Bounded Collusion-Resistant Registered Functional Encryption for Circuits

Yijian Zhang^{1,3}, Jie Chen^{1,2,⊠}, Debiao He⁴, and Yuqing Zhang^{5,6}

¹ Shanghai Key Laboratory of Trustworthy Computing, School of Software Engineering, East China Normal University,

Shanghai, China.

s080001@e.ntu.edu.sg

² Institute for Math & AI, Wuhan University, Wuhan, China.

³ Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong NSW, Australia.

⁴ School of Cyber Science and Engineering, Wuhan University, Wuhan, China.

⁵ National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China.
⁶ School of Cyberspace Security, Hainan University, China.

Abstract. As an emerging primitive, *Registered Functional Encryption* (RFE) eliminates the key-escrow issue that threatens numerous works for functional encryption, by replacing the trusted authority with a transparent key curator and allowing each user to sample their decryption keys locally. In this work, we present a new black-box approach to construct RFE for all polynomial-sized circuits. It considers adaptive simulation-based security in the bounded collusion model (Gorbunov et al. - CRYPTO'12), where the security can be ensured only if there are no more than $Q \ge 1$ corrupted users and Q is fixed at the setup phase. Unlike earlier works, we do not employ unpractical *Indistinguishability Obfuscation (iO)*. Conversely, it can be extended to support unbounded users, which is previously only known from *iO*.

Technically, our general compiler exploits garbled circuits and a novel variant of slotted *Registered Broadcast Encryption* (RBE), namely global slotted RBE. This primitive is similar to slotted RBE, but needs *optimally compact* public parameters and ciphertext, so as to satisfy the efficiency requirement of the resulting RFE. Then we present two concrete global slotted RBE from pairings and lattices, respectively. With proposed compiler, we hence obtain two bounded collusion-resistant RFE schemes. Here, the first scheme relies on *k*-Lin assumption, while the second one supports unbounded users under LWE and evasive LWE assumptions.

1 Introduction

Registered Functional Encryption (RFE) [FFM⁺23,DP23] has emerged as a rising public-key cryptographic primitive recently. Unlike standard *Functional Encryption* (FE) [BSW11], RFE is particularly initiated to eliminate key-escrow problem that a lot of FE schemes have suffered for many years. In RFE, a common random string crs is initialized by the key curator who broadcasts crs to all users later. Then this curator is just responsible for providing registration service for each user, without holding any secret. With crs, a newly joined user can produce a pair of public key pk and secret key sk locally, then he submits a specified function *f* along with pk to the curator for registration. After receiving (*f*, pk), the curator updates current master public key mpk and helper secret key hsk for the new user. For encryption, the data provider uses mpk to generate a ciphertext ct associated with private data *x*, and the user can perform decryption algorithm over ct with (sk, hsk) to learn *f*(*x*) and nothing else. During this process, it is required that (i) all registration procedures are deterministic and auditable, and (ii) mpk and hsk must be compact (i.e., polylogarithmic in the total number of user) and updates for mpk and hsk should be efficient.

Previously, lots of significant progress have been made on constructing RFE for various kinds of limited functionality. Focusing on identity-based policy, Garg et al. [GHMR18] put forth the first registration-based encryption construction, which inspired a line of subsequent works enhancing the security [GV20,DKL⁺23] and efficiency [GKMR23] of this primitive. In addition, a more generic subclass of RFE, i.e., registered attribute-based encryption (RABE), was built relying on general assumptions over bilinear groups [HLWW23,ZZGQ23], and then it was also achieved from lattice-based assumptions [FWW23].

In light of these notable achievements, it is natural to ask how to construct RFE for more powerful and generic functionality, i.e., polynomial-sized circuits. Unfortunately, all existing constructions [FFM⁺23,DP23] are built upon the existence of *Indistinguishability Obfuscation (iO)*. An exception is Branco et al.'s work [BLM⁺24], which proposed a generic framework based on RFE for linear function (also called linear RFE in short), but we observe the security of their result is pretty weak, only achieving selective indistinguishability-based (IND) security against adversary with single corrupt key. In their definition, the adversary is forced to submit the challenge message and specify the corrupted user set in advance, and IND security is actually inadequate for some cases as noted in [BSW11]. For FE, stronger simulation-based (SIM) security is more desirable and up to now has facilitated a series of beneficial applications [AW17,KW17,AFNV19,JLLW23]. Thus, Zhu et al. [ZLZ⁺24] formalized the definition of SIM secure RFE and presented concrete realizations, whereas they also considered the selective setting and only focused on linear/quadratic function. Given all these, an open question that arises is

Can we construct a registered functional encryption for all polynomial-sized circuits that achieves SIM security without assistance of iO?

