required that $P \in \mathcal{P}$).

Let $\mathsf{Func}_{\{1,...,u\}\times\mathcal{W}\times\mathcal{T}\times\{0,1\},\mathcal{W}}$ denote the set of functions from $\{1, ..., u\} \times \mathcal{W} \times \mathcal{T} \times \{0, 1\}$ to $\mathcal{W}$, and let $\mathcal{E}(\mathcal{T}, \mathcal{W})$ denote the set of blockciphers with keyspace $\mathcal{T}$ and message space $\mathcal{W}$.

Definition 1 (muTCCRL **advantage)** Given a function $H^E : \mathcal{W} \times \mathcal{T} \to \mathcal{W}$, a subset $\mathcal{R} \subseteq \mathcal{W}$, and a distinguisher $\mathcal{D}$, define

$$\mathbf{Adv}^{\mathrm{muTCCRL}}_{H,\mathcal{R},\mathcal{P},u,\mu}(\mathcal{D}) := \Bigg| \Pr_{E\xleftarrow{\$}\mathcal{E}(\mathcal{T},\mathcal{W}),\mathbf{R}\xleftarrow{\$}(\mathcal{R})^u}\left[\mathcal{D}^{E,\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}},\mathcal{L}_{\mathbf{R}}}=1\right] - \Pr_{f\leftarrow\mathsf{Func}_{\{1,...,u\}\times\mathcal{W}\times\mathcal{T}\times\{0,1\},\mathcal{W}},E\xleftarrow{\$}\mathcal{E}(\mathcal{T},\mathcal{W}),\mathbf{R}\xleftarrow{\$}(\mathcal{R})^u}\left[\mathcal{D}^{E,f,\mathcal{L}_{\mathbf{R}}}=1\right]\Bigg|,$$

where both probabilities are also over choice of E and we require that

(i) $\mathcal{D}$ never queries both $(\mathsf{id}, w, i, 0)$ and $(\mathsf{id}, w, i, 1)$ to its second oracle (for any id, w, i).
(ii) For all $i \in \mathcal{T}$, the number of queries (across all the u users) of the form $(\star, \star, i, \star)$ to $\mathcal{D}$'s second oracle is at most μ.
(iii) Every query (id, P) of $\mathcal{D}$ to its third oracle $\mathcal{L}_{\mathbf{R}}$ has $P \in \mathcal{P}$.

We call a muTCCRL adversary/distinguisher $\mathcal{D}$ $(q_C, q_E, M, q_{L,max})$-*bounded*, if:

(i) $\mathcal{D}$ makes at most q_E queries to E and at most q_C queries to $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}/f$;
(ii) $\mathcal{D}$ makes key leaking queries with at most M distinct user indices id, and for any of them, $\mathcal{D}$ makes at most $q_{L,max}$ queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$.

As will be seen, the four parameters give a complicated though fine-grained characterization of adversarial power in the muTCCRL setting.

We recover the definition of Guo et al. [11] if we remove the key leaking oracle $\mathcal{L}_{\mathbf{R}}$. Note that we follow Guo et al. [11] and explicitly allow the concrete security bound to depend on the maximum number of times μ an attacker repeats any particular tweak.

We remark that Chen and Tessaro [7] also discussed the issue when the key set $\mathcal{R}$ depends on the ideal cipher E. In our current formalism, the cipher E is uniformly sampled *after* $\mathcal{R}$ is fixed and given. In this manner, the primitive-dependency is avoided (we thank Chen and Tessaro for pointing the two issues).

4 Multi-user TCCRL Security of $\widehat{\mathsf{MMO}}^E$

This section proves muTCCRL security for the hash

$$\widehat{\mathsf{MMO}}^E(x, i) := E(i, \sigma(x)) \oplus \sigma(x),$$

where $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is a blockcipher and σ is a linear orthomorphism. We only consider the case of $\mathcal{D}$ using *oracle-free* predicates for its key leaking oracle queries. Namely, for every query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$, the predicate evaluation $P(R_{\mathsf{id}})$ does not query the ideal cipher E. Formally, let $\mathcal{P}_{\mathsf{free}}$ be the set of all such oracle-free predicates. For clarity, we will also sketch the influences of oracle-freeness in footnote 3.

Theorem 1 *If σ is a linear orthomorphism and E is modeled as an ideal cipher, then the* muTCCRL *advantage of any $(q_C, q_E, M, q_{L,max})$-bounded adversary $\mathcal{D}$ against $\widehat{\mathsf{MMO}}^E$ has upper bound*

$$\begin{aligned}&\mathbf{Adv}^{\mathrm{muTCCRL}}_{H,\mathcal{R},\mathcal{P},u,\mu}(\mathcal{D})\\ &\leq \frac{2\mu q_E(M+1)(q_{L,max}+1)}{|\mathcal{R}|} + \frac{(\mu-1)\cdot q_C(M+1)(q_{L,max}+1)}{|\mathcal{R}|}. \qquad (2)\end{aligned}$$

Let q_L be the total number of adversarial key leaking queries. In the single-user setting, one has $M = 1$ and $q_{L,max} = q_L$, and the bound becomes

$$\mathbf{Adv}^{\mathrm{muTCCRL}}_{H,\mathcal{R},\mathcal{P},1,\mu}(\mathcal{D}) \leq \frac{4\mu q_E(q_L+1)}{|\mathcal{R}|} + \frac{2(\mu-1)\cdot q_C(q_L+1)}{|\mathcal{R}|}. \qquad (3)$$

This bound can also be obtained by adapting our proof to the single-user setting, but a single analysis in the multi-user setting turns out to be sufficient.

Below we first elaborate on the concrete bounds in Sect. 4.1. We then give the main proof flow of Theorem 1 in Sect. 4.2, and the proof of a core lemma is deferred to Sect. 4.3. We conclude this section with several matching attacks in Sect. 4.4.

4.1 Bounds in concrete scenarios

As demonstrated by Guo et al. [11, Theorem 3] (also see Theorem 2 of this paper), μ can be limited to $O(n)$ or even $O(1)$ by using somewhat random tweaks in the protocol. By this,

- Eq. (3) indicates single-user security up to $q_E q_L \ll |\mathcal{R}|$ and $q_C q_L \ll |\mathcal{R}|$, which is much inferior to Guo et al. [11, Theorem 2].
- Eq. (2) indicates multi-user security up to $Mq_E q_{L,max} \ll |\mathcal{R}|$ and $Mq_C q_{L,max} \ll |\mathcal{R}|$. In the worst case $M = u$, and it suffers from the well-known multi-user security degradation.

Unfortunately, these are tight: for single-user we refer to the attack in Sect. 4.4.1, while for multi-user we refer to the attack in Appendix B.

On the other hand, in concrete scenarios, $q_{L,max}$, the number of maximal key leaking queries per user, may be rather limited, which entails much better concrete security. For example, in an execution of the OT extension protocol, $q_{L,max}$ is equal to the number ι of iterations in OT extension. The number

of iterations depends on the concrete applications and memory, but we often have $\iota = O(1)$ in general (e.g, see Sect. 5). In this case, single-user security is ensured up to $|\mathcal{R}|/\iota \approx |\mathcal{R}|$ queries, while multi-user security is ensured up to $|\mathcal{R}|/(M\iota) \approx |\mathcal{R}|/M$ queries. We refer to Theorem 2 for more details.

We further remark that although our multi-user bound Eq. (2) suffers from the multi-user loss (the factor of M), it remains non-trivial. As mentioned before, our method, once adapted, can yield the (tight) single-user bound Eq. (3). With this, the multi-user bound derived via the trivial hybrid argument is

$$\frac{4u\mu q_E(q_L+1)}{|\mathcal{R}|} + \frac{2u(\mu-1)\cdot q_C(q_L+1)}{|\mathcal{R}|} \tag{4}$$

In many cases we have $q_{L,max} \ll q_L$, and this bound is much inferior to Eq. (2). For example, when $q_{L,max} = O(1)$ (as in Sect. 5) while $q_L = Mq_{L,max}$, Eq. (2) indicates multi-user security up to $|\mathcal{R}|/(\mu M q_{L,max}) \approx |\mathcal{R}|/M$ queries, while Eq. (4) indicates multi-user security up to $|\mathcal{R}|/(u\mu M q_{L,max}) \approx |\mathcal{R}|/(uM)$ queries. This improvement and the aforementioned tightness also demonstrate the usefulness of our complicated proof approach.

4.2 Proof of Theorem 1

4.2.1 A glimpse on our approach

We use the H-coefficient method. Our definition of bad transcripts and subsequent calculations are basically the same as the existing miTCCR proof [11]. Our novelty lies in calculating probability of obtaining bad transcripts (bad probability for short), which was significantly complicated by the key leaking queries (we remark that such a tight treatment of key leaking queries seems new in the literature).

In detail, bad transcripts are characterized by certain conditions. In previous proofs (e.g., [5,4,7,11,12]), the probabilities of such conditions are usually functions of adversarial resources. In our proof, however, they depend on more detailed characteristics of the adversarial transcripts, and we cannot have a tight universal upper bound.

To remedy, we first derive a transcript-dependent bound on the probability. We then calculate the expectation of this probability over attainable transcripts sampled according to the ideal world executions. This calculation relies on the prefix-freeness of attainable transcripts, which may be a new observation as well.

This expectation approach may remind the reader about Hoang and Tessaro [15]. However, in their paradigm(s) expectations are only computed for ratios between real and ideal world probabilities, and the probability bounds for bad transcripts or variables remain universal (i.e., it has to address the worst case). In comparison, we compute expectations for bad transcript probability. To our knowledge, our approach seems new in the literature.

We refer to the subsequent sections for details.

4.2.2 Preparations

We provide a brief review of the H-coefficient technique [22, 5], adapted from [12]. Fix a deterministic distinguisher $\mathcal{D}$ that is given access to an ideal cipher $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, a key leaking oracle $\mathcal{L}_{\mathbf{R}}$, as well as an additional construction oracle $\mathcal{O}$: in the real world, $\mathcal{O}$ is the oracle defined in Eq. (1); in the ideal world, $\mathcal{O}$ is the function uniformly chosen from $\mathsf{Func}_{\{1,\ldots,u\}\times\mathcal{W}\times\mathcal{T}\times\{0,1\},\mathcal{W}}$. We are interested in bounding the maximum difference between the probabilities that $\mathcal{D}$ outputs 1 in the real world vs. the ideal world, where the maximum is taken over all $(q_C, q_E, M, q_{L,max})$-bounded $\mathcal{D}$ (see Sect. 3).

For any predicate P, let $\mathcal{R}(P) \subseteq \mathcal{R}$ be the set of keys that fulfill P, i.e.,

$$\mathcal{R}(P) := \big\{R \in \mathcal{R} : P(R) = 1\big\}, \tag{5}$$

4.2.3 H-coefficient method

A raw transcript of D's interaction is an ordered list

$$\mathcal{Q} = \big((\mathsf{T}_1, \mathsf{Q}_1, \mathsf{A}_1), (\mathsf{T}_2, \mathsf{Q}_2, \mathsf{A}_2), ...\big), \tag{6}$$

where the i-th triple $(\mathsf{T}_i, \mathsf{Q}_i, \mathsf{A}_i)$ means:

- When $\mathsf{T}_i = E$, it has $\mathsf{Q}_i = (k, x)$ and $\mathsf{A}_i = y \in \{0,1\}^n$ which indicates that the i-th query is a forward query to the ideal cipher $E(k, x) \to y$;
- When $\mathsf{T}_i = E^{-1}$, it has $\mathsf{Q}_i = (k, y)$ and $\mathsf{A}_i = x \in \{0,1\}^n$ which indicates that the i-th query is a backward query to the ideal cipher $E^{-1}(k, y) \to x$;
- When $\mathsf{T}_i = \mathcal{O}$, it has $\mathsf{Q}_i = (\mathsf{id}, w, i, b)$ and $\mathsf{A}_i = z \in \{0,1\}^n$ which indicates that the i-th query is a construction query $\mathcal{O}(\mathsf{id}, w, i, b) \to z$;
- When $\mathsf{T}_i = \mathcal{L}$, it has $\mathsf{Q}_i = (\mathsf{id}, P)$ and $\mathsf{A}_i = r \in \{0,1\}$ which indicates that the i-th query is a key leaking query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P) \to r$.
  For every $\mathsf{id} \in \{1, ..., u\}$, let

  $$(\mathcal{L}, (\mathsf{id}, P_{\mathsf{id},1}), r_{\mathsf{id},1}), \ldots, (\mathcal{L}, (\mathsf{id}, P_{\mathsf{id},t_{\mathsf{id}}-1}), r_{\mathsf{id},t_{\mathsf{id}}-1}), (\mathcal{L}, (\mathsf{id}, P_{\mathsf{id},t_{\mathsf{id}}}), r_{\mathsf{id},t_{\mathsf{id}}})$$

  be the ordered list of all key leaking queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ (the id-th user) in $\mathcal{Q}$. It necessarily holds $r_{\mathsf{id},1} = ... = r_{\mathsf{id},t_{\mathsf{id}}-1} = 1$: otherwise, the id-th user's "session" should have aborted and $\mathcal{D}$ should not have been able to query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P_{t_{\mathsf{id}}})$.

A raw transcript $\mathcal{Q}$ is *attainable* for some fixed $\mathcal{D}$ if there exist some ideal world oracles such that the interaction of $\mathcal{D}$ with those oracles would lead to transcript $\mathcal{Q}$. Denote by $\mathcal{T}$ the set of such attainable raw transcripts.

Our definition of transcripts deviates from the common forms (e.g., [5, 4]): we consider *ordered* list, and the query types matter as well. As will become clear, our arguments rely on these ingredients. On the other hand, the fundamental ideas and lemmas of the H-coefficient method still hold for our formalism.

We follow previous works [5] and reveal the keys to $\mathcal{D}$ at the end of the interactions. For this, let

$$\mathcal{L}_{\mathbf{R}} \vdash \mathcal{Q}$$

denote the event that the key leaking oracle $\mathcal{L}_{\mathbf{R}}$ gives responses that are consistent with all leaking query records in $\mathcal{Q}$, i.e., $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P) = r$ for all $(\mathcal{L}, (\mathsf{id}, P), r) \in \mathcal{Q}$. Then, the key vector $\mathbf{R}$ is appended to the transcript to facilitate the analysis: in the real world, these are the actual keys used by the oracles $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}$ and $\mathcal{L}_{\mathbf{R}}$, whereas in the ideal world it's a "dummy" key vector uniformly sampled from the set

$$\mathcal{R}(\mathcal{Q}) := \big\{\mathbf{R}^* \in (\mathcal{R})^u : \mathcal{L}_{\mathbf{R}^*} \vdash \mathcal{Q}\big\}, \tag{7}$$

This means they may *not* be the same as the keys actually used by $\mathcal{L}_{\mathbf{R}}$ in the ideal world. Define $\mathcal{Q}_x := (\mathcal{Q}, \mathbf{R})$ as the final adversarial transcript. A transcript $\mathcal{Q}_x = (\mathcal{Q}, \mathbf{R})$ is *attainable* for some fixed $\mathcal{D}$, if $\mathcal{Q} \in \mathcal{T}$ *and* $\mathbf{R} \in \mathcal{R}(\mathcal{Q})$, i.e., $\mathbf{R}$ can be sampled as the "dummy" key vector. Denote by $\mathcal{T}_x$ the set of such attainable (final) transcripts.

Fix a deterministic distinguisher $\mathcal{D}$ that interacts with either the real world oracles $(E, \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}, \mathcal{L}_{\mathbf{R}})$ or the ideal world oracles $(E, f, \mathcal{L}_{\mathbf{R}})$. Let T_{re}, resp. T_{id}, be the random variable corresponding to D's transcript in the real, resp. ideal, world. The H-coefficient technique involves defining a partition of $\mathcal{T}$ into a "bad" set $\mathcal{T}_{\mathsf{bad}}$ and a "good" set $\mathcal{T}_{\mathsf{good}} = \mathcal{T} \setminus \mathcal{T}_{\mathsf{bad}}$, and then showing that

$$\Pr\big[T_{\mathrm{id}} \in \mathcal{T}_{\mathsf{bad}}\big] \leq \varepsilon_1$$

and

$$\forall \mathcal{Q}_x \in \mathcal{T}_{\mathsf{good}} : \ \frac{\Pr\big[T_{\mathrm{re}} = \mathcal{Q}_x\big]}{\Pr\big[T_{\mathrm{id}} = \mathcal{Q}_x\big]} \geq 1 - \varepsilon_2.$$

The distinguishing advantage of $\mathcal{D}$ is then at most $\varepsilon_1 + \varepsilon_2$.

Ideal world probability. One of the key insights of the H-coefficient technique is that the value of $\Pr\big[T_{\mathrm{re}} = \mathcal{Q}_x\big]/\Pr\big[T_{\mathrm{id}} = \mathcal{Q}_x\big]$ is equal to the ratio between the probability that the real-world oracles are consistent with $\mathcal{Q}_x$ and the probability that the ideal-world oracles are consistent with $\mathcal{Q}_x$. To this end, for each transcript $\mathcal{Q}_x = (\mathcal{Q}, \mathbf{R})$ and each $k \in \{0,1\}^n$, define $\mathcal{Q}[E, k]$ as

$$\mathcal{Q}[E, k] := \big\{(k, x, y) : (E, (k, x), y) \in \mathcal{Q} \text{ or } (E^{-1}, (k, y), x) \in \mathcal{Q}\big\}, \tag{8}$$

and define $\mathcal{Q}[E] := \cup_{k \in \{0,1\}^n} \mathcal{Q}[E, k]$ as their union. Let $E \vdash \mathcal{Q}$ denote the event that block cipher E is consistent with all ideal cipher queries and answers in $\mathcal{Q}$, i.e., that $E(k, x) = y$ as long as $(E, (k, x), y) \in \mathcal{Q}$ or $(E^{-1}, (k, y), x) \in \mathcal{Q}$. Then, the probability to have $E \vdash \mathcal{Q}$ for an ideal cipher (with n-bit blocks and n-bit keys) is

$$\left(\prod_{k \in \{0,1\}^n} (2^n)_{|\mathcal{Q}[E,k]|}\right)^{-1},$$

where for integers $1 \leq b \leq a$, we set $(a)_b = a \cdot (a-1) \cdots (a-b+1)$, with $(a)_0 = 1$ by convention.

Define $\mathcal{Q}[\mathcal{O}]$ as the set of construction queries in $\mathcal{Q}$, i.e.,

$$\mathcal{Q}[\mathcal{O}] := \big\{(\mathsf{id}, w, i, b, z) : (\mathcal{O}, (\mathsf{id}, w, i, b), z) \in \mathcal{Q}\big\}. \tag{9}$$

Similarly, for a function $f \in \mathsf{Func}_{\{1,\ldots,u\}\times\mathcal{W}\times\mathcal{T}\times\{0,1\},\mathcal{W}}$, let $f \vdash \mathcal{Q}$ denote the event that f is consistent with all construction queries and answers in $\mathcal{Q}$, i.e., that $f(\mathsf{id}, w, i, b) = z$ for all $(\mathcal{O}, (\mathsf{id}, w, i, b), z) \in \mathcal{Q}$. Then, the probability to have $f \vdash \mathcal{Q}$ for a random function $f \xleftarrow{\$} \mathsf{Func}_{\{1,\ldots,u\}\times\mathcal{W}\times\mathcal{T}\times\{0,1\},\mathcal{W}}$ is

$$\frac{1}{2^{|\mathcal{Q}[\mathcal{O}]|n}}.$$

For each $\mathsf{id} \in \{1, ..., u\}$, let $\big(\mathcal{L}, (\mathsf{id}, P_{\mathsf{id},1}), r_{\mathsf{id},1}\big), \ldots, \big(\mathcal{L}, (\mathsf{id}, P_{t_{\mathsf{id}}}), r_{\mathsf{id},t_{\mathsf{id}}}\big)$ be the key leaking query records of the id-th user in $\mathcal{Q}$, where $t_{\mathsf{id}} \leq q_{L,max}$. Define

$$\mathcal{R}(\mathcal{Q}, \mathsf{id}) := \big\{R \in \mathcal{R} : P_{\mathsf{id},1}(R) = r_{\mathsf{id},1} \wedge ... \wedge P_{\mathsf{id},t_{\mathsf{id}}}(R) = r_{\mathsf{id},t_{\mathsf{id}}}\big\} \tag{10}$$

as the key set compatible with $\big(\mathcal{L}, (\mathsf{id}, P_{\mathsf{id},1}), r_{\mathsf{id},1}\big), \ldots, \big(\mathcal{L}, (\mathsf{id}, P_{t_{\mathsf{id}}}), r_{\mathsf{id},t_{\mathsf{id}}}\big)$. This means $\mathcal{R}(\mathcal{Q}) = \mathcal{R}(\mathcal{Q}, 1) \times \mathcal{R}(\mathcal{Q}, 2) \times ... \times \mathcal{R}(\mathcal{Q}, u)$, and further

$$\begin{aligned}\Pr\big[\mathcal{L}_{\mathbf{R}} \vdash \mathcal{Q}\big] &= \Pr\big[(R_1, ..., R_u) \xleftarrow{\$} (\mathcal{R})^u : R_1 \in \mathcal{R}(\mathcal{Q}, 1) \wedge ... \wedge R_u \in \mathcal{R}(\mathcal{Q}, u)\big] \\ &= \prod_{\mathsf{id}=1}^{u} \frac{|\mathcal{R}(\mathcal{Q}, \mathsf{id})|}{|\mathcal{R}|}.\end{aligned}$$

For simplicity, write

$$(E, f, \mathbf{R}) \vdash \mathcal{Q}$$

for the event $E \vdash \mathcal{Q} \wedge f \vdash \mathcal{Q} \wedge \mathcal{L}_{\mathbf{R}} \vdash \mathcal{Q}$. The key insight is that $T_{\mathrm{id}} = \mathcal{Q}$, the event that the ideal world execution gives rise to the raw transcript $\mathcal{Q}$, is equivalent with the event $(E, f, \mathbf{R}) \vdash \mathcal{Q}$.

Finally, in the ideal world, the probability that the "dummy" key vector sampled at the end equals a given vector $\mathbf{R}$ is $\prod_{\mathsf{id}=1}^{u} \frac{1}{|\mathcal{R}(\mathcal{Q},\mathsf{id})|}$.[3] Therefore, for any attainable (final) transcript $\mathcal{Q}_x = (\mathcal{Q}, \mathbf{R})$, the probability that the ideal world is consistent with $\mathcal{Q}_x$ is computed by

$$\begin{aligned}&\frac{1}{\prod_{k\in\{0,1\}^n}(2^n)_{|\mathcal{Q}[E,k]|}} \times \frac{1}{2^{nq_C}} \times \left(\prod_{\mathsf{id}=1}^{u} \frac{|\mathcal{R}(\mathcal{Q}, \mathsf{id})|}{|\mathcal{R}|}\right) \times \left(\prod_{\mathsf{id}=1}^{u} \frac{1}{|\mathcal{R}(\mathcal{Q}, \mathsf{id})|}\right) \\ &= \frac{1}{\prod_{k\in\{0,1\}^n}(2^n)_{|\mathcal{Q}[E,k]|} \cdot 2^{nq_C} \cdot |\mathcal{R}|^u}.\end{aligned} \tag{11}$$

(We assume $|\mathcal{Q}[\mathcal{O}]| = q_C$, i.e., D always makes exactly q_C queries to its construction oracles.)

[3] If the predicates can be oracle-dependent, then it seems we need to append the ideal cipher query records of the predicates to $\mathcal{Q}$ as well: otherwise, it is non-trivial to define $\mathcal{R}(\mathcal{Q}, \mathsf{id})$. This may induce an "unreal" loss in the derived security bounds.

Real world probability. It remains to address the probability that the real world is consistent with $\mathcal{Q}_x \in \mathcal{T}_{\mathsf{good}}$. Since, in the real world, the behavior of the second oracle is completely determined by E and $\mathbf{R}$, we can also write $(E, \mathbf{R}) \vdash \mathcal{Q}[\mathcal{O}]$ to denote the event that cipher E and keys $\mathbf{R}$ are consistent with the construction queries/answers in $\mathcal{Q}$. For a (good) transcript $\mathcal{Q}$, the probability that the real world is consistent with $\mathcal{Q}$ is exactly

$$\begin{aligned}&\Pr\big[E \vdash \mathcal{Q}\big] \times \Pr\big[\mathcal{L}_{\mathbf{R}^*} \vdash \mathcal{Q}\big] \times \Pr\big[\mathbf{R}^* = \mathbf{R} \mid \mathcal{L}_{\mathbf{R}^*} \vdash \mathcal{Q}\big] \\ &\qquad \times \Pr\big[(E, \mathbf{R}^*) \vdash \mathcal{Q}[\mathcal{O}] \mid E \vdash \mathcal{Q} \wedge \mathbf{R}^* = \mathbf{R}\big] \\ =\ &\Pr\big[E \vdash \mathcal{Q}\big] \times \Pr\big[\mathbf{R}^* \xleftarrow{\$} (\mathcal{R})^u : \mathbf{R}^* = \mathbf{R}\big] \times \Pr\big[(E, \mathbf{R}^*) \vdash \mathcal{Q}[\mathcal{O}] \mid E \vdash \mathcal{Q} \wedge \mathbf{R}^* = \mathbf{R}\big].\end{aligned}$$

We have $\Pr\big[E \vdash \mathcal{Q}\big] = 1/\prod_{k\in\{0,1\}^n}(2^n)_{|\mathcal{Q}[E,k]|}$ exactly as before. The crux of the proof thus reduces to showing a bound on $\Pr\big[(E, \mathbf{R}^*) \vdash \mathcal{Q}[\mathcal{O}] \mid E \vdash \mathcal{Q} \wedge \mathbf{R}^* = \mathbf{R}\big]$. Note that we can equivalently express it as $\Pr\big[\forall\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big) \in \mathcal{Q} : \mathcal{O}^{\mathrm{mu^1TCCRL}}_{\mathbf{R}}(\mathsf{id}, w, i, b) = z \mid E \vdash \mathcal{Q}\big]$.

4.2.4 Bad transcripts

We say a transcript $(\mathcal{Q}, \mathbf{R})$ is *bad* if:

- (B-1) There is a query record $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big) \in \mathcal{Q}$ and a record of the form $(i, \sigma(R_{\mathsf{id}} \oplus w), \star)$ or of the form $(i, \star, \sigma(R_{\mathsf{id}} \oplus w) \oplus b \cdot R_{\mathsf{id}} \oplus z)$ in $\mathcal{Q}[E]$.
- (B-2) There are distinct $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)$ and $\big(\mathcal{O}, (\mathsf{id}', w', i, b'), z'\big) \in \mathcal{Q}$ using the same "tweak" i such that $\sigma(R_{\mathsf{id}} \oplus w) = \sigma(R_{\mathsf{id}'} \oplus w')$.
- (B-3) There are distinct $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)$ and $\big(\mathcal{O}, (\mathsf{id}', w', i, b'), z'\big) \in \mathcal{Q}$ using the same "tweak" i such that $\sigma(R_{\mathsf{id}} \oplus w) \oplus b \cdot R_{\mathsf{id}} \oplus z = \sigma(R_{\mathsf{id}'} \oplus w') \oplus b' \cdot R_{\mathsf{id}'} \oplus z'$.

As mentioned in Sect. 4.2.1, the conditions are actually the same as [11].

We bound the probabilities of the above conditions regarding the ideal world probability. First, to have tight bounds for (B-1) and (B-2), we need to break them into $2u$ subconditions. In detail, for every user index $\mathsf{id} \in \{1, ..., u\}$, we define two conditions:

- (B1,id) For the index id, there exists a query record $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big) \in \mathcal{Q}$ and a record of the form $(i, \sigma(R_{\mathsf{id}} \oplus w), \star)$ or $(i, \star, \sigma(R_{\mathsf{id}} \oplus w) \oplus b \cdot R_{\mathsf{id}} \oplus z)$ in $\mathcal{Q}[E]$.
- (B2,id) For the index id, there exist two records $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)$ and $\big(\mathcal{O}, (\mathsf{id}', w', i, b'), z'\big) \in \mathcal{Q}$ such that $\sigma(R_{\mathsf{id}} \oplus w) = \sigma(R_{\mathsf{id}'} \oplus w')$.

It is easy to see (B-1) = (B1,1) $\vee$ ... $\vee$ (B1,u) and (B-2) = (B2,1) $\vee$ ... $\vee$ (B2,u).

We next focus on (B1,id) and (B2,id). These two subconditions are fulfilled only if the id-th key R_{id} in the "dummy" key vector $\mathbf{R}$ (sampled at the end) falls into certain sets of "bad keys". For this, for any $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big) \in \mathcal{Q}$, define

$$\begin{aligned}&\mathsf{BadK}^{+}_1(\mathsf{id}, w, i, b, z) := \big\{R^* \in \mathcal{R} : (i, \sigma(R^* \oplus w), \star) \in \mathcal{Q}[E]\big\} \\ &\mathsf{BadK}^{-}_1(\mathsf{id}, w, i, b, z) := \big\{R^* \in \mathcal{R} : (i, \star, \sigma(R^* \oplus w) \oplus bR^* \oplus z) \in \mathcal{Q}[E]\big\}. \qquad (12)\end{aligned}$$

For each record $(i, x, y) \in \mathcal{Q}[E, i]$, the number of R^* such that $\sigma(R^* \oplus w) = x$ is exactly one, since σ is a permutation. This means

$$\left|\mathsf{BadK}_1^+(\mathsf{id}, w, i, b, z)\right| \leq \left|\mathcal{Q}[E, i]\right|.$$

On the other hand, the condition $(i, \star, \sigma(R^* \oplus w) \oplus bR^* \oplus z) \in \mathcal{Q}[E]$ is equivalent with $(i, \star, \sigma(R^*) \oplus \sigma(w) \oplus bR^* \oplus z) \in \mathcal{Q}[E]$ by linearity of σ. Now, note that:

- When $b = 0$, the number of R^* such that $(i, \sigma(R^* \oplus w), \star) \in \mathcal{Q}[E]$ is at most $|\mathcal{Q}[E, i]|$, since σ is a permutation;
- When $b = 1$, the number of R^* such that $(i, \star, \sigma(R^* \oplus w) \oplus bR^* \oplus z) \in \mathcal{Q}[E]$ is at most $|\mathcal{Q}[E, i]|$ as well, since σ is an orthomorphism.

Therefore, it always holds $\left|\mathsf{BadK}_1^-(\mathsf{id}, w, i, b, z)\right| \leq |\mathcal{Q}[E, i]|$.

Define a set of "bad keys" for id as:

$$\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id}) := \bigcup_{(\mathcal{O}, (\mathsf{id}, w, i, b), z) \in \mathcal{Q}} \Big(\mathsf{BadK}_1^+(\mathsf{id}, w, i, b, z) \cup \mathsf{BadK}_1^-(\mathsf{id}, w, i, b, z)\Big).$$

We will calculate the upper bound on its size later.

We follow similar ideas for (B2,id). First, note that $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)$ and $\big(\mathcal{O}, (\mathsf{id}', w', i, b'), z'\big) \in \mathcal{Q}$ have $\sigma(R_{\mathsf{id}} \oplus w) = \sigma(R_{\mathsf{id}'} \oplus w')$ only if $\mathsf{id}' \neq \mathsf{id}$: otherwise, it implies $w = w'$ which is not possible by the restriction (i) of Definition 1.

When $\mathsf{id}' \neq \mathsf{id}$, (B2,$\mathsf{id}$) occurs only if R_{id} falls into certain bad sets. For this, for each pair of distinct records $\big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)$, $\big(\mathcal{O}, (\mathsf{id}', w', i, b'), z'\big) \in \mathcal{Q}$ with $\mathsf{id}' \neq \mathsf{id}$, define

$$\mathsf{BadK}_2\big((\mathsf{id}, w, i, b, z), (\mathsf{id}', w', i, b', z')\big) := \big\{R^* \in \mathcal{R} : \sigma(R^* \oplus w) = \sigma(R_{\mathsf{id}'} \oplus w')\big\}.$$

The number of R^* satisfying $\sigma(R^* \oplus w) = \sigma(R_{\mathsf{id}'} \oplus w')$ is exactly 1. Therefore,

$$\left|\mathsf{BadK}_2\big((\mathsf{id}, w, i, b, z), (\mathsf{id}', w', i, b', z')\big)\right| = 1.$$

Define another set of "bad keys" for id as:

$$\mathsf{BadK}_2(\mathcal{Q}, \mathsf{id}) := \bigcup_{(\mathcal{O}, (\mathsf{id}, w, i, b), z), (\mathcal{O}, (\mathsf{id}', w', i, b'), z') \in \mathcal{Q}} \mathsf{BadK}_2\big((\mathsf{id}, w, i, b, z), (\mathsf{id}', w', i, b', z')\big).$$

Since the key vector $\mathbf{R} = (R_1, ..., R_u)$ in $\mathcal{Q}_x = (\mathcal{Q}, \mathbf{R})$ is sampled from $\mathcal{R}(\mathcal{Q})$ at the end, the id-th key R_{id} in $\mathbf{R}$ is sampled from $\mathcal{R}(\mathcal{Q}, \mathsf{id})$, and it holds

$$\Pr\big[R_{\mathsf{id}} \in \mathsf{BadK}_i(\mathcal{Q}, \mathsf{id}) \mid T_{\mathrm{id}} = \mathcal{Q}\big] \leq \min\left\{\frac{\left|\mathsf{BadK}_i(\mathcal{Q}, \mathsf{id})\right|}{\left|\mathcal{R}(\mathcal{Q}, \mathsf{id})\right|}, 1\right\} \leq \frac{\left|\mathsf{BadK}_i(\mathcal{Q}, \mathsf{id})\right|}{\left|\mathcal{R}(\mathcal{Q}, \mathsf{id})\right|}$$

for $i = 1, 2$. Since (B1,id)$\vee$(B2,id) is fulfilled if and only if $R_{\mathsf{id}} \in \big(\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id}) \cup \mathsf{BadK}_2(\mathcal{Q}, \mathsf{id})\big)$, we have

$$\begin{aligned}
&\Pr\big[(\text{B1,id}) \vee (\text{B2,id})\big] \\
&\leq \sum_{\mathcal{Q}\in\mathcal{T}} \left(\Pr\big[T_{\text{id}} = \mathcal{Q}\big] \times \Pr\big[R_{\mathsf{id}} \in \big(\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id}) \cup \mathsf{BadK}_2(\mathcal{Q}, \mathsf{id})\big) \mid T_{\text{id}} = \mathcal{Q}\big] \right) \\
&\leq \sum_{\mathcal{Q}\in\mathcal{T}} \left(\Pr\big[T_{\text{id}} = \mathcal{Q}\big] \times \frac{\big|\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id})\big| + \big|\mathsf{BadK}_2(\mathcal{Q}, \mathsf{id})\big|}{\big|\mathcal{R}(\mathcal{Q}, \mathsf{id})\big|} \right). \qquad (13)
\end{aligned}$$

We now distinguish the users that received key leaking queries from the others. Formally, let $\mathcal{U} \subseteq \{1, ..., u\}$ be the set such that $\mathsf{id} \in \mathcal{U}$ if and only if $\big(\mathcal{L}, (\mathsf{id}, P), r\big) \in \mathcal{Q}$ for some P and r (i.e., $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ was queried). Then,

$$\begin{aligned}
\Pr\big[(\text{B-1}) \vee (\text{B-2})\big] &\leq \sum_{\mathsf{id}\in\{1,\ldots,u\}} \Pr\big[(\text{B1,id}) \vee (\text{B2,id})\big] \\
&= \underbrace{\sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \Pr\big[(\text{B1,id}) \vee (\text{B2,id})\big]}_{A_1} + \underbrace{\sum_{\mathsf{id}\in\mathcal{U}} \Pr\big[(\text{B1,id}) \vee (\text{B2,id})\big]}_{A_2}.
\end{aligned} \qquad (14)$$

The analysis of A_1 is much simpler than that of A_2. Below we calculate their upper bounds in turn.