Bounded Collusion Model. In this work, we will focus on bounded collusion-resistant RFE for circuits from weak assumptions, and consider stronger adaptive SIM security. Compared to plain RFE, bounded collusion-resistant RFE additionally requires that a prior-bound Q^1 of the number of corrupted users should be declared at the setup phase. The adversary cannot extract any useful information about encrypted data x (except for $C_1(x), \ldots, C_Q(x)$) even when he is able to adaptively query secret keys with respect to circuits C_1, \ldots, C_Q .

Bounded collusion-resistant FE has been studied extensively, and a number of works gained satisfactory results from general cryptographic tools, including public-key encryption (PKE) [SS10], multi-party computation (MPC) [GVW12,AV19] and FE for linear/quadratic function [ALS16,AR17]. This model is firstly proposed to construct FE for circuits without *iO*, since several works [AJ15,BV15] have shown that fully collusion-resistant FE for circuits exactly implies *iO*, making itself difficult to be deduced from weak assumptions. This rule may also work on RFE, imagine that RFE can trivially simulate FE if the key curator acts as central authority by preparing sufficient secret keys for all possible functions and then distributing each to matched users.

1.1 Results

As a matter of fact, the notion of RFE should be naturally "bounded" since the user number L is fixed during initialization. A crucial point is the size of master public key and helper secret key, which should be poly(C, log L) (here, C denotes the size of circuit), namely *compactness*. However, if we think of that in bounded collusion model, the overhead of all parameters could be poly(L). Such fact contradicts to compactness, so we decide to slightly relax it by considering a lower collusion bound $Q \ll L$ and allowing master public key and helper key of size poly(C, Q, $\log L$).

In this work, we manage to answer above question and conclude our contributions as follows:

¹ Generally speaking, the collusion bound Q is implied by the security parameter 1^{λ} . Since [GVW12] defined bounded collusionresistant FE, it has been widely accepted that Q is an integer much less than the total number of system users, which means not many users collude with adversary. In this work, our bounded collusion-resistant RFE also inherits this assumption as default.

- We propose a new black-box approach to construct bounded collusion-resilient RFE for all polynomial-sized circuits. It mainly contains two ingredients, i.e., garbled circuits and global slotted registered broadcast encryption, where the latter can be regarded as a compact variant of slotted registered broadcast encryption. Furthermore, our approach would also be useful when constructing RFE with unbounded users property, i.e., all parameters of size not scaling with *L*. Prior to this work, only *iO*-based works [FFM⁺23,DP23] are known to realize unbounded users.
- With above general compiler, we obtain two bounded collusion-resistant RFE constructions, both of which are adaptively SIM secure (without malicious case). The first one is provably secure under *k*-Lin assumption in the standard model. Another one is secure in the random oracle model, relying on LWE and evasive LWE assumptions [Wee22]. The second RFE could be extended to support unbounded users. Compared to selective security, adaptive security does not require the adversary commit any challenge information, as well as the queried input to oracles.

Reference	Security	Assumption	Unbounded	Full
[FFM ⁺ 23,DP23]	AD-IND	SSB + <i>iO</i>	\checkmark	\checkmark
[BLM ⁺ 24]	SEL-IND	<i>q</i> -type DDH	×	×
Ours	AD-SIM	<i>k</i> -Lin	×	×
	AD-SIM	LWE + evasive LWE + RO	\checkmark	×

Table 1: Comparison among existing RFE for circuits. In the column of "Security", "AD" and "SEL" denote adaptive and selective security, respectively. In the column of "Assumption", "SSB" represents somewhere statistically binding hash functions, and "RO" represents random oracle. The column "Unbounded" and "Full" denote unbounded users and full collusion-resistance.

As shown in Table 1, it is clear that our technique greatly differs from current works. Instead of unpractical *iO*, our results are based on more general assumptions, and achieve adaptive SIM security.

Prior to this work, adaptively secure RFE for circuits can also be gained from a generic framework introduced by Branco et al. [BLM⁺24]. Nevertheless, following this line, it would at least require a linear RFE with same security level. As we mentioned before, Zhu et al. [ZLZ⁺24] provided several schemes with SIM security, whereas they considered weaker selective settings. On the other hand, if post-quantum security or unbounded users are additionally required, linear RFE with comparable features ought to be ready. However, all existing linear RFE rely on pairing-based assumptions and only support a finite number of users.

1.2 Technique Overview

As introduced in [HLWW23,FFM⁺23], RFE can be generically derived from slotted RFE via "power-of-two" transformation. In slotted RFE, the key curator is replaced by a stateless aggregator who aggregates all public keys and functions to generates mpk and hsk's at once. In a similar sense, bounded