Bounding A_1. For any index $\mathsf{id} \in (\{1, ..., u\}\setminus\mathcal{U})$, $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ was never queried and the key R_{id} in $\mathbf{R}$ is sampled from $\mathcal{R}(\mathcal{Q}, \mathsf{id}) = \mathcal{R}$. Therefore,

$$\begin{aligned}
&\sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \Pr\big[(\text{B1,id}) \vee (\text{B2,id})\big] \\
&\leq \sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \sum_{\mathcal{Q}\in\mathcal{T}} \left(\Pr\big[T_{\text{id}} = \mathcal{Q}\big] \times \frac{\big|\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id})\big| + \big|\mathsf{BadK}_2(\mathcal{Q}, \mathsf{id})\big|}{\big|\mathcal{R}\big|} \right) \\
&= \sum_{\mathcal{Q}\in\mathcal{T}} \Pr\big[T_{\text{id}} = \mathcal{Q}\big] \times \left(\sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \frac{\big|\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id})\big| + \big|\mathsf{BadK}_2(\mathcal{Q}, \mathsf{id})\big|}{\big|\mathcal{R}\big|} \right).
\end{aligned}$$

We have

$$\begin{aligned}
\sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \big|\mathsf{BadK}_1(\mathcal{Q}, \mathsf{id})\big| &\leq \sum_{(\mathsf{id},w,i,b,z)\in\mathcal{Q}_{\mathcal{O}}:\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} 2 \cdot \big|\mathcal{Q}[E, i]\big| \\
&\leq \sum_{i\in\{0,1\}^n} \underbrace{\sum_{(\mathsf{id},w,i,b,z)\in\mathcal{Q}_{\mathcal{O}}}}_{\leq\mu} 2 \cdot \big|\mathcal{Q}[E, i]\big| \\
&\leq \mu \cdot \sum_{i\in\{0,1\}^n} 2 \cdot \big|\mathcal{Q}[E, i]\big| = 2\mu q_E. \qquad (15)
\end{aligned}$$

Moreover, if we let $q_{C,i} \leq \mu$ denote the number of queries in $\mathcal{Q}[\mathcal{O}]$ using tweak i, then

$$\begin{aligned}\sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \left|\mathsf{BadK}_2(\mathcal{Q},\mathsf{id})\right| &\leq \sum_{(\mathcal{O},(\mathsf{id},w,i,b),z),(\mathcal{O},(\mathsf{id}',w',i,b'),z')\in\mathcal{Q}} 1 \\ &\leq \sum_{i\in\{0,1\}^n} \binom{q_{C,i}}{2} \\ &\leq (\mu-1)\sum_{i\in\{0,1\}^n} q_{C,i} \leq \frac{(\mu-1)\cdot q_C}{2} \qquad (16)\end{aligned}$$

To simplify notations, define a constant

$$CON := 2\mu q_E + \frac{(\mu-1)\cdot q_C}{2}. \qquad (17)$$

It then holds

$$\begin{aligned}A_1 = \sum_{\mathsf{id}\in(\{1,\ldots,u\}\setminus\mathcal{U})} \Pr\big[(\mathrm{B1},\mathsf{id})\vee(\mathrm{B2},\mathsf{id})\big] &\leq \sum_{\mathcal{Q}\in\mathcal{T}}\left(\Pr\big[T_{\mathrm{id}}=\mathcal{Q}\big]\times\frac{CON}{|\mathcal{R}|}\right) \\ &\leq \frac{CON}{|\mathcal{R}|}. \qquad (18)\end{aligned}$$

Bounding A_2. For any "key leaked" index $\mathsf{id}\in\mathcal{U}$, the key R_{id} in $\mathbf{R}$ is sampled from $\mathcal{R}(\mathcal{Q},\mathsf{id})\subseteq\mathcal{R}$, which varies with id. For $j=1,2$, we follow the ideas of Eqs. (15) and (16) to bound $\left|\mathsf{BadK}_j(\mathcal{Q},\mathsf{id})\right|$ (instead of the sum $\sum_{\mathsf{id}\in\mathcal{U}}\left|\mathsf{BadK}_j(\mathcal{Q},\mathsf{id})\right|$):

$$\begin{aligned}\left|\mathsf{BadK}_1(\mathcal{Q},\mathsf{id})\right| &\leq \sum_{(w,i,b,z):(\mathsf{id},w,i,b,z)\in\mathcal{Q}_{\mathcal{O}}} 2\cdot\left|\mathcal{Q}[E,i]\right| \\ &\leq \sum_{i\in\{0,1\}^n}\underbrace{\sum_{(\mathsf{id},w,i,b,z)\in\mathcal{Q}_{\mathcal{O}}}}_{\leq\mu} 2\cdot\left|\mathcal{Q}[E,i]\right| \leq 2\mu q_E, \\ \left|\mathsf{BadK}_2(\mathcal{Q},\mathsf{id})\right| &\leq \sum_{(\mathcal{O},(\mathsf{id},w,i,b),z),(\mathcal{O},(\mathsf{id}',w',i,b'),z')\in\mathcal{Q}} 1 \\ &\leq \sum_{i\in\{0,1\}^n}\binom{q_{C,i}}{2} \leq \frac{(\mu-1)\cdot q_C}{2}.\end{aligned}$$

Therefore, $\left|\mathsf{BadK}_1(\mathcal{Q},\mathsf{id})\right| + \left|\mathsf{BadK}_2(\mathcal{Q},\mathsf{id})\right| \leq CON$ for the constant defined in Eq. (17). Injecting this into Eq. (13) yields

$$\Pr\big[(\mathrm{B1},\mathsf{id})\vee(\mathrm{B2},\mathsf{id})\big] \leq \sum_{\mathcal{Q}\in\mathcal{T}}\left(\Pr\big[T_{\mathrm{id}}=\mathcal{Q}\big]\times\frac{\left|\mathsf{BadK}_1(\mathcal{Q},\mathsf{id})\right|+\left|\mathsf{BadK}_2(\mathcal{Q},\mathsf{id})\right|}{\left|\mathcal{R}(\mathcal{Q},\mathsf{id})\right|}\right)$$

$$\leq \underbrace{\sum_{\mathcal{Q}\in\mathcal{T}} \left(\Pr\big[(E,f,\mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{CON}{\big|\mathcal{R}(\mathcal{Q},\mathsf{id})\big|} \right)}_{S_{\mathsf{id}}}. \tag{19}$$

For any index $\mathsf{id} \in \mathcal{U}$, i.e., $\mathcal{L}_{\mathbf{R}}(\mathsf{id},\cdot)$ was queried at most $q_{L,max}$ times (as per our assumption), we will prove in Sect. 4.3 that

$$S_{\mathsf{id}} \leq \frac{(q_{L,max}+1)CON}{|\mathcal{R}|}, \tag{20}$$

which is the most technical step (and the bound is independent of id). By this and by $|\mathcal{U}| \leq M$ (as per our assumption), we have

$$\begin{aligned} A_2 = \sum_{\mathsf{id}\in\mathcal{U}} \Pr\big[(\text{B1},\mathsf{id}) \vee (\text{B2},\mathsf{id})\big] &\leq \sum_{\mathsf{id}\in\mathcal{U}} \frac{(q_{L,max}+1)CON}{|\mathcal{R}|} \\ &\leq \frac{M(q_{L,max}+1)CON}{|\mathcal{R}|}. \end{aligned} \tag{21}$$

Summary for (B-1) and (B-2). Gathering Eqs. (14), (18) and (21) yields

$$\begin{aligned} \Pr\big[(\text{B-1}) \vee (\text{B-2})\big] \leq A_1 + A_2 &\leq \frac{CON}{|\mathcal{R}|} + \frac{M(q_{L,max}+1)CON}{|\mathcal{R}|} \\ &\leq \frac{(M+1)(q_{L,max}+1)CON}{|\mathcal{R}|}. \end{aligned} \tag{22}$$

(B-3), and summary for bad transcripts. We finally consider (B-3). For fixed $i \in \{0,1\}^n$, consider a pair of distinct (id,w,i,b,z), $(\mathsf{id}',w',i,b',z') \in \mathcal{Q}_{\mathcal{O}}$. Using the fact that $z,z' \in \{0,1\}^n$ are uniform and independent, we immediately have

$$\Pr\big[\sigma(R_{\mathsf{id}}\oplus w)\oplus bR_{\mathsf{id}}\oplus z = \sigma(R_{\mathsf{id}'}\oplus w')\oplus b'R_{\mathsf{id}'}\oplus z'\big] = \frac{1}{2^n}.$$

If we let $q_{C,i} \leq \mu$ denote the number of queries in $\mathcal{Q}[\mathcal{O}]$ using tweak i, then

$$\Pr\big[(\text{B-3})\big] \leq \sum_{i\in\{0,1\}^n} \binom{q_{C,i}}{2} \cdot \frac{1}{2^n} \leq (\mu-1) \sum_{i\in\{0,1\}^n} \frac{q_{C,i}}{2^{n+1}} \leq \frac{(\mu-1)\cdot q_C}{2^{n+1}}. \tag{23}$$

Gathering Eqs. (22) and (23) and using $|\mathcal{R}| \leq 2^n$ yield

$$\begin{aligned} &\Pr\big[T_{\text{id}} \in \mathcal{T}_{\mathsf{bad}}\big] \leq \Pr\big[(\text{B-1}) \vee (\text{B-2})\big] + \Pr\big[(\text{B-3})\big] \\ &\leq (M+1)(q_{L,max}+1)\Big(2\mu q_E + \frac{(\mu-1)\cdot q_C}{2}\Big)\Big/|\mathcal{R}| + \frac{(\mu-1)\cdot q_C}{2^{n+1}} \\ &\leq \frac{2\mu q_E(M+1)(q_{L,max}+1)}{|\mathcal{R}|} + \frac{(\mu-1)\cdot q_C(M+1)(q_{L,max}+1)}{|\mathcal{R}|}. \end{aligned} \tag{24}$$

4.2.5 Bounding the ratio

Fix a good transcript $\mathcal{Q}_x = (\mathcal{Q}, \mathbf{R})$. The probability that the ideal world is consistent with this transcript is given by Eq. (11). The probability that the real world is consistent with this transcript is

$$\frac{\Pr\big[\forall(\mathcal{O},(\mathsf{id},w,i,b),z) \in \mathcal{Q} : \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id},w,i,b) = z \mid E \vdash \mathcal{Q}\big]}{\prod_{k\in\{0,1\}^n}(2^n)_{|\mathcal{Q}[E,k]|}} \times \Pr\big[\mathbf{R}^* \xleftarrow{\$} (\mathcal{R})^u : \mathbf{R}^* = \mathbf{R}\big]. \tag{25}$$

We can express the numerator of the above as

$$\prod_{j=1}^{q} \Pr[\ \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id},w_j,i_j,b_j) = z_j \mid E \vdash \mathcal{Q} \wedge \forall \ell < j : \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}_\ell,w_\ell,i_\ell,b_\ell) = z_\ell].$$

Note that $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}_j,w_j,i_j,b_j) = z_j$ iff $\widehat{\mathsf{MMO}}^E\big(R_{\mathsf{id}_j}\oplus w_j, i_j\big)\oplus b_j R_{\mathsf{id}_j} = z_j$, i.e.,

$$E\big(i_j, \sigma(R_{\mathsf{id}_j}\oplus w_j)\big) = \sigma(R_{\mathsf{id}_j}\oplus w_j)\oplus b_j R_{\mathsf{id}_j}\oplus z_j.$$

Since the transcript is good, there is no query of the form $(i_j, \sigma(R_{\mathsf{id}_j}\oplus w_j), \star)$ in $\mathcal{Q}[E]$ (since (B-1) does not occur), nor is $E(i_j, \sigma(R_{\mathsf{id}_j}\oplus w_j))$ determined by the fact that $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}_\ell,w_\ell,i_\ell,b_\ell) = z_\ell$ for all $\ell < j$ (since (B-2) does not occur). Similarly, there is no query of the form $(i_j, \star, \sigma(R\oplus w_j)\oplus b_j R\oplus z_j)$ in $\mathcal{Q}[E]$ (since (B-1) does not occur), nor is $E^{-1}(i_j, \sigma(R_{\mathsf{id}_j}\oplus w_j)\oplus b_j R_{\mathsf{id}_j}\oplus z_j)$ determined by the fact that $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}_\ell,w_\ell,i_\ell,b_\ell) = z_\ell$ for all $\ell < j$ (since neither (B-2) nor (B-3) occurs). Thus, for all j we have

$$\Pr[\ \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id},w_j,i_j,b_j) = z_j \mid E \vdash \mathcal{Q} \wedge \forall \ell < j : \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}_\ell,w_\ell,i_\ell,b_\ell) = z_\ell] \geq 1/2^n.$$

It follows that

$$\Pr\big[\forall(\mathcal{O},(\mathsf{id},w,i,b),z) \in \mathcal{Q} : \mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id},w,i,b) = z \mid E \vdash \mathcal{Q}\big] \geq 1/2^{nq_C},$$

and so the probability that the real world is consistent with the transcript is at least the probability that the ideal world is consistent with the transcript. This means Eq. (24) already provides the final advantage bound. This completes the proof.

4.3 Proof of Eq. (20)

Recall that

$$S_{\mathsf{id}} = \sum_{\mathcal{Q}\in\mathcal{T}} \left(\Pr\big[(E,f,\mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{CON}{\big|\mathcal{R}(\mathcal{Q},\mathsf{id})\big|}\right),$$

where $\mathcal{T}$ is the set of all attainable transcripts. Below we proceed with five steps: (1) In Sect. 4.3.1, we introduce the notion of attainable (transcript) prefixes and establish a useful property; (2) In Sect. 4.3.2, we present a "folding lemma" Lemma 2 regarding the sum over transcripts; (3) In Sect. 4.3.3, we study the "mostly folded" (weighted) sum over transcripts and establish an upper bound as the function of the involved coefficients; (4) In Sect. 4.3.4, we bound coefficients in the (weighted) sum. With these, we finally show how to derive Eq. (20) in Sect. 4.3.5.

4.3.1 Attainable (transcript) prefixes

Recall from Sect. 4.2.3 that a transcript is an ordered list

$$\mathcal{Q} = \big((\mathsf{T}_1, \mathsf{Q}_1, \mathsf{A}_1), (\mathsf{T}_2, \mathsf{Q}_2, \mathsf{A}_2), ...\big).$$

For *any ordered list* $\mathcal{Q}$ *of such form*, the number of triples $(\mathsf{T}, \mathsf{Q}, \mathsf{A})$ in $\mathcal{Q}$ is called the *length* of $\mathcal{Q}$, and is denoted $|\mathcal{Q}|$. Define

$$\ell_m := \max_{\mathcal{Q} \in \mathcal{T}} \big\{|\mathcal{Q}|\big\}$$

as the maximal length of attainable transcripts in $\mathcal{T}$.

For any attainable transcript $\mathcal{Q}$, its *prefix of length* ℓ ($\ell \leq |\mathcal{Q}|$) is obtained by deleting the last $|\mathcal{Q}| - \ell$ triples in $\mathcal{Q}$. For any integer $\ell \in \{1, ..., \ell_m\}$, define the set of attainable (transcript) prefixes $\mathcal{T}_\ell$ as

$$\begin{aligned} \mathcal{T}_\ell := &\big\{\mathcal{Q} : \mathcal{Q} \in \mathcal{T},\ |\mathcal{Q}| \leq \ell\big\} \\ &\cup \big\{\mathcal{Q} : |\mathcal{Q}| = \ell \text{ and } (\mathcal{Q}, \mathcal{Q}_{\mathsf{suf}}) \in \mathcal{T} \text{ for some suffix } \mathcal{Q}_{\mathsf{suf}}\big\}. \end{aligned} \tag{26}$$

Namely,

(i) every transcript of length $\leq \ell$ in $\mathcal{T}$ is in $\mathcal{T}_\ell$, and
(ii) for every transcript of length $> \ell$ in $\mathcal{T}$, its *prefix* of length ℓ is in $\mathcal{T}_\ell$.

Clearly, $|\mathcal{T}_{\ell-1}| \leq |\mathcal{T}_\ell|$ for every $\ell \in [2, \ell_m]$.

Certainly, when $\ell < \ell_m$, transcripts in $\mathcal{T}_\ell$ may not be "attainable", i.e., there may exist $\mathcal{Q} \in \mathcal{T}_\ell$ with $\Pr\big[T_{\mathrm{id}} = \mathcal{Q}\big] = 0$. However, they are "attainable" in the sense that for any $\mathcal{Q} \in \mathcal{T}_\ell$, *there always exists some appropriate suffix* $\mathcal{Q}_{\mathsf{suf}}$ *such that* $\Pr\big[T_{\mathrm{id}} = (\mathcal{Q}, \mathcal{Q}_{\mathsf{suf}})\big] > 0$. Consider the execution tree of the interaction between $\mathcal{D}$ and the ideal world oracles, i.e., each time $\mathcal{D}$ issues a query, the tree forks into as many branches as there are possible answers. Then, every $\mathcal{Q} \in \mathcal{T}$ is associated with a complete path in this tree, while *every* $\mathcal{Q} \in \mathcal{T}_\ell$ *is associated with either a complete path or the prefix of several complete paths in this tree.* Therefore, there always exists ideal world randomness $(E, f, \mathbf{R})$ that leads $\mathcal{D}$ to run along $\mathcal{Q}$ (although $\mathcal{D}$ may not terminate at the end of $\mathcal{Q}$).

Attainable transcripts are prefix-free. The set $\mathcal{T}_\ell$ of attainable prefixes of length ℓ can be further partitioned $\mathcal{T}_\ell = \mathcal{T}_{\ell,1} \sqcup \mathcal{T}_{\ell,2}$, where:

- $\mathcal{T}_{\ell,1} = \{\mathcal{Q} \in \mathcal{T}_\ell,\ |\mathcal{Q}| \leq \ell - 1\}$ consists of the transcripts of length $\leq \ell - 1$ in $\mathcal{T}_\ell$, and
- $\mathcal{T}_{\ell,2} = \{\mathcal{Q} \in \mathcal{T}_\ell,\ |\mathcal{Q}| = \ell\}$ consists of the transcripts of length ℓ in $\mathcal{T}_\ell$.

By the definition of $\mathcal{T}_{\ell-1}$, it can be seen:

- $\mathcal{T}_{\ell,1} \subseteq \mathcal{T}_{\ell-1}$, and
- for every $\mathcal{Q} = (\mathcal{Q}_{\mathsf{pre}}, (\mathsf{T}, \mathsf{Q}, \mathsf{A})) \in \mathcal{T}_{\ell,2}$, the prefix $\mathcal{Q}_{\mathsf{pre}}$ is in $\mathcal{T}_{\ell-1}$.

With this in mind, define $\overline{\mathcal{T}_{\ell-1,2}}$ as the set of length $\ell-1$ prefixes of transcripts in $\mathcal{T}_{\ell,2}$, i.e.,

$$\overline{\mathcal{T}_{\ell-1,2}} := \{\mathcal{Q}_{\mathsf{pre}} : (\mathcal{Q}_{\mathsf{pre}}, (\mathsf{T}, \mathsf{Q}, \mathsf{A})) \in \mathcal{T}_{\ell,2} \text{ for some } (\mathsf{T}, \mathsf{Q}, \mathsf{A})\}. \tag{27}$$

We next prove $\mathcal{T}_{\ell,1} \cap \overline{\mathcal{T}_{\ell-1,2}} = \emptyset$, i.e., *attainable transcripts are prefix-free.* This also means $\mathcal{T}_{\ell-1} = \mathcal{T}_{\ell,1} \sqcup \overline{\mathcal{T}_{\ell-1,2}}$. This seems an interesting general property in the information theoretic setting.

Proposition 1

$$\mathcal{T}_{\ell,1} \cap \overline{\mathcal{T}_{\ell-1,2}} = \emptyset, \text{ or equivalently, } \mathcal{T}_{\ell-1} = \mathcal{T}_{\ell,1} \sqcup \overline{\mathcal{T}_{\ell-1,2}} \tag{28}$$

Proof We show that for every $\mathcal{Q} \in \mathcal{T}_{\ell-1}$, exactly one of the following holds:

- $\mathcal{Q}$ is also in $\mathcal{T}_\ell$ (and thus in $\mathcal{T}_{\ell,1}$);
- $\mathcal{Q}$ is the prefix of some $\mathcal{Q}_{\mathsf{pre}} \in \mathcal{T}_\ell$ (thus $\mathcal{Q} \in \overline{\mathcal{T}_{\ell-1,2}}$).

By these, $\mathcal{T}_{\ell,1} \cap \overline{\mathcal{T}_{\ell-1,2}} = \emptyset$.

The argument is as follows. Since $\mathcal{Q} \in \mathcal{T}_{\ell-1}$, $\mathcal{Q}$ is attainable with some randomness $(E, f, \mathbf{R})$. Assume that $\mathcal{D}$ has obtained $\mathcal{Q}$ by its first $\ell-1$ queries. Since $\mathcal{D}$ is deterministic, the next action has been fixed.

- If $\mathcal{D}$ does not issue queries anymore, then $|\mathcal{Q}| = \ell - 1$ and $\mathcal{Q} \in \mathcal{T}_{\ell,1}$. Meanwhile, since $\mathcal{D}$ terminates, $(\mathcal{Q}, (\mathsf{T}, \mathsf{Q}, \mathsf{A}))$ is not attainable for any $(\mathsf{T}, \mathsf{Q}, \mathsf{A})$, meaning that $(\mathcal{Q}, (\mathsf{T}, \mathsf{Q}, \mathsf{A})) \notin \mathcal{T}_\ell$.
- Otherwise, assume that the next query of $\mathcal{D}$ is (T, Q). Then $(\mathcal{Q}, (\mathsf{T}, \mathsf{Q}, \mathsf{A})) \in \mathcal{T}_{\ell,2}$ for all valid answer A, which means $\mathcal{Q} \in \overline{\mathcal{T}_{\ell-1,2}}$. In this case, $\mathcal{Q}$ itself is not a (complete) attainable transcript and $\mathcal{Q} \notin \mathcal{T}_{\ell,1}$.

This establishes the claim. □

4.3.2 Folding lemma

With the above, S_{id} is a (weighted) sum over the set $\mathcal{T} = \mathcal{T}_{\ell_m}$. The "folding lemma" states that S_{id} can be bounded by weighted sums over the smaller sets $\mathcal{T}_{\ell_m-1}, \mathcal{T}_{\ell_m-2}, ..., \mathcal{T}_1$.

Lemma 2 *For every $\ell \in [2, \ell_m]$, any weighted sum over $\mathcal{T}_\ell$ can be bounded by a weighted sum over the smaller set $\mathcal{T}_{\ell-1}$.*

Formally, let

$$S_{\mathit{id},\ell} = \sum_{\mathcal{Q}\in\mathcal{T}_\ell} \left(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q}, \mathit{id}, \ell) \times CON}{|\mathcal{R}(\mathcal{Q}, \mathit{id})|} \right) \tag{29}$$

for some coefficient function $\lambda(\cdot, \mathit{id}, \ell)$. Then, there exists a coefficient function $\lambda(\cdot, \mathit{id}, \ell-1)$ such that

$$S_{\mathit{id},\ell} \le S_{\mathit{id},\ell-1} := \sum_{\mathcal{Q}\in\mathcal{T}_{\ell-1}} \left(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q}, \mathit{id}, \ell-1) \times CON}{|\mathcal{R}(\mathcal{Q}, \mathit{id})|} \right).$$

Proof Recall from Sect. 4.3.1 that $\mathcal{T}_\ell = \mathcal{T}_{\ell,1} \sqcup \mathcal{T}_{\ell,2}$. By this,

$$\begin{aligned} S_{\mathsf{id},\ell} &= \sum_{\mathcal{Q}\in\mathcal{T}_\ell} \left(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q}, \mathsf{id}, \ell) \times CON}{\big|\mathcal{R}(\mathcal{Q}, \mathsf{id})\big|} \right) \\ &= \underbrace{\sum_{\mathcal{Q}\in\mathcal{T}_{\ell,1}} \left(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q}, \mathsf{id}, \ell) \times CON}{\big|\mathcal{R}(\mathcal{Q}, \mathsf{id})\big|} \right)}_{S_{\mathsf{id},\ell,1}} \\ &\quad + \underbrace{\sum_{\mathcal{Q}\in\mathcal{T}_{\ell,2}} \left(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q}, \mathsf{id}, \ell) \times CON}{\big|\mathcal{R}(\mathcal{Q}, \mathsf{id})\big|} \right)}_{S_{\mathsf{id},\ell,2}}. \end{aligned} \tag{30}$$

To proceed, we make a claim as follows.

Proposition 2 *The sum $S_{\mathit{id},\ell,2}$ defined in Eq. (30) is bounded by a sum over $\overline{\mathcal{T}_{\ell-1,2}} = \mathcal{T}_{\ell-1} \backslash \mathcal{T}_{\ell,1}$. In detail, there exists a coefficient function $\lambda'(\cdot, \mathit{id}, \ell-1)$ such that*

$$S_{\mathit{id},\ell,2} \le \sum_{\mathcal{Q}\in\overline{\mathcal{T}_{\ell-1,2}}} \left(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda'(\mathcal{Q}, \mathit{id}, \ell-1) \times CON}{|\mathcal{R}(\mathcal{Q}, \mathit{id})|} \right).$$

where

$$\lambda'(\mathcal{Q}, \mathit{id}, \ell-1) = \begin{cases} \max_{\mathsf{A}}\big\{\lambda((\mathcal{Q}, (\mathsf{T}, \mathsf{Q}, \mathsf{A})), \mathit{id}, \ell)\big\} & \text{if } (\mathcal{Q}, (\mathsf{T}, \mathsf{Q}, \mathsf{A})) \in \mathcal{T}_{\ell,2} \text{ and } \mathsf{T} \in \{E, E^{-1}, \mathcal{O}\} \\ \max_{r=0,1}\big\{\lambda((\mathcal{Q}, (\mathcal{L}, \mathsf{Q}, r)), \mathit{id}, \ell)\big\} & \text{if } (\mathcal{Q}, (\mathcal{L}, \mathsf{Q}, r)) \in \mathcal{T}_{\ell,2} \text{ and } \mathsf{Q} = (\mathit{id}', \star),\ \mathit{id}' \neq \mathit{id} \\ \lambda((\mathcal{Q}, (\mathcal{L}, \mathsf{Q}, 0)), \mathit{id}, \ell) + \lambda((\mathcal{Q}, (\mathcal{L}, \mathsf{Q}, 1)), \mathit{id}, \ell) & \text{if } (\mathcal{Q}, (\mathcal{L}, \mathsf{Q}, r)) \in \mathcal{T}_{\ell,2} \text{ and } \mathsf{Q} = (\mathit{id}, \star) \end{cases}$$

To ease understanding, its proof is presented after this lemma. By Eq. (30) and Proposition 2, we have

$$S_{\mathsf{id},\ell} = S_{\mathsf{id},\ell,1} + S_{\mathsf{id},\ell,2} \le \sum_{\mathcal{Q}\in\mathcal{T}_{\ell,1}} \left(\Pr\big[(E,f,\mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q},\mathsf{id},\ell)\times CON}{\big|\mathcal{R}(\mathcal{Q},\mathsf{id})\big|}\right) + \sum_{\mathcal{Q}\in\overline{\mathcal{T}_{\ell-1,2}}} \left(\Pr\big[(E,f,\mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda'(\mathcal{Q},\mathsf{id},\ell-1)\times CON}{|\mathcal{R}(\mathcal{Q},\mathsf{id})|}\right),$$

where the coefficient function $\lambda'(\cdot,\mathsf{id},\ell-1)$ is defined as in Proposition 2. Since $\mathcal{T}_{\ell-1} = \mathcal{T}_{\ell,1} \sqcup \overline{\mathcal{T}_{\ell-1,2}}$ by Proposition 1, we eventually have

$$S_{\mathsf{id},\ell} \le \sum_{\mathcal{Q}\in\mathcal{T}_{\ell-1}} \left(\Pr\big[(E,f,\mathbf{R}) \vdash \mathcal{Q}\big] \times \frac{\lambda(\mathcal{Q},\mathsf{id},\ell-1)\times CON}{|\mathcal{R}(\mathcal{Q},\mathsf{id})|}\right),$$

where the coefficient function $\lambda(\mathcal{Q},\mathsf{id},\ell-1)$ is defined as:

$$\lambda(\mathcal{Q},\mathsf{id},\ell-1) = \begin{cases} \lambda(\mathcal{Q},\mathsf{id},\ell) & \text{if } \mathcal{Q}\in\mathcal{T}_{\ell,1} \\ \max_{\mathsf{A}}\big\{\lambda((\mathcal{Q},(\mathsf{T},\mathsf{Q},\mathsf{A})),\mathsf{id},\ell)\big\} & \text{if } (\mathcal{Q},(\mathsf{T},\mathsf{Q},\mathsf{A}))\in\mathcal{T}_{\ell,2} \text{ and } \mathsf{T}\in\{E,E^{-1},\mathcal{O}\} \\ \max_{r=0,1}\big\{\lambda((\mathcal{Q},(\mathcal{L},\mathsf{Q},r)),\mathsf{id},\ell)\big\} & \text{if } (\mathcal{Q},(\mathcal{L},\mathsf{Q},r))\in\mathcal{T}_{\ell,2} \text{ and } \mathsf{Q}=(\mathsf{id}',\star),\ \mathsf{id}'\neq\mathsf{id} \\ \lambda((\mathcal{Q},(\mathcal{L},\mathsf{Q},0)),\mathsf{id},\ell)+\lambda((\mathcal{Q},(\mathcal{L},\mathsf{Q},1)),\mathsf{id},\ell) & \text{if } (\mathcal{Q},(\mathcal{L},\mathsf{Q},r))\in\mathcal{T}_{\ell,2} \text{ and } \mathsf{Q}=(\mathsf{id},\star) \end{cases} \tag{31}$$

This completes the proof (of Lemma 2). □

Proof of Proposition 2. Consider each $\mathcal{Q}\in\mathcal{T}_{\ell,2}$ and assume $\mathcal{Q} = \big(\mathcal{Q}_{\mathsf{pre}},(\mathsf{T},\mathsf{Q},\mathsf{A})\big)$, i.e., the latest query in $\mathcal{Q}$ is Q. We distinguish four cases.

– Case 1: $\mathsf{T}=\mathcal{O}$, i.e., $\mathsf{Q}=(\mathsf{id},w,i,b)$ is a construction query. Then it is easy to see all the 2^n transcripts

$$\big(\mathcal{Q}_{\mathsf{pre}},\big(\mathcal{O},(\mathsf{id},w,i,b),z\big)\big),\quad z\in\{0,1\}^n$$

are attainable (because every $z\in\{0,1\}^n$ can be returned by $f(\mathsf{id},w,i,b)$) and are in $\mathcal{T}_{\ell,2}$. For all of them, it holds

$$\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}},\big(\mathcal{O},(\mathsf{id},w,i,b),z\big)\big),\mathsf{id}\big) = \mathcal{R}\big(\mathcal{Q}_{\mathsf{pre}},\mathsf{id}\big),$$

since this set only depends on the key leaking query records, and the key leaking query records in these 2^n transcripts are the same as those in $\mathcal{Q}_{\mathsf{pre}}$. Therefore, summing over these 2^n transcripts yields

$$\sum_{(\mathcal{Q}_{\mathsf{pre}},(\mathcal{O},(\mathsf{id},w,i,b),z)),\ z\in\{0,1\}^n} \Big(\Pr\big[(E,f,\mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \Pr\big[f(\mathsf{id},w,i,b)=z\big]$$

$$\times \frac{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)\big), \mathsf{id}, \ell\big) \times CON}{\big|\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{O}, (\mathsf{id}, w, i, b), z)\big), \mathsf{id}\big)\big|}\Big)$$

$$\leq 2^n \times \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{1}{2^n} \times \frac{\max_{z\in\{0,1\}^n}\big\{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)\big), \mathsf{id}, \ell\big)\big\} \times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})|}$$

$$= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\lambda'(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell - 1) \times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})|},$$

where $\lambda'(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell - 1) = \max_{z\in\{0,1\}^n}\big\{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(\mathcal{O}, (\mathsf{id}, w, i, b), z\big)\big), \mathsf{id}, \ell\big)\big\}$.

– Case 2: $\mathsf{T} = E$, i.e., $\mathsf{Q} = (k, x)$ is a forward ideal cipher query. Let $\mathcal{S} := \big\{y \in \{0,1\}^n : (k, \star, y) \in \mathcal{Q}_{\mathsf{pre}}\big\}$. Then, it can be seen all the $2^n - |\mathcal{S}|$ transcripts

$$\big(\mathcal{Q}_{\mathsf{pre}}, \big(E, (k, x), y\big)\big), \quad y \in \big(\{0,1\}^n \backslash \mathcal{S}\big)$$

are attainable (because every $y \in (\{0,1\}^n \backslash \mathcal{S})$ can be returned by $E(k, x)$) and are in $\mathcal{T}_{\ell,2}$. For all of them, it holds $\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(E, (k, x), y\big)\big), \mathsf{id}\big) = \mathcal{R}\big(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}\big)$ which resembles Case 1. Therefore, summing over these $2^n - |\mathcal{S}|$ transcripts yields

$$\sum_{(\mathcal{Q}_{\mathsf{pre}}, (E,(k,x),y)),\ y\in(\{0,1\}^n\backslash\mathcal{S})} \Big(\Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \Pr\big[E(k, x) = y \mid E \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(E, (k, x), y\big)\big), \mathsf{id}, \ell\big) \times CON}{\big|\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}}, (E, (k, x), y)\big), \mathsf{id}\big)\big|}\Big)$$

$$\leq \big(2^n - |\mathcal{S}|\big) \times \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{1}{2^n - |\mathcal{S}|} \times \frac{\max_{y\in(\{0,1\}^n\backslash\mathcal{S})}\big\{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(E, (k, x), y\big)\big), \mathsf{id}, \ell\big)\big\} \times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})|}$$

$$= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\lambda'(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell - 1) \times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})|},$$

where $\lambda'(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell - 1) = \max_{y\in(\{0,1\}^n\backslash\mathcal{S})}\big\{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, \big(E, (k, x), y\big)\big), \mathsf{id}, \ell\big)\big\}$.

– Case 3: $\mathsf{T} = E^{-1}$, i.e., $\mathsf{Q} = (k, y)$ is a backward ideal cipher query. It is essentially the same as Case 2.
– Case 4: $\mathsf{T} = \mathcal{L}$ and the query $\mathsf{Q} = (\mathsf{id}', P)$ has $\mathsf{id}' \neq \mathsf{id}$. Then, both of the two transcripts

$$\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), 0)\big), \quad \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), 1)\big)$$

are attainable and are in $\mathcal{T}_{\ell,2}$.
Recall from Eq. (10) that for $j = 1, ..., u$, $\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, j)$ is the set of keys R_j that fulfills the predicates queried to $\mathcal{L}_{\mathbf{R}}(j, \cdot)$. Then, conditioned on

$(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}$, for $j = 1, ..., u$ (including $j = \mathsf{id}$), the key R_j is uniformly distributed in $\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, j)$. By these, we have

$$\begin{aligned}
&\Pr\big[(E, f, \mathbf{R}) \vdash \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), 0)\big)\big] \\
&= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \\
&\quad \times \Pr\big[R_{\mathsf{id}'} \in (\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\backslash\mathcal{R}(P)) \mid R_{\mathsf{id}'} \in \mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\big] \\
&= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\backslash\mathcal{R}(P)\big|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\big|}. \qquad (32)
\end{aligned}$$

Similarly,

$$\begin{aligned}
&\Pr\big[(E, f, \mathbf{R}) \vdash \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), 1)\big)\big] \\
&= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{|\mathcal{R}(P)|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\big|}. \qquad (33)
\end{aligned}$$

Since $\mathsf{id}' \neq \mathsf{id}$, the response of the new query $\mathsf{Q} = (\mathsf{id}', P)$ has nothing to do with the distribution of R_{id}:

$$\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), 0)\big), \mathsf{id}\big) = \mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), 1)\big), \mathsf{id}\big) = \mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}).$$

Therefore,

$$\begin{aligned}
&\sum_{r=0,1} \Pr\big[(E, f, \mathbf{R}) \vdash \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), r)\big)\big] \times \frac{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), r)\big), \mathsf{id}, \ell\big) \times CON}{\big|\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), r)\big), \mathsf{id}\big)\big|} \\
&\leq \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\max_{r=0,1}\big\{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), r)\big), \mathsf{id}, \ell\big)\big\} \times CON}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})\big|} \\
&\qquad \times \Big(\frac{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\backslash\mathcal{R}(P)\big|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\big|} + \frac{|\mathcal{R}(P)|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}')\big|}\Big) \\
&= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\lambda'(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell - 1) \times CON}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})\big|},
\end{aligned}$$

with $\lambda'(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell - 1) = \max_{r=0,1}\big\{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}', P), r)\big), \mathsf{id}, \ell\big)\big\}$.

– Case 5: $\mathsf{T} = \mathcal{L}$ and the query $\mathsf{Q} = (\mathsf{id}, P)$ is to the id-th user. Then, both of the two transcripts

$$\big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}, P), 0)\big), \quad \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}, P), 1)\big)$$

are attainable and are in $\mathcal{T}_{\ell,2}$.
The analysis is similar to Case 4. Concretely, substituting the index id' in Eqs. (32) and (33) with id yields the probabilities needed in this case:

$$\begin{aligned}
&\Pr\big[(E, f, \mathbf{R}) \vdash \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}, P), 0)\big)\big] \\
&= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})\backslash\mathcal{R}(P)\big|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})\big|}, \\
&\Pr\big[(E, f, \mathbf{R}) \vdash \big(\mathcal{Q}_{\mathsf{pre}}, (\mathcal{L}, (\mathsf{id}, P), 1)\big)\big] \\
&= \Pr\big[(E, f, \mathbf{R}) \vdash \mathcal{Q}_{\mathsf{pre}}\big] \times \frac{|\mathcal{R}(P)|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id})\big|}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\sum_{r=0,1}\Pr\big[(E,f,\mathbf{R})\vdash\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),r)\big)\big]\times\frac{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),r)\big),\mathsf{id},\ell\big)\times CON}{\big|\mathcal{R}\big(\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),r)\big)\big)\big|}\\
&=\Pr\big[(E,f,\mathbf{R})\vdash\mathcal{Q}_{\mathsf{pre}}\big]\times\Bigg(\frac{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})\backslash\mathcal{R}(P)\big|}{\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})\big|}\\
&\qquad\qquad\times\frac{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),0)\big),\mathsf{id},\ell\big)\times CON}{\big(\big|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})\backslash\mathcal{R}(P)\big|\big)\times\prod_{j=1,\ldots,\mathsf{id}-1,\mathsf{id}+1,\ldots,u}|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},j)|}\\
&\qquad\qquad+\frac{|\mathcal{R}(P)|}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})|}\times\frac{\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),1)\big),\mathsf{id},\ell\big)\times CON}{|\mathcal{R}(P)|\times\prod_{j=1,\ldots,\mathsf{id}-1,\mathsf{id}+1,\ldots,u}|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},j)|}\Bigg)\\
&=\Pr\big[(E,f,\mathbf{R})\vdash\mathcal{Q}_{\mathsf{pre}}\big]\times\frac{\lambda(\mathcal{Q}_{\mathsf{pre}},\mathsf{id},\ell-1)\times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})|\times\prod_{j=1,\ldots,\mathsf{id}-1,\mathsf{id}+1,\ldots,u}|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},j)|}\\
&=\Pr\big[(E,f,\mathbf{R})\vdash\mathcal{Q}_{\mathsf{pre}}\big]\times\frac{\lambda'(\mathcal{Q}_{\mathsf{pre}},\mathsf{id},\ell-1)\times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})|},
\end{aligned}$$

with $\lambda'(\mathcal{Q}_{\mathsf{pre}},\mathsf{id},\ell-1)=\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),0)\big),\mathsf{id},\ell\big)+\lambda\big(\big(\mathcal{Q}_{\mathsf{pre}},(\mathcal{L},(\mathsf{id},P),1)\big),\mathsf{id},\ell\big)$.

In summary, in every case, it holds

$$\begin{aligned}
S_{\mathsf{id},\ell,2}&=\sum_{\mathcal{Q}\in\mathcal{T}_\ell,|\mathcal{Q}|=\ell}\left(\Pr\big[(E,f,\mathbf{R})\vdash\mathcal{Q}\big]\times\frac{\lambda(\mathcal{Q},\mathsf{id},\ell)\times CON}{|\mathcal{R}(\mathcal{Q},\mathsf{id})|}\right)\\
&\le\sum_{\mathcal{Q}_{\mathsf{pre}}:(\mathcal{Q}_{\mathsf{pre}},(\mathsf{T},\mathsf{Q},\mathsf{A}))\in\mathcal{T}_\ell}\left(\Pr\big[(E,f,\mathbf{R})\vdash\mathcal{Q}_{\mathsf{pre}}\big]\times\frac{\lambda'(\mathcal{Q}_{\mathsf{pre}},\mathsf{id},\ell-1)\times CON}{|\mathcal{R}(\mathcal{Q}_{\mathsf{pre}},\mathsf{id})|}\right)
\end{aligned}$$

for the function $\lambda'(\mathcal{Q}_{\mathsf{pre}},\mathsf{id},\ell-1)$ defined in the main claim. This completes the proof.

4.3.3 The sum $S_{id,1}$

Lemma 2 "reduces" $S_{\mathsf{id}}=S_{\mathsf{id},\ell_m}$ to the "mostly folded" weighted sum

$$S_{\mathsf{id},1}:=\sum_{\mathcal{Q}\in\mathcal{T}_1}\left(\Pr\big[(E,f,\mathbf{R})\vdash\mathcal{Q}\big]\times\frac{\lambda(\mathcal{Q},\mathsf{id},1)\times CON}{|\mathcal{R}(\mathcal{Q},\mathsf{id})|}\right).\tag{34}$$

It can be seen that transcripts in $\mathcal{T}_1$ are all of the form $\big((\mathsf{T}_1,\mathsf{Q}_1,\star)\big)$, and are all induced by the possible answers to the first query Q_1 of the distinguisher. Since $\mathcal{D}$ is deterministic, this query is fixed and $\mathcal{T}_1$ contains all the possible responses. By these, it turns out that $S_{\mathsf{id},1}$ is bounded by a simple function of the coefficients $\lambda(\cdot,\mathsf{id},1)$.

Lemma 3 *Let $\mathcal{T}_1=\big\{\big((\mathsf{T}_1,\mathsf{Q}_1,\mathsf{A}_{1,1}),(\mathsf{T}_1,\mathsf{Q}_1,\mathsf{A}_{1,2}),\ldots\big)\big\}$. Then,*

$S_{id,1}\le$

$$\begin{cases} \frac{\max_{\mathsf{A}\in\{0,1\}^n}\left\{\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,\mathsf{A})),\mathit{id},1)\right\}\times CON}{|\mathcal{R}|} & \text{if } \mathsf{T}_1 \in \{E, E^{-1}, \mathcal{O}\} \\ \frac{\max_{\mathsf{A}=0,1}\left\{\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,\mathsf{A})),\mathit{id},1)\right\}\times CON}{|\mathcal{R}|} & \text{if } \mathsf{T}_1 = \mathcal{L} \text{ and} \\ & \mathcal{Q} = (\mathit{id}', \star),\ \mathit{id}' \neq \mathit{id} \\ \frac{\left(\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,0)),\mathit{id},1)+\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,1)),\mathit{id},1)\right)\times CON}{|\mathcal{R}|} & \text{if } \mathsf{T}_1 = \mathcal{L} \text{ and } \mathcal{Q} = (\mathit{id}, \star) \end{cases} \tag{35}$$

Proof Depending on T_1 and Q_1, we distinguish four cases.

– Case 1: $\mathsf{T}_1 = \mathcal{O}$, i.e., $\mathsf{Q}_1 = (\mathsf{id}, w, i, b)$ is a construction query. Then it is easy to see

$$\mathcal{T}_1 = \left\{\left(\mathcal{O}, (\mathsf{id}, w, i, b), z\right)\right\}_{z\in\{0,1\}^n}.$$

For all of them, it holds $\mathcal{R}\left(\left(\mathcal{O}, (\mathsf{id}, w, i, b), z\right), \mathsf{id}\right) = \mathcal{R}$. Therefore,

$$\begin{aligned} S_{\mathsf{id},1} &= \sum_{\mathcal{Q}\in\mathcal{T}_1}\left(\Pr\left[(E, f, \mathbf{R}) \vdash \mathcal{Q}\right] \times \frac{\lambda(\mathcal{Q}, \mathsf{id}, 1) \times CON}{|\mathcal{R}(\mathcal{Q}, \mathsf{id})|}\right) \\ &\leq 2^n \times \frac{1}{2^n} \times \frac{\max_{z\in\{0,1\}^n}\left\{\lambda\left(\left(\mathcal{O}, (\mathsf{id}, w, i, b), z\right), \mathsf{id}, 1\right)\right\} \times CON}{|\mathcal{R}|} \\ &= \frac{\max_{z\in\{0,1\}^n}\left\{\lambda\left(\left(\mathcal{O}, (\mathsf{id}, w, i, b), z\right), \mathsf{id}, 1\right)\right\} \times CON}{|\mathcal{R}|}. \end{aligned}$$

– Case 2: $\mathsf{T}_1 = E$, i.e., $\mathsf{Q}_1 = (k, x)$ is a forward ideal cipher query. Then it is easy to see

$$\mathcal{T}_1 = \left\{\left(E, (k, x), y\right)\right\}_{y\in\{0,1\}^n}.$$

In a similar vein to Case 1, we have

$$\begin{aligned} S_{\mathsf{id},1} &= \sum_{\mathcal{Q}\in\mathcal{T}_1}\left(\Pr\left[(E, f, \mathbf{R}) \vdash \mathcal{Q}\right] \times \frac{\lambda(\mathcal{Q}, \mathsf{id}, 1) \times CON}{|\mathcal{R}(\mathcal{Q}, \mathsf{id})|}\right) \\ &\leq 2^n \times \frac{1}{2^n} \times \frac{\max_{y\in\{0,1\}^n}\left\{\lambda\left(\left(E, (k, x), y\right), \mathsf{id}, 1\right)\right\} \times CON}{|\mathcal{R}|} \\ &= \frac{\max_{y\in\{0,1\}^n}\left\{\lambda\left(\left(E, (k, x), y\right), \mathsf{id}, 1\right)\right\} \times CON}{|\mathcal{R}|}. \end{aligned}$$

– Case 3: $\mathsf{T}_1 = E^{-1}$, i.e., $\mathsf{Q}_1 = (k, y)$ is a backward ideal cipher query. It is essentially the same as Case 2.
– Case 4: $\mathsf{T}_1 = \mathcal{L}$ and the query $\mathsf{Q}_1 = (\mathsf{id}', P)$ has $\mathsf{id}' \neq \mathsf{id}$. Then,

$$\mathcal{T}_1 = \left\{(\mathcal{L}, (\mathsf{id}', P), 0),\ (\mathcal{L}, (\mathsf{id}', P), 1)\right\}.$$

Similarly to Case 4 in the proof of Proposition 2, the response of this query has nothing to do with R_{id}, and thus

$$\mathcal{R}\left((\mathcal{L}, (\mathsf{id}', P), 0), \mathsf{id}\right) = \mathcal{R}\left((\mathcal{L}, (\mathsf{id}', P), 1), \mathsf{id}\right) = \mathcal{R}.$$

On the other hand, the number of choices for $R_{\mathsf{id}'}$ such that $P(R_{\mathsf{id}'}) = 0$, resp. $P(R_{\mathsf{id}}) = 1$, is $|\mathcal{R}| - |\mathcal{R}(P)|$, resp. $|\mathcal{R}(P)|$. Therefore,

$$\begin{aligned} S_{\mathsf{id},1} &= \sum_{r=0,1} \Pr\big[(E, f, \mathbf{R}) \vdash (\mathcal{L}, (\mathsf{id}', P), r)\big] \times \frac{\lambda\big((\mathcal{L}, (\mathsf{id}', P), r), \mathsf{id}, 1\big) \times CON}{\big|\mathcal{R}\big((\mathcal{L}, (\mathsf{id}', P), r), \mathsf{id}\big)\big|}\Big) \\ &= \Big(\frac{|\mathcal{R}| - |\mathcal{R}(P)|}{|\mathcal{R}|} \times \frac{\lambda\big((\mathcal{L}, (\mathsf{id}', P), 0), \mathsf{id}, 1\big) \times CON}{|\mathcal{R}|} + \\ &\qquad\qquad \frac{|\mathcal{R}(P)|}{|\mathcal{R}|} \times \frac{\lambda\big((\mathcal{L}, (\mathsf{id}', P), 1), \mathsf{id}, 1\big) \times CON}{|\mathcal{R}|}\Big) \\ &\leq \frac{\max_{r=0,1}\big\{\lambda\big((\mathcal{L}, (\mathsf{id}', P), r), \mathsf{id}, r\big)\big\} \times CON}{|\mathcal{R}|}. \end{aligned}$$

– Case 5: $\mathsf{T}_1 = \mathcal{L}$ and the query $\mathsf{Q}_1 = (\mathsf{id}, P)$ is to the id-th user. Then,

$$\mathcal{T}_1 = \big\{(\mathcal{L}, (\mathsf{id}, P), 0),\ (\mathcal{L}, (\mathsf{id}, P), 1)\big\}.$$

The number of choices for R_{id} such that $P(R_{\mathsf{id}}) = 0$, resp. $P(R_{\mathsf{id}}) = 1$, is $|\mathcal{R}| - |\mathcal{R}(P)|$, resp. $|\mathcal{R}(P)|$. Therefore,

$$\begin{aligned} S_{\mathsf{id},1} &= \sum_{r=0,1} \Pr\big[(E, f, \mathbf{R}) \vdash (\mathcal{L}, (\mathsf{id}, P), r)\big] \times \frac{\lambda\big((\mathcal{L}, (\mathsf{id}, P), r), \mathsf{id}, 1\big) \times CON}{\big|\mathcal{R}\big((\mathcal{L}, (\mathsf{id}, P), r), \mathsf{id}\big)\big|}\Big) \\ &= \Big(\frac{|\mathcal{R}| - |\mathcal{R}(P)|}{|\mathcal{R}|} \times \frac{\lambda\big((\mathcal{L}, (\mathsf{id}, P), 0), \mathsf{id}, 1\big) \times CON}{|\mathcal{R}| - |\mathcal{R}(P)|} + \\ &\qquad\qquad \frac{|\mathcal{R}(P)|}{|\mathcal{R}|} \times \frac{\lambda\big((\mathcal{L}, (\mathsf{id}, P), 1), \mathsf{id}, 1\big) \times CON}{|\mathcal{R}(P)|}\Big) \\ &= \frac{\Big(\lambda\big((\mathcal{L}, (\mathsf{id}, P), 0), \mathsf{id}, 1\big) + \lambda\big((\mathcal{L}, (\mathsf{id}, P), 1), \mathsf{id}, 1\big)\Big) \times CON}{|\mathcal{R}|}. \end{aligned}$$

These complete the proof. □

4.3.4 Bounding the coefficients

Recall from Eq. (19) that a basic condition is $\lambda(\mathcal{Q}, \mathsf{id}, \ell_m) = 1$ for any attainable transcript $\mathcal{Q} \in \mathcal{T} = \mathcal{T}_{\ell_m}$. With this and the above "folding lemma", we now establish upper bounds on the coefficients $\lambda(\cdot, \mathsf{id}, 1), ..., \lambda(\cdot, \mathsf{id}, \ell_m)$ that appeared in the previous sections.

Lemma 4 *For any $\mathcal{Q} \in \mathcal{T}_\ell$, $|\mathcal{Q}| = \ell$, assume that if the interaction between $\mathcal{D}$ and the ideal world oracles yields $\mathcal{Q}$ for its first ℓ queries, then $\mathcal{D}$ makes at most j queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ subsequently. Then, $\lambda(\mathcal{Q}, \mathsf{id}, \ell) \leq j + 1$.*

The lemma can also be stated as a property of the aforementioned execution tree. In detail, consider *any subtree* in the execution tree, and let $\mathcal{Q}$, $|\mathcal{Q}| = \ell$, be the (transcript) prefix corresponding to the path from the root of the execution

tree to the root of the subtree. Then, if none of the paths of this subtree has more than j key leaking queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id},\cdot)$, then the coefficient is bounded by $\lambda(\mathcal{Q},\mathsf{id},\ell) \leq j+1$.

Proof (Proof of Lemma 4) Towards a contradiction, assume that there exists such a $\mathcal{Q}$ with $\lambda(\mathcal{Q},\mathsf{id},\ell) \geq j+2$. We distinguish between $j=0$ and $j>0$, since the former case also serves as a helpful intermediate result.

Base case: $j=0$. Namely, after obtaining the transcript $\mathcal{Q}$, $\mathcal{D}$ never queries $\mathcal{L}_{\mathbf{R}}(\mathsf{id},\cdot)$ anymore. Since $\mathcal{D}$ is deterministic, the next action is fixed.

If $\mathcal{D}$ terminates, then it actually has $\mathcal{Q} \in \mathcal{T}$ is a (complete) attainable transcript, and our assumption $\lambda(\mathcal{Q},\mathsf{id},\ell) \geq j+2 = 2$ clearly contradicts the basic condition that $\lambda(\mathcal{Q},\mathsf{id},\ell_m) = \lambda(\mathcal{Q},\mathsf{id},\ell)$ should have been 1.

If $\mathcal{D}$ still makes queries, then the next query $(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1})$ is fixed, and it holds $\mathsf{Q}_{\ell+1} \neq (\mathsf{id},\star)$ by our assumption of $j=0$. Therefore, Eq. (31) yields

$$\lambda(\mathcal{Q},\mathsf{id},\ell) = \max_{\mathsf{A}_{\ell+1}} \Big\{ \lambda\big((\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}_{\ell+1})),\mathsf{id},\ell+1\big) \Big\}, \tag{36}$$

and our assumption $\lambda(\mathcal{Q},\mathsf{id},\ell) \geq j+2 = 2$ implies that there exists $\mathsf{A}^{\circ}_{\ell+1}$ such that $\lambda\big((\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}^{\circ}_{\ell+1})),\mathsf{id},\ell+1\big) \geq 2$.

We can now repeat our argument for $(\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}^{\circ}_{\ell+1}))$, and it eventually implies the existence of some $\mathcal{Q}_{\mathsf{suf}}$ such that $(\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}^{\circ}_{\ell+1},\mathcal{Q}_{\mathsf{suf}})) \in \mathcal{T} = \mathcal{T}_{\ell_m}$ is "complete" and $\lambda\big(\big(\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}^{\circ}_{\ell+1}),\mathcal{Q}_{\mathsf{suf}}\big),\mathsf{id},\ell'\big) \geq 2$ for $\ell' = \big|\big(\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}^{\circ}_{\ell+1}),\mathcal{Q}_{\mathsf{suf}}\big)\big|$. This contradicts the basic condition.

The case of $j>0$. Namely, after obtaining the transcript $\mathcal{Q}$, $\mathcal{D}$ subsequently makes at most $j \geq 1$ queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id},\cdot)$. Since $\mathcal{D}$ is deterministic, the next query $(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1})$ is fixed. We distinguish three cases as follows.

- Case 1: $\mathcal{D}$ terminates. Then it has $\mathcal{Q} \in \mathcal{T}$, and our assumption $\lambda(\mathcal{Q},\mathsf{id},\ell) \geq j+2 \geq 2$ contradicts that $\lambda(\mathcal{Q},\mathsf{id},\ell_m) = \lambda(\mathcal{Q},\mathsf{id},\ell)$ should have been 1.
- Case 2: $\mathsf{Q}_{\ell+1} = (\mathsf{id},P)$ is a key leaking query to $\mathcal{L}_{\mathbf{R}}(\mathsf{id},\cdot)$. Then, the answer has $\mathsf{A}_{\ell+1} \in \{0,1\}$, and Eq. (31) yields

  $$\lambda(\mathcal{Q},\mathsf{id},\ell) = \lambda\big(\big(\mathcal{Q},(\mathcal{L},\mathsf{Q}_{\ell+1},0)\big),\mathsf{id},\ell+1\big) + \lambda\big(\big(\mathcal{Q},(\mathcal{L},\mathsf{Q}_{\ell+1},1)\big),\mathsf{id},\ell+1\big).$$

  Note that if $\mathcal{D}$ obtains $\big(\mathcal{Q},(\mathcal{L},\mathsf{Q}_{\ell+1},0)\big)$, then the "session" of the id-th user aborts and $\mathcal{D}$ cannot make key leaking queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id},\cdot)$ anymore. Therefore, $\lambda\big(\big(\mathcal{Q},(\mathcal{L},\mathsf{Q}_{\ell+1},0)\big),\mathsf{id},\ell+1\big) = 1$ by our result on the base case that has been established.
  Thus, our assumption $\lambda(\mathcal{Q},\mathsf{id},\ell) \geq j+2$ implies $\lambda\big(\big(\mathcal{Q},(\mathcal{L},\mathsf{Q}_{\ell+1},1)\big),\mathsf{id},\ell+1\big) \geq j+1$.
- Case 3: $\mathsf{Q}_{\ell+1} \neq (\mathsf{id},\star)$. In this case, Eq. (31) yields

  $$\lambda(\mathcal{Q},\mathsf{id},\ell) = \max_{\mathsf{A}_{\ell+1}} \Big\{ \lambda\big((\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}_{\ell+1})),\mathsf{id},\ell+1\big) \Big\}. \tag{37}$$

  and our assumption $\lambda(\mathcal{Q},\mathsf{id},\ell) \geq j+2$ implies there exists $\mathsf{A}^{\circ}_{\ell+1}$ such that $\lambda\big((\mathcal{Q},(\mathsf{T}_{\ell+1},\mathsf{Q}_{\ell+1},\mathsf{A}^{\circ}_{\ell+1})),\mathsf{id},\ell+1\big) \geq j+2$.

In summary, our assumption $\lambda(\mathcal{Q}, \mathsf{id}, \ell) \geq j+2$ implies that at least one of the following three holds:

(i) $\mathcal{Q} \in \mathcal{T} = \mathcal{T}_{\ell_m}$ is "complete" while $\lambda(\mathcal{Q}, \mathsf{id}, \ell) \geq j+2 \geq 2$; or
(ii) There exists $\mathcal{Q}_{\mathsf{pre}} \in \mathcal{T}_{\ell+1}$, $|\mathcal{Q}_{\mathsf{pre}}| = \ell+1$, such that: (a) once obtaining $\mathcal{Q}_{\mathsf{pre}}$, $\mathcal{D}$ makes at most $j-1$ queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ subsequently; and (b) $\lambda(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell+1) \geq j+1 = (j-1)+2$; or
(iii) There exists $\mathcal{Q}_{\mathsf{pre}} \in \mathcal{T}_{\ell+1}$, $|\mathcal{Q}_{\mathsf{pre}}| = \ell+1$, such that: (a) once obtaining $\mathcal{Q}_{\mathsf{pre}}$, $\mathcal{D}$ makes at most j queries to $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ subsequently; and (b) $\lambda(\mathcal{Q}_{\mathsf{pre}}, \mathsf{id}, \ell+1) \geq j+2$.

In the second and third cases, we can repeat the argument for $\mathcal{Q}_{\mathsf{pre}}$, and it will eventually imply the existence of some $\mathcal{Q}_{\mathsf{suf}}$ such that $(\mathcal{Q}, \mathcal{Q}_{\mathsf{suf}}) \in \mathcal{T} = \mathcal{T}_{\ell_m}$ is "complete" and $\lambda\big((\mathcal{Q}, \mathcal{Q}_{\mathsf{suf}}), \mathsf{id}, \ell'\big) \geq 2$ for $\ell' = \big|(\mathcal{Q}, \mathcal{Q}_{\mathsf{suf}})\big|$. This contradicts the basic condition. By these, the assumption $\lambda(\mathcal{Q}, \mathsf{id}, \ell) \geq j+2$ does not hold, which completes the proof. □

4.3.5 Deriving Eq. (20)

By Lemmas 2 and 3, it holds

$$S_{\mathsf{id}} = S_{\mathsf{id},\ell_m} \leq S_{\mathsf{id},\ell_m-1} \leq \ldots \leq S_{\mathsf{id},1}$$
$$\leq \begin{cases} \frac{\max_{\mathsf{A}\in\{0,1\}^n}\left\{\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,\mathsf{A})),\mathsf{id},1)\right\}\times CON}{|\mathcal{R}|} & \text{if } \mathsf{T}_1 \in \{E, E^{-1}, \mathcal{O}\} \\ \frac{\max_{\mathsf{A}=0,1}\left\{\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,\mathsf{A})),\mathsf{id},1)\right\}\times CON}{|\mathcal{R}|} & \text{if } \mathsf{T}_1 = \mathcal{L} \text{ and } \mathcal{Q} = (\mathsf{id}', \star),\ \mathsf{id}' \neq \mathsf{id} \\ \frac{\left(\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,0)),\mathsf{id},1)+\lambda((\mathcal{Q},(\mathsf{T}_1,\mathsf{Q}_1,1)),\mathsf{id},1)\right)\times CON}{|\mathcal{R}|} & \text{if } \mathsf{T}_1 = \mathcal{L} \text{ and } \mathcal{Q} = (\mathsf{id}, \star) \end{cases}$$

Finally

- When $\mathsf{Q}_1 \neq (\mathsf{id}, \star)$, Lemma 4 implies $\lambda(((\mathsf{T}_1, \mathsf{Q}_1, \mathsf{A})), \mathsf{id}, 1) \leq q_{L,max}+1$ for any valid answer A, and thus $S_{\mathsf{id}} \leq S_{\mathsf{id},1} \leq q_{L,max}+1$;
- When $\mathsf{Q}_1 = (\mathsf{id}, P)$ for some P, Lemma 4 implies $\lambda(((\mathsf{T}_1, \mathsf{Q}_1, 0)), \mathsf{id}, 1) = 1$ and $\lambda(((\mathsf{T}_1, \mathsf{Q}_1, \mathsf{A})), \mathsf{id}, 1) \leq q_{L,max}$, and thus $S_{\mathsf{id}} \leq S_{\mathsf{id},1} \leq q_{L,max}+1$.

These complete the proof for Eq. (20).

4.4 Attacks in relevant settings

We first present two attacks in the single-user TCCRL setting in Sect. 4.4.1. We then exhibit two attacks in the multi-user muTCCRL setting in Sect. 4.4.2.

4.4.1 Attacks in the single-user setting

Since there is no multiple users, we **omit the user index id** from the oracle inputs to $\mathcal{O}$ and $\mathcal{L}$. In addition, as discussed in Sect. 4.1, we have $q_L = q_{L,max}$.

Birthday attack. The single-user security bound in Eq. (3) indicates the existence of attacks making q_E queries to E and q_L queries to the key leaking oracle with $q_E q_L \approx |\mathcal{R}|$. We now exhibit such an attack. To this end, assume $\mathcal{R} = \{0,1\}^n$ for simplicity. For any fixed value of q_L, let $\ell = \lceil \log_2 q_L \rceil$, let $[j]_\ell$ be the ℓ-bit encoding of the integer j, and let

$$\mathcal{R}_j = \big\{R \in \{0,1\}^n : \mathsf{leftbits}_\ell(R) = [j]_\ell\big\}. \tag{38}$$

Then, $\mathcal{R} = \{0,1\}^n = \cup_{j=0}^{2^\ell-1}\mathcal{R}_j$. Based on this, we define a series of predicates: for any $j \in \{0,...,2^\ell-1\}$,

$$P_j(R) = 1 \text{ if and only if } R \notin \mathcal{R}_j.$$

With the above preparations, an attack could proceed as follows.

1. Choose $(w,i,0)$ in arbitrary and query $\mathcal{O}_R^{\mathrm{TCCRL}}(w,i,0) \to y$ to obtain y.
2. For $j = 0,...,2^\ell-1$, query $\mathcal{L}_R(P_j)$ to see if $R \in \mathcal{R}_j$, till the oracle $\mathcal{L}_R$ aborts. Note that abortion always occurs since $\cup_{j=0}^{2^\ell-1}\mathcal{R}_j = \{0,1\}^n$.
3. When $\mathcal{L}_R$ aborts, we know $R \in \mathcal{R}_j$ by the definitions, i.e., $\mathsf{leftbits}_\ell(R) = [j]_\ell$. This has significantly reduced the possible key space.
4. Let $\mathcal{U} := w \oplus \mathcal{R}_j$. Query $E(i,u) \to v$ for all $u \in \mathcal{U}$ ($q_E = 2^{n-\ell}$ queries in total). Let $E(i,u^*) \to v^* = y$, then we can recover R via $R = w \oplus u^*$.

This attack consumes 1 construction query (consequently, the limitation enforced by μ is fulfilled), q_L key leaking oracle queries and $2^{n-\ell} = 2^n/q_L$ ideal cipher queries, and succeeds with probability roughly 1. Therefore, the $n - \log_2 q_L$ bits provable security is tight, and security loss is significant when q_L is large.

Attack using Linear masking predicates. As mentioned in Sect. 4.1, q_L can be rather limited in concrete scenarios. For this, consider the linear masking predicates discussed by Roy [24]. In detail, it requires that for every leaking query P there exists $a \in \{0,1\}^n$ such that $P(R) = \langle a, R\rangle$. In this case, every "non-trivial" key leaking query halves the size of the possible key space, and q_L is essentially restricted to $q_L \le n$. Concrete security is thus ensured up to $\frac{|\mathcal{R}|}{\mu(n+1)}$ ideal cipher queries and $2^n/\mu$ construction queries.

To shed more lights, we also provide a concrete attack. Again, assume $\mathcal{R} = \{0,1\}^n$ for simplicity. We define a series of predicates: for any $j \in \{1,2,...,n\}$,

$$P_j(R) = 1 \text{ if and only if } \langle [2^{j-1}]_n, R\rangle = 1. \tag{39}$$

With the above preparations, an attack could proceed as follows.

1. Choose $(w,i,0)$ in arbitrary and query $\mathcal{O}_R^{\mathrm{TCCRL}}(w,i,0) \to y$ to obtain y.
2. For $j = 1,2,...,n$, query $\mathcal{L}_R(P_j)$ to see if $\langle [2^{j+1}]_n, R\rangle = 1$:
   - When $\mathcal{L}_R$ aborts, we know:
     - The rightmost $j-1$ bits of R are all 1, and
     - The j-th rightmost bit of R is 0.

This has reduced the possible key space to 2^{n-j}.
Let $\mathcal{R}^* := \left\{R \in \{0,1\}^n : \mathsf{rightbits}_\ell(R) = [2^{j-1}-1]_j\right\}$ and $\mathcal{U} := w \oplus \mathcal{R}^*$. Query $E(i,u) \to v$ for all $u \in \mathcal{U}$ (2^{n-j} queries in total). Let $E(i,u^*) \to v^* = y$, then we can recover R via $R = w \oplus u^*$.

– If $\mathcal{L}_R$ never aborts, then $R = [2^n - 1]_n$, i.e., all bits of R are 1. This recovers R.[4]

This attack consumes 1 construction query and has roughly 1 success probability. However, unlike ordinary attacks, this attack has probabilistic complexities. We now calculate the expectations of its leaking oracle and ideal cipher query complexities. To this end, note that for any $j \in \{1,...,n\}$, the probability to have

$$P_j(R) = 0 \wedge P_{j-1}(R) = 1 \wedge ... \wedge P_1(R) = 1 \tag{40}$$

is $\frac{1}{2^j}$. When the "right" key satisfies Eq. (40), the attack consumes j key leaking queries and 2^{n-j} ideal cipher queries.

Finally, when the "right" key satisfies

$$P_n(R) = 1 \wedge P_{n-1}(R) = 1 \wedge ... \wedge P_1(R) = 1 \tag{41}$$

(the probability is $1/2^n$), the attack consumes n leaking oracle queries and 1 ideal cipher queries. Therefore,

$$\mathbb{E}[q_L] = \Big(\sum_{j=1}^{n} \frac{j}{2^j}\Big) + \frac{n}{2^n} = \frac{1-\frac{1}{2^n}}{1-\frac{1}{2}} + \frac{n}{2^{n-1}} \leq 2 + \frac{n}{2^{n-1}} \approx 2,$$

$$\mathbb{E}[q_E] = \Big(\sum_{j=1}^{n} \frac{2^{n-j}}{2^j}\Big) + \frac{1}{2^n} = 2^n \times \Big(\Big(\sum_{j=1}^{n} \frac{1}{4^n}\Big) + \frac{1}{4^n}\frac{1}{4^n}\Big) \leq 2^n/3.$$

We remark that the expected complexities are somewhat incomparable with the bound in Theorem 1, which addresses the worse case.

4.4.2 Attacks in the multi-user setting

Birthday attack using 1 leaking query per user. As will be seen in Sect. 5, in the application to OT extension one has $q_{L,max} = 1$. We now show that in this case, there is an attack with $q_E M \approx |\mathcal{R}|$.

Again, assume $\mathcal{R} = \{0,1\}^n$ for simplicity. For any fixed value of M such that $M \leq u$, fix $\mathcal{R}^\circ \subset \mathcal{R}$ with $|\mathcal{R}^\circ| = 2^n/M$. Define

$$P(R) = 1 \text{ if and only if } R \in \mathcal{R}^\circ.$$

Our attack proceeds as follows.

[4] We stress that this is insufficient for distinguishing, since the same result may be obtained in the ideal world. To distinguish, one could query the ideal cipher $E\big(i, \sigma(w \oplus [2^n - 1]_n)\big) \to y'$ and check if $y' = y$. Crucially, this distinguishing attack has $q_E \geq 1$, and the complexities are matched by Theorem 1.

1. For $\mathsf{id} \in \{1, ..., u\}$, query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$, till $R_{\mathsf{id}} \in \mathcal{R}^{\circ}$, i.e., $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$ does not abort. Let id° be the first index such that $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^{\circ}, P)$ does not abort.
2. Choose $(w, i, 0)$ in arbitrary and query $\mathcal{O}_{\mathbf{R}}^{\text{muTCCRL}}(\mathsf{id}^{\circ}, w, i, 0) \to y = \widehat{\mathsf{MMO}}^{E}(w \oplus R_{\mathsf{id}^{\circ}}, i)$ to obtain y.
3. Let $\mathcal{U} := w \oplus \mathcal{R}^{\circ}$. Query $E(i, u) \to v$ for all $u \in \mathcal{U}$ ($|\mathcal{R}^{\circ}|$ queries in total). Let $E(i, u^*) \to v^* = y$, then we can recover R via $R = w \oplus u^*$.

This attack has $q_C = 1$, $q_{L,max} = 1$ (but $q_L = M$) and $|\mathcal{R}^{\circ}| = 2^n/M$ ideal cipher queries. Since $\Pr\left[R \xleftarrow{\$} \{0,1\}^n : R \in \mathcal{R}^{\circ}\right] = |\mathcal{R}^{\circ}|/2^n = 1/M$, it is expected to have at least 1 user index id° such that $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^{\circ}, P)$ does not abort and $R_{\mathsf{id}^{\circ}} \in \mathcal{R}^{\circ}$. By querying $E(i, u) \to v$ for all $u \in \mathcal{U}$, one can then recover the key $R_{\mathsf{id}^{\circ}}$. Since $M q_{L,max} q_E = M \times \frac{2^n}{M} = 2^n$, this matches our bound in Theorem 1.

Linear masking predicates in multi-user setting. Consider the aforementioned linear masking predicates discussed by Roy [24]. Again, assume $\mathcal{R} = \{0,1\}^n$ for simplicity. Recall from Eq. (39) for the definition of the predicate P_j. Let $\ell = \lfloor \log_2 u \rfloor$. With the above preparations, we provide an attack as follows.

1. For $\mathsf{id} = 1, ..., u$, $j = 1, 2, ..., \ell$, query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P_j)$ to see if $\langle [2^{j+1}]_n, R_{\mathsf{id}} \rangle = 1$, till $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ aborts.
2. Let id° be the smallest user index such that $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ does not abort. Choose $(w, i, 0)$ in arbitrary and query $\mathcal{O}_{\mathbf{R}}^{\text{muTCCRL}}(\mathsf{id}^{\circ}, w, i, 0) \to y = \widehat{\mathsf{MMO}}^{E}(w \oplus R_{\mathsf{id}^{\circ}}, i)$ to obtain y.
3. Let $\mathcal{R}^* := \left\{R \in \{0,1\}^n : \mathsf{rightbits}_{\ell}(R) = [2^{\ell} - 1]_{\ell}\right\}$ and $\mathcal{U} := w \oplus \mathcal{R}^*$. Query $E(i, u) \to v$ for all $u \in \mathcal{U}$ ($2^{n-\ell}$ queries in total). Let $E(i, u^*) \to v^* = y$, then we can recover $R_{\mathsf{id}^{\circ}}$ via $R_{\mathsf{id}^{\circ}} = w \oplus u^*$.

As analyzed before, for every id the probability that $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, \cdot)$ does not abort is $1/2^{\ell}$. Since $\ell = \lfloor \log_2 u \rfloor$, we are expected to have some index id° such that $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^{\circ}, \cdot)$ does not abort. Therefore, the success probability is roughly 1. This attack consumes 1 construction query, $u\lfloor \log_2 u \rfloor$ leaking oracle queries ($\log_2 u$ queries per user) and $2^{n-\ell} \approx 2^n/u$ ideal cipher queries.

5 Oblivious-Transfer Extension

As an application of Theorem 1, in this section we show an OT extension protocol with non-trivial multi-user security. Following [7], we also focus on the random-OT-to-standard-OT transformation and its malicious security, which suffices for an instructive example. Following [12], we also present all our protocols in the $\mathcal{F}_{\Delta\text{-ROT}}$-hybrid model: see Fig. 1. This ideal functionality provides an abstraction of the first phase of OT extension.

Functionality $\mathcal{F}_{\Delta\text{-ROT}}(m,k)$

Initialize: Upon receiving (Init, Δ) from $\mathsf{P_A}$ with $\Delta \in \{0,1\}^k$, and (Init) from $\mathsf{P_B}$, store Δ and ignore subsequent Init commands.

Set up correlations: Upon receiving $(x_1, \ldots, x_m)$ from $\mathsf{P_B}$ with $x_i \in \{0,1\}$ do:

1. For each $i \in \{1, ..., m\}$, sample uniform $\mathbf{a}_i, \mathbf{b}_i \in \{0,1\}^k$ such that $\mathbf{a}_i \oplus \mathbf{b}_i = x_i \cdot \Delta$.
2. If $\mathsf{P_A}$ is corrupted, wait for $\mathcal{A}$ to send $\{\mathbf{a}_i\}$ and recompute $\{\mathbf{b}_i\}$ accordingly. If $\mathsf{P_B}$ is corrupted, wait for $\mathcal{A}$ to send $\{\mathbf{b}_i\}$ and recompute $\{\mathbf{a}_i\}$ accordingly.
3. Send $\{\mathbf{a}_i\}$ to $\mathsf{P_A}$ and $\{\mathbf{b}_i\}$ to $\mathsf{P_B}$.

Global key query: If $\mathsf{P_B}$ is corrupted then $\mathcal{A}$ can send a predicate $P : \{0,1\}^k \to \{0,1\}$ to the functionality after initialization but before sending its input. If $P(\Delta) = 1$, the functionality sends 1 to $\mathcal{A}$; otherwise, the functionality aborts and notifies $\mathsf{P_A}$.

Fig. 1: Functionality $\mathcal{F}_{\Delta\text{-ROT}}$.

Functionality $\mathcal{F}_{\text{S-OT}}(m,n)$

Upon receiving $\big((\mathbf{m}_1^0, \mathbf{m}_1^1), \ldots, (\mathbf{m}_m^0, \mathbf{m}_m^1)\big)$ from $\mathsf{P_A}$ with $\mathbf{m}_i^b \in \{0,1\}^n$ for all $i \in \{1, ..., m\}$ and $b \in \{0,1\}$ and $(x_1, \ldots, x_m)$ from $\mathsf{P_B}$ with $x_i \in \{0,1\}$, send $\{\mathbf{m}_i^{x_i}\}$ to $\mathsf{P_B}$.

Fig. 2: Functionality $\mathcal{F}_{\text{S-OT}}$ for standard OT.

Protocol $\prod_{\text{S-OT}}^{m,k,n}$ $(k < n)$

Inputs: $\mathsf{P_A}$ has $(\mathbf{m}_1^0, \mathbf{m}_1^1), \ldots, (\mathbf{m}_m^0, \mathbf{m}_m^1)$ with $\mathbf{m}_i^b \in \{0,1\}^n$ for all $i \in \{1, ..., m\}$ and $b \in \{0,1\}$, and $\mathsf{P_B}$ has $x_1, \ldots, x_m$ with $x_i \in \{0,1\}$.

Protocol:

1. $\mathsf{P_A}$ chooses uniform $\Delta \xleftarrow{\$} \{0,1\}^k$ and sends (Init, Δ) to $\mathcal{F}_{\Delta\text{-ROT}}$; $\mathsf{P_B}$ sends (Init) to $\mathcal{F}_{\Delta\text{-ROT}}$.
2. $\mathsf{P_B}$ sends $(x_1, \ldots, x_m)$ to $\mathcal{F}_{\Delta\text{-ROT}}$, which returns $\mathbf{a}_1, \ldots, \mathbf{a}_m$ to $\mathsf{P_A}$ and $\mathbf{b}_1, \ldots, \mathbf{b}_m$ to $\mathsf{P_B}$.
3. Player $\mathsf{P_A}$ chooses $IV \xleftarrow{\$} \{0, 1, ..., 2^n - 1\}$, and computes, for all $i \in \{1, ..., m\}$,
$$\begin{aligned} \mathbf{c}_i^0 &:= H(\mathbf{a}_i, IV \oplus [i]_n) \oplus \mathbf{m}_i^0, \\ \mathbf{c}_i^1 &:= H(\mathbf{a}_i \oplus \Delta, IV \oplus [i]_n) \oplus \mathbf{m}_i^1 \end{aligned} \tag{42}$$
$\mathsf{P_A}$ then sends $IV, \mathbf{c}_1^0, \mathbf{c}_1^1, ..., \mathbf{c}_m^0, \mathbf{c}_m^0$ to $\mathsf{P_B}$.
4. $\mathsf{P_B}$ then computes $\mathbf{m}_i^{x_i} := \mathbf{c}_i^{x_i} \oplus H(\mathbf{b}_i, IV \oplus [i]_n)$ for all $i \in \{1, ..., m\}$, and outputs $(\mathbf{m}_1^{x_1}, ..., \mathbf{m}_m^{x_m})$. Player $\mathsf{P_A}$ outputs $\perp$.

Fig. 3: Protocol $\prod_{\text{S-OT}}^{m,k,n}$ in the $\mathcal{F}_{\Delta\text{-ROT}}$-hybrid model.

5.1 Multi-user security definition of 2PC malicious security

Fig. 2 describes the standard OT functionality $\mathcal{F}_{\text{S-OT}}$. Ideal functionalities proceed in rounds of simultaneous inputs, for which they produce (simultaneously) outputs. A functionality $\mathcal{F}$ offers three interfaces two are to the players P_A and P_B, and the third to the adversary $\mathcal{A}$. In each round of each protocol instance, either (1) one party sends a message to the other party, or (2) they simultaneously interact with the functionality $\mathcal{F}$.

In the multi-user setting, we are interested in running u (independent initiated) instances of a (synchronous) two-party hybrid-model protocol $\Pi^{(1)} = (\mathsf{P}_{\mathsf{A},1}, \mathsf{P}_{\mathsf{B},1}), ..., \Pi^{(u)} = (\mathsf{P}_{\mathsf{A},u}, \mathsf{P}_{\mathsf{B},u})$ accessing a functionality $\mathcal{F}$ and implementing u independent instances of a target functionality $\mathcal{G}$. We remark that while the u instances are accessing the same $\mathcal{F}$, they initiate $\mathcal{F}$ with independently chosen inputs.

We now distinguish the real-world from the ideal-world execution. Both of them are parameterized by a set $\mathsf{Corr} \subsetneq \{\mathsf{P}_{\mathsf{A},1}, \mathsf{P}_{\mathsf{B},1}, ..., \mathsf{P}_{\mathsf{A},u}, \mathsf{P}_{\mathsf{B},u}\}$ of corrupted parties controlled by the adversary $\mathcal{A}$. For each $\mathsf{id} \in \{1, ..., u\}$, the case of both $\mathsf{P}_{\mathsf{A},\mathsf{id}} \in \mathsf{Corr}$ and $\mathsf{P}_{\mathsf{B},\mathsf{id}} \in \mathsf{Corr}$ is uninteresting. Since we are in the malicious setting, we require that exactly one of $\mathsf{P}_{\mathsf{A},\mathsf{id}}$ and $\mathsf{P}_{\mathsf{B},\mathsf{id}}$ falls in Corr.

- **Real-world execution.** Initially, we fix the input(s) $X_{\overline{\mathsf{Corr}}}$ of the uncorrupted parties. Then, we run the u protocol instances $\Pi^{(1)}, ..., \Pi^{(u)}$, and the adversary (1) can choose the messages meant to be sent by the corrupted players (if any) in the protocol instances $\Pi^{(1)}, ..., \Pi^{(u)}$, (2) has access to the player's interface in $\mathcal{F}$, and (3) it has access to $\mathcal{A}$'s dedicated interface in $\mathcal{F}$, as well as to all messages sent in the u protocol instances. Finally, the adversary outputs some value z. We let $\mathsf{REAL}^{\Pi^{(1)},...,\Pi^{(u)},\mathcal{F}}_{\mathsf{Corr},\mathcal{A}}(X_{\overline{\mathsf{Corr}}}) = \big(X_{\overline{\mathsf{Corr}}}, z\big)$.
- **Ideal-world execution.** Here, we consider u instances $\mathcal{G}^{(1)}, ..., \mathcal{G}^{(u)}$, and supply the input(s) $X_{\overline{\mathsf{Corr}}}$ to their corresponding interfaces. The adversary $\mathcal{A}$ interacts with a simulator $\mathcal{S}$, which can use the interfaces of $\mathcal{G}^{(1)}, ..., \mathcal{G}^{(u)}$ for corrupted parties, as well as the adversarial interface. $\mathcal{A}$ will produce an output z, and we define $\mathsf{IDEAL}^{\mathcal{G}^{(1)},...,\mathcal{G}^{(u)}}_{\mathsf{Corr},\mathcal{A},\mathcal{S}}\big(X_{\overline{\mathsf{Corr}}}\big) = \big(X_{\overline{\mathsf{Corr}}}, z\big)$.

We then define

$$\begin{aligned}&\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi,\mathsf{Corr},u}\left(\mathcal{A},\mathcal{D},\mathcal{S},X_{\overline{\mathsf{Corr}}}\right)\\ &:= \Pr\left[\mathcal{D}\big(\mathsf{REAL}^{\Pi^{(1)},...,\Pi^{(u)},\mathcal{F}}_{\mathsf{Corr},\mathcal{A}}(X_{\overline{\mathsf{Corr}}})\big)=1\right] - \Pr\left[\mathcal{D}\big(\mathsf{IDEAL}^{\mathcal{G}^{(1)},...,\mathcal{G}^{(u)}}_{\mathsf{Corr},\mathcal{A},\mathcal{S}}\left(X_{\overline{\mathsf{Corr}}}\right)\big)=1\right].\end{aligned}$$

To establish security, we need to show that for any adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$ such that $\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi,\mathsf{Corr},u}\left(\mathcal{A},\mathcal{D},\mathcal{S},X_{\overline{\mathsf{Corr}}}\right)$ is sufficiently small.

5.2 OT extension with non-trivial multi-user security

We consider the random-OT-to-standard-OT transformation of Guo et al. [12, Fig. 3] that implements $\mathcal{F}_{\mathsf{S\text{-}OT}}(m,n)$ from $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ using a tweakable correlation robust hash function $H : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, and improve its multi-user security by introducing a random IV (which is inspired by [11]). Our improved protocol $\prod^{m,k,n}_{\mathsf{S\text{-}OT}}$ is given in Fig. 3. Its malicious security is given below.

Theorem 2 *For every adversary $\mathcal{A}$ that corrupts at most M receivers, every distinguisher $\mathcal{D}$, there exists a simulator $\mathcal{S}$ and an adversary $\mathcal{B}$ such that for every*

$$X = \big((\mathbf{m}^0_{1,1}, \mathbf{m}^1_{1,1}), \ldots, (\mathbf{m}^0_{1,m}, \mathbf{m}^1_{1,m}),$$

$$\ldots,$$
$$(\mathbf{m}^0_{u,1}, \mathbf{m}^1_{u,1}), \ldots, (\mathbf{m}^0_{u,m}, \mathbf{m}^1_{u,m})\big), \tag{43}$$

it holds

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi^{m,k,n}_{\mathrm{OT}},\mathsf{Corr},u}(\mathcal{A},\mathcal{D},\mathcal{S},X) \le \mathbf{Adv}^{\mathrm{muTCCRL}}_{H,\{0,1\}^k,\mathcal{P}_{\mathsf{free}},u,\mu}(\mathcal{B}),$$

where $\mathcal{F} = \mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$, $\mathcal{G} = \mathcal{F}_{\mathsf{S}\text{-}\mathsf{OT}}(m,n)$, *and* $\mathcal{B}$ *is* $(u\cdot m, q_{\mathcal{A}} + q_{\mathcal{D}} + u\cdot m\cdot q_H, M, 1)$*-bounded, where* $q_{\mathcal{A}}$ *and* $q_{\mathcal{D}}$ *are the numbers of ideal-primitive queries of* $\mathcal{A}$ *and* $\mathcal{D}$*'s, respectively, and* q_H *is the number of ideal-primitive queries in one evaluation of* H*.*

When H *is* $\widehat{\mathsf{MMO}}^E$*, for any threshold* μ *we further have (note that* $q_H = 1$*)*

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi^{m,k,n}_{\mathrm{OT}},\mathsf{Corr},u}(\mathcal{A},\mathcal{D},\mathcal{S},X) \le \frac{(um)^{\mu+1}}{(\mu+1)!\cdot 2^{\mu n}} + \frac{4\mu(q_{\mathcal{A}}+q_{\mathcal{D}}+um)(M+1)}{2^k} + \frac{2(\mu-1)um(M+1)}{2^k}. \tag{44}$$

<u>*Discussion*</u>. Under the condition $2um \le 2^n$, it holds $\frac{1}{2(n+1)!}\times\big(\frac{2um}{2^n}\big)^{n+1} \le \frac{um}{2^n}$. Therefore, in Eq. (44), setting the threshold $\mu = n$ yields

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi^{m,k,n}_{\mathrm{OT}},\mathsf{Corr},u}(\mathcal{A},\mathcal{D},\mathcal{S},X) \le \frac{4n(q_{\mathcal{A}}+q_{\mathcal{D}}+um)(M+1)}{2^k} + \frac{2(n-1)um(M+1)}{2^k} + \frac{um}{2^n}. \tag{45}$$

The single-user security of many state-of-the-art OT extension protocols can be tightly reduced to our single-user bound Eq. (3). For example, when H is $\widehat{\mathsf{MMO}}^E$, our protocol $\Pi^{m,k,n}_{\mathrm{OT}}$ achieves single-user security of

$$\frac{8(q_{\mathcal{A}}+q_{\mathcal{D}}+m)}{2^k} + \frac{4m}{2^k}.$$

(Note that $\mu = 1$ due to the design of $\Pi^{m,k,n}_{\mathrm{OT}}$.) By this, for u users the naïve hybrid argument implies multi-user security of

$$\frac{8u(q_{\mathcal{A}}+q_{\mathcal{D}}+m)}{2^k} + \frac{4um}{2^k}. \tag{46}$$

It is likely to have $M \ll u$ and m relatively small in practice. Therefore, the 1st terms in Eqs. (45) and (46) likely dominates, and it is likely to have

$$\frac{4n(q_{\mathcal{A}}+q_{\mathcal{D}}+um)(M+1)}{2^k} \ll \frac{8u(q_{\mathcal{A}}+q_{\mathcal{D}}+m)}{2^k}.$$

i.e., our dedicated bound Eq. (44) is better than the naïve one. In particular, in our bound $\frac{4n(q_{\mathcal{A}}+q_{\mathcal{D}}+um)(M+1)}{2^k}$ the quantities $q_{\mathcal{A}}$ and $q_{\mathcal{D}}$ (representing the offline computation power of $\mathcal{A}$ and $\mathcal{D}$) are free of the factor u.

Proof We start by describing the simulator $\mathcal{S}$. For each index $\mathsf{id} \in \{1,\ldots,u\}$, $\mathcal{S}$ distinguishes two cases as follows.

Case 1: player $\mathsf{P}_{\mathsf{A},id}$ *is corrupted.* Thus, the adversary $\mathcal{A}$ controls $\mathsf{P}_{\mathsf{A},\mathsf{id}}$ as well as the adversarial interface of $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$. In the case, the proof is fairly straightforward. Specifically, $\mathcal{S}$ emulates functionality $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ by receiving Δ and $(\mathbf{a}_1,\ldots,\mathbf{a}_m)$ from $\mathcal{A}$. Then, $\mathcal{S}$ (on behalf of $\mathsf{P}_{\mathsf{B},\mathsf{id}}$) receives $(IV,\mathbf{c}_1^0,\mathbf{c}_1^1,...,\mathbf{c}_m^0,\mathbf{c}_m^0)$ from $\mathcal{A}$, and extracts the messages as follows:

$$\begin{aligned}\mathbf{m}_i^0 &:= H(\mathbf{a}_i, IV\oplus[i]_n)\oplus\mathbf{c}_i^0,\\ \mathbf{m}_i^1 &:= H(\mathbf{a}_i\oplus\Delta, IV\oplus[i]_n)\oplus\mathbf{c}_i^1\end{aligned} \tag{47}$$

for each $i\in\{1,...,m\}$. Finally, $\mathcal{S}$ sends $\{(\mathbf{m}_i^0,\mathbf{m}_i^1)\}_{i=1}^m$ to the functionality $\mathcal{F}_{\mathsf{S}\text{-}\mathsf{OT}}(m,n)$ as the OT messages of sender $\mathsf{P}_{\mathsf{A},\mathsf{id}}$.

Case 2: player $\mathsf{P}_{\mathsf{B},id}$ *is corrupted.* Thus, the adversary $\mathcal{A}$ controls $\mathsf{P}_{\mathsf{B},\mathsf{id}}$ as well as the adversarial interface of $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$, and $\mathcal{S}$ is responsible to simulate the $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ functionality. It proceeds as follows:

- The simulator $\mathcal{S}$ initially chooses $\Delta_{\mathsf{id}}\xleftarrow{\$}\{0,1\}^k$ and $IV_{\mathsf{id}}\xleftarrow{\$}\{0,1,...,2^n-1\}$, and takes an input $P_{\mathsf{id}}:\{0,1\}^k\to\{0,1\}$ at $\mathcal{A}$'s interface for $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$, and returns $P_{\mathsf{id}}(\Delta_{\mathsf{id}})$ to $\mathcal{A}$ at the same interface. Further, if $P_{\mathsf{id}}(\Delta_{\mathsf{id}})=0$, $\mathcal{S}$ stops accepting any further messages from $\mathsf{P}_{\mathsf{A},\mathsf{id}}$ or $\mathsf{P}_{\mathsf{B},\mathsf{id}}$. (Thus, in the following, we assume $P_{\mathsf{id}}(\Delta_{\mathsf{id}})=1$.)
- Upon receiving $(x_{\mathsf{id},1},\ldots,x_{\mathsf{id},m})$ at $\mathsf{P}_{\mathsf{B},\mathsf{id}}$'s interface for $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$, and $\mathbf{z}_{\mathsf{id},1},\ldots,\mathbf{z}_{\mathsf{id},m}$ at $\mathcal{A}$'s interface, the simulator $\mathcal{S}$ inputs $(x_{\mathsf{id},1},\ldots,x_{\mathsf{id},m})$ to $\mathsf{P}_{\mathsf{B},\mathsf{id}}$'s interface of $\mathcal{F}_{\mathsf{S}\text{-}\mathsf{OT}}(m,k)$, and obtains $\mathbf{m}_{\mathsf{id},1}^{x_1},\ldots,\mathbf{m}_{\mathsf{id},m}^{x_m}$ back.
- The simulator $\mathcal{S}$ outputs $(\mathbf{z}_{\mathsf{id},1},\ldots,\mathbf{z}_{\mathsf{id},m})$ at $\mathsf{P}_{\mathsf{B},\mathsf{id}}$'s interface of $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$.
- Finally, $\mathcal{S}$ sets

$$\mathbf{c}_{\mathsf{id},i}^{x_i}\leftarrow H\left(\mathbf{z}_{\mathsf{id},i},IV_{\mathsf{id}}\oplus[i]_n\right)\oplus\mathbf{m}_{\mathsf{id},i}^{x_{\mathsf{id},i}},\quad \mathbf{c}_{\mathsf{id},i}^{1-x_{\mathsf{id},i}}\xleftarrow{\$}\{0,1\}^n.$$

  for all $i\in\{1,...,m\}$. It then outputs $IV_{\mathsf{id}},\mathbf{c}_{\mathsf{id},1}^0,\mathbf{c}_{\mathsf{id},1}^1,\ldots,\mathbf{c}_{\mathsf{id},m}^0,\mathbf{c}_{\mathsf{id},m}^1$ as the protocol message sent to $\mathsf{P}_{\mathsf{B},\mathsf{id}}$.

Reduction to muTCCRL *security.* Now, we proceed to define the adversary $\mathcal{B}$ against muTCCRL security of H. In our setting, $\mathcal{B}$ has access to a pair of oracles $(\mathcal{O},\mathcal{L}_{\boldsymbol{\Delta}})$ (for $\boldsymbol{\Delta}=(\Delta_1,...,\Delta_u)\xleftarrow{\$}(\{0,1\}^k)^u$), where $\mathcal{O}$ implements either $\mathcal{O}_{\boldsymbol{\Delta}}^{\mathrm{muTCCRL}}$ or f. Due to the presence of the key leaking oracle, the construction of $\mathcal{B}$ is simpler than previous works [12,7]. In detail, for each $\mathsf{id}\in\{1,...,u\}$, $\mathcal{B}$ simulates the above ideal world execution as follows:

1. If player $\mathsf{P}_{\mathsf{A},\mathsf{id}}$ is corrupted then $\mathcal{B}$ simulates the protocol execution by extracting the OT messages as described above. Else, i.e., player $\mathsf{P}_{\mathsf{B},\mathsf{id}}$ is corrupted, $\mathcal{B}$ proceeds to step 2.
2. $\mathcal{B}$ initially takes an input $P_{\mathsf{id}}:\{0,1\}^k\to\{0,1\}$ at $\mathcal{A}$'s interface for functionality $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$. It queries $\mathcal{L}_{\boldsymbol{\Delta}}(\mathsf{id},P_{\mathsf{id}})\to r$, returns 1 to $\mathcal{A}$ if $r=1$, and stops accepting any further messages if $\mathcal{L}_{\boldsymbol{\Delta}}(\mathsf{id},P_{\mathsf{id}})$ aborts.
3. Upon receiving $(x_{\mathsf{id},1},\ldots,x_{\mathsf{id},m})$ at $\mathsf{P}_{\mathsf{B},\mathsf{id}}$'s interface for $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$, and $\mathbf{z}_{\mathsf{id},1},\ldots,\mathbf{z}_{\mathsf{id},m}$ at $\mathcal{A}$'s interface, $\mathcal{B}$ inputs $(x_{\mathsf{id},1},\ldots,x_{\mathsf{id},m})$ to $\mathsf{P}_{\mathsf{B},\mathsf{id}}$'s interface of $\mathcal{F}_{\mathsf{S}\text{-}\mathsf{OT}}(m,k)$, and obtains $\mathbf{m}_{\mathsf{id},1}^{x_{\mathsf{id},1}},\ldots,\mathbf{m}_{\mathsf{id},m}^{x_{\mathsf{id},m}}$ back.

4. $\mathcal{B}$ outputs $(\mathbf{z}_{\mathsf{id},1}, \ldots, \mathbf{z}_{\mathsf{id},m})$ at $\mathsf{P}_{\mathsf{B},\mathsf{id}}$'s interface of $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$.
5. Finally, $\mathcal{S}$ sets

$$\mathbf{c}_{\mathsf{id},i}^{x_{\mathsf{id},i}} \leftarrow H\left(\mathbf{z}_{\mathsf{id},i}, IV_{\mathsf{id}} \oplus [i]_n\right) \oplus \mathbf{m}_{\mathsf{id},i}^{x_{\mathsf{id},i}},$$
$$\mathbf{c}_{\mathsf{id},i}^{1-x_{\mathsf{id},i}} \leftarrow \mathcal{O}\left(\mathbf{z}_{\mathsf{id},i}, IV_{\mathsf{id}} \oplus [i]_n\right) \oplus \mathbf{m}_{\mathsf{id},i}^{x_{\mathsf{id},i}}.$$

for all $i \in \{1, ..., m\}$. It then outputs $IV_{\mathsf{id}}, \mathbf{c}_{\mathsf{id},1}^0, \mathbf{c}_{\mathsf{id},1}^1, \ldots, \mathbf{c}_{\mathsf{id},m}^0, \mathbf{c}_{\mathsf{id},m}^1$ as the protocol message sent to $\mathsf{P}_{\mathsf{B},\mathsf{id}}$.

$\mathcal{B}$ finally outputs $\mathcal{D}$'s decision bit. It is easy to see: when $\mathcal{O}$ implements $\mathcal{O}_{\mathbf{\Delta}}^{\text{muTCCRL}}$, $\mathcal{B}$ simulates the real world execution; when $\mathcal{O}$ implements f, $\mathcal{B}$ simulates the ideal world execution.

Moreover, it can be seen that $\mathcal{B}$ is $(u \cdot m, q_{\mathcal{A}} + q_{\mathcal{D}} + u \cdot m \cdot q_H, M, 1)$-bounded:

(i) It makes at most $u \cdot m$ queries to $\mathcal{O}_{\mathbf{R}}^{\text{muTCCRL}}/f$ and at most $q_{\mathcal{A}} + q_{\mathcal{D}} + u \cdot m \cdot q_H$ queries to E;
(ii) Since $\mathcal{A}$ corrupts at most M receivers, $\mathcal{B}$ makes key leaking queries to at most M users as well. Moreover, for each of them $\mathcal{B}$ make only 1 leaking query, meaning that $q_{L,max} = 1$.

Therefore,

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi_{\text{OT}}^{m,k,n},\mathsf{Corr},u}(\mathcal{A},\mathcal{D},\mathcal{S},X) \leq \mathbf{Adv}^{\text{muTCCRL}}_{H,\{0,1\}^k,\mathcal{P}_{\mathsf{free}},u,\mu}(\mathcal{B}). \tag{48}$$

When H is $\widehat{\mathsf{MMO}}^E$, for any threshold μ we have

$$\Pr\left[\mu^* > \mu\right] \leq \frac{(um)^{\mu+1}}{(\mu+1)! \cdot 2^{\mu n}}$$

by Lemma 1. Therefore,

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})\text{-mu-mpc}}_{\Pi_{\text{OT}}^{m,k,n},\mathsf{Corr},u}(\mathcal{A},\mathcal{D},\mathcal{S},X) \leq \frac{(um)^{\mu+1}}{(\mu+1)! \cdot 2^{\mu n}} + \frac{4\mu(q_{\mathcal{A}} + q_{\mathcal{D}} + um)(M+1)}{2^k} + \frac{2(\mu-1)um(M+1)}{2^k}$$

by Theorem 1. This completes the proof. □

6 Conclusion

Many OT extension schemes are built upon tweakable circular correlation robust (TCCR) hash functions, and allow the adversary to extract key information via a key leaking query. With this in mind, we incorporate key leaking query mechanism into the security definition of [11] and propose a notion named *multi-user tweakable circular correlation robustness with key leakages*. We then exhibit both security proofs and matching attacks w.r.t. the blockcipher-based TCCR hash of [11]. This enables constructing an OT extension protocol with non-trivial multi-user security. Our results may provide useful building blocks to the NIST standardization process of multi-party threshold cryptographic schemes [20].

Acknowledgments

We thank the anonymous reviewers in advance.

Data Deposition Information: No datasets have been used

Conflict of Interest: The authors have no conflicts of interest to declare that are relevant to the content of this article.

Funding: Chun Guo was supported by the National Key Research and Development Program of China (grant 2022YFA1004900), the National Natural Science Foundation of China (grant 62372274), and the Taishan Scholars Program (for Young Scientists) of Shandong. Xiao Wang was supported by NSF awards 2016240 and 2236819. Kang Yang was supported by the National Natural Science Foundation of China (Grant Nos. 62102037, 61932019). Yu Yu was supported by the National Natural Science Foundation of China (grants 62125204 and 92270201), and the Major Program of Guangdong Basic and Applied Research (grant 2019B030302008), and was also supported by the XPLORER PRIZE.

A Proof of Lemma 1

Consider the ith sequence of balls. As per our assumption, these q_i balls are thrown into the bins of indices $\gamma(1)\oplus IV_i, \gamma(2)\oplus IV_i, ..., \gamma(q_i)\oplus IV_i$ with $IV_i \xleftarrow{\$} \{0,1\}^n$. Since γ is bijective, the q_i indices are pairwise distinct. Therefore, for a certain bin, the probability that it gets a ball after the ith experiment is $q_i/2^n$.

Now, consider some μ sequences of balls, i.e., the i_1th, ..., i_μth, and consider the event that there is a $a \in \{0,1\}^n$ such that every one of those sequences hits the ath bin. By the above, the probability is

$$2^n \times \frac{q_{i_1}}{2^n} \times \cdots \times \frac{q_{i_\mu}}{2^n} = \frac{q_{i_1} \times \cdots \times q_{i_\mu}}{2^{n\cdot(\mu-1)}}.$$

Since μ^* is the maximum number of balls in any of the 2^n bins, we have

$$\Pr[\mu^* \geq \mu] \quad \leq \sum_{0<i_1<i_2<\cdots<i_\mu\leq u} \frac{q_{i_1} \times \cdots \times q_{i_\mu}}{2^{n\cdot(\mu-1)}}$$

Observing that

$$\begin{aligned}(q_1 + q_2 + \cdots + q_u)^\mu &\geq \sum_{i_1\neq i_2\neq\cdots\neq i_\mu} q_{i_1} \times \cdots \times q_{i_\mu} \\ &= \mu! \cdot \sum_{i_1<i_2<\cdots<i_\mu} q_{i_1} \times \cdots \times q_{i_\mu},\end{aligned}$$

we have

$$\sum_{i_1<i_2<\cdots<i_\mu} q_{i_1} \times \cdots \times q_{i_\mu} \leq \frac{(q_1 + q_2 + \cdots + q_u)^\mu}{\mu!}.$$

Therefore,

$$\Pr[\mu^* > \mu] = \Pr[\mu^* \geq \mu + 1] \quad \leq \frac{1}{2^{n\cdot\mu}} \times \frac{(q_1 + \cdots + q_u)^{\mu+1}}{(\mu+1)!} = \frac{q^{\mu+1}}{(\mu+1)! \cdot 2^{n\cdot\mu}}.$$

This complete the proof.

B The Matching Multi-user Attack Suggested by the Anonymous Reviewer

The previous version of this paper claimed a multi-user security bound of

$$O\Big(\frac{\mu q_E q_L}{|\mathcal{R}|} + \frac{\mu q_C q_L}{|\mathcal{R}|}\Big). \tag{49}$$

When the previous version was first submitted to Designs, Codes and Cryptography, the anonymous reviewer pointed out an attack with success probability

$$\Theta\Big(\frac{q_E M q_{L,max}}{|\mathcal{R}|}\Big),$$

and this invalidates the previous claim of Eq. (49). On the other hand, this does match our fixed bound of Eq. (2), establishing the tightness of Theorem 1.

We now describe this attack. Following Sect. 4.4, we assume $\mathcal{R} = \{0,1\}^n$ for simplicity. We will use two types of predicates. First, fix $\mathcal{R}^\circ \subset \mathcal{R}$ with $|\mathcal{R}^\circ| = 2^n/u$. Define

$$P^\circ(R) = 1 \text{ if and only if } R \in \mathcal{R}^\circ.$$

We further fix some integer ρ and partition $\mathcal{R}^\circ$ into ρ subsets $\mathcal{R}^\circ = \mathcal{R}_1 \sqcup ... \sqcup \mathcal{R}_\rho$, such that $|\mathcal{R}_1| = ... = |\mathcal{R}_\rho| = \frac{2^n}{\rho u}$. Based on this, we define a series of predicates: for any $j \in \{1, ..., \rho\}$,

$$P_j(R) = 1 \text{ if and only if } R \notin \mathcal{R}_j.$$

With the above preparations, the attack proceeds as follows.

1. For $\mathsf{id} \in \{1, ..., u\}$, query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$, till $R_{\mathsf{id}} \in \mathcal{R}^\circ$, i.e., $\mathcal{L}_{\mathbf{R}}(\mathsf{id}, P)$ does not abort. Let id° be the first index such that $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^\circ, P)$ does not abort.
2. Choose $(w, i, 0)$ in arbitrary and query $\mathcal{O}_{\mathbf{R}}^{\mathrm{muTCCRL}}(\mathsf{id}^\circ, w, i, 0) \to y = \widehat{\mathsf{MMO}}^E(w \oplus R_{\mathsf{id}^\circ}, i)$ to obtain y.
3. For $j = 1, ..., \rho$, query $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^\circ, P_j)$ to see if $R_{\mathsf{id}^\circ} \in \mathcal{R}_j$, till $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^\circ, \cdot)$ aborts. Note that abortion always occurs since $R_{\mathsf{id}^\circ} \in \mathcal{R}^\circ$ and since $\mathcal{R}^\circ = \mathcal{R}_1 \sqcup ... \sqcup \mathcal{R}_\rho$.
4. When $\mathcal{L}_{\mathbf{R}}(\mathsf{id}^\circ, \cdot)$ aborts, we know $R_{\mathsf{id}^\circ} \in \mathcal{R}_j$ by the definitions. Let $\mathcal{U} := w \oplus \mathcal{R}_j$. Query $E(i, u) \to v$ for all $u \in \mathcal{U}$ ($\frac{2^n}{\rho u}$ queries in total). Let $E(i, u^*) \to v^* = y$, then we can recover R_{id° via $R_{\mathsf{id}^\circ} = w \oplus u^*$.

This attack has $q_C = 1$ (and thus $\mu = 1$), $M = u$, $q_{L,max} = \rho$ and $q_E = \frac{2^n}{\rho u}$, and succeeds with probability roughly 1. By this, our proven bound $O\big(\frac{q_E M q_{L,max}}{|\mathcal{R}|}\big)$ of Eq. (2) is tight. However, it has $q_L = u + \rho$ and violates our previous claim $O\big(\frac{\mu q_E q_L}{|\mathcal{R}|} + \frac{\mu q_C q_L}{|\mathcal{R}|}\big)$ of Eq. (49).

References

1. Bellare, M., Hoang, V.T., Keelveedhi, S., Rogaway, P.: Efficient garbling from a fixed-key blockcipher. In: 2013 IEEE Symposium on Security and Privacy. pp. 478–492. IEEE Computer Society Press (May 2013)

2. Bellare, M., Hoang, V.T., Rogaway, P.: Foundations of garbled circuits. In: Yu, T., Danezis, G., Gligor, V.D. (eds.) ACM CCS 12. pp. 784–796. ACM Press (Oct 2012)
3. Boyle, E., Couteau, G., Gilboa, N., Ishai, Y., Kohl, L., Rindal, P., Scholl, P.: Efficient two-round OT extension and silent non-interactive secure computation. In: ACM CCS 19. pp. 291–308. ACM Press (2019)
4. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.P.: Minimizing the two-round Even-Mansour cipher. Journal of Cryptology 31(4), 1064–1119 (Oct 2018)
5. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer (May 2014)
6. Chen, W., Popa, R.A.: Metal: A metadata-hiding file-sharing system. In: NDSS 2020. The Internet Society (2020)
7. Chen, Y.L., Tessaro, S.: Better security-efficiency trade-offs in permutation-based two-party computation. pp. 275–304. LNCS, Springer (2021)
8. Choi, S.G., Katz, J., Kumaresan, R., Zhou, H.S.: On the security of the "free-XOR" technique. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 39–53. Springer (Mar 2012)
9. Diamond, B.E.: On the security of KOS. Cryptology ePrint Archive, Report 2022/1371 (2022), `https://eprint.iacr.org/2022/1371`
10. Dittmer, S., Ishai, Y., Lu, S., Ostrovsky, R.: Authenticated garbling from simple correlations. pp. 57–87. LNCS, Springer (2022)
11. Guo, C., Katz, J., Wang, X., Weng, C., Yu, Y.: Better concrete security for half-gates garbling (in the multi-instance setting). In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2020(2). pp. 793–822. LNCS, Springer (Aug 2020)
12. Guo, C., Katz, J., Wang, X., Yu, Y.: Efficient and secure multiparty computation from fixed-key block ciphers. In: 2020 IEEE Symposium on Security and Privacy. pp. 825–841. IEEE Computer Society Press (2020)
13. Guo, X., Yang, K., Wang, X., Zhang, W., Xie, X., Zhang, J., Liu, Z.: Half-tree: Halving the cost of tree expansion in COT and DPF. pp. 330–362. LNCS, Springer (2023)
14. Hazay, C., Scholl, P., Soria-Vazquez, E.: Low cost constant round MPC combining BMR and oblivious transfer. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017(1). LNCS, vol. 10624, pp. 598–628. Springer (Dec 2017)
15. Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016(1). LNCS, vol. 9814, pp. 3–32. Springer (Aug 2016)
16. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 145–161. Springer (Aug 2003)
17. Katz, J., Ranellucci, S., Rosulek, M., Wang, X.: Optimizing authenticated garbling for faster secure two-party computation. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018(3). LNCS, vol. 10993, pp. 365–391. Springer (Aug 2018)
18. Keller, M., Orsini, E., Scholl, P.: Actively secure OT extension with optimal overhead. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015(1). LNCS, vol. 9215, pp. 724–741. Springer (Aug 2015)
19. Kolesnikov, V., Schneider, T.: Improved garbled circuit: Free XOR gates and applications. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008(2). LNCS, vol. 5126, pp. 486–498. Springer (Jul 2008)
20. NIST: NIST First Call for Multi-Party Threshold Schemes. National Institute of Standards and Technology (2023), `https://csrc.nist.gov/pubs/ir/8214/c/ipd`.
21. Orrù, M., Orsini, E., Scholl, P.: Actively secure 1-out-of-N OT extension with application to private set intersection. In: Handschuh, H. (ed.) CT-RSA 2017. LNCS, vol. 10159, pp. 381–396. Springer (Feb 2017)
22. Patarin, J.: The "coefficients H" technique (invited talk). In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer (Aug 2009)
23. Roy, L.: SoftSpokenOT: Communication–computation tradeoffs in OT extension. Cryptology ePrint Archive, Report 2022/192 (2022), `https://eprint.iacr.org/2022/192`
24. Roy, L.: SoftSpokenOT: Quieter OT extension from small-field silent VOLE in the minicrypt model. pp. 657–687. LNCS, Springer (2022)

25. Scholl, P.: Extending oblivious transfer with low communication via key-homomorphic PRFs. In: Abdalla, M., Dahab, R. (eds.) PKC 2018(1). LNCS, vol. 10769, pp. 554–583. Springer (Mar 2018)
26. Wang, X., Ranellucci, S., Katz, J.: Authenticated garbling and efficient maliciously secure two-party computation. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 17. pp. 21–37. ACM Press (Oct / Nov 2017)
27. Wang, X., Ranellucci, S., Katz, J.: Global-scale secure multiparty computation. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 17. pp. 39–56. ACM Press (Oct / Nov 2017)
28. Weng, C., Yang, K., Katz, J., Wang, X.: Wolverine: Fast, scalable, and communication-efficient zero-knowledge proofs for boolean and arithmetic circuits. pp. 1074–1091. IEEE Computer Society Press (2021)
29. Yang, K., Wang, X., Zhang, J.: More efficient MPC from improved triple generation and authenticated garbling. In: ACM CCS 20. pp. 1627–1646. ACM Press (2020)
30. Yang, K., Weng, C., Lan, X., Zhang, J., Wang, X.: Ferret: Fast extension for correlated OT with small communication. In: ACM CCS 20. pp. 1607–1626. ACM Press (2020)
31. Yao, A.C.C.: How to generate and exchange secrets (extended abstract). In: 27th FOCS. pp. 162–167. IEEE Computer Society Press (Oct 1986)
32. Zahur, S., Rosulek, M., Evans, D.: Two halves make a whole - reducing data transfer in garbled circuits using half gates. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015(2). LNCS, vol. 9057, pp. 220–250. Springer (Apr 2015)
33. Zhu, R., Cassel, D., Sabry, A., Huang, Y.: NANOPI: Extreme-scale actively-secure multi-party computation. In: ACM CCS 18. pp. 862–879. ACM Press (2018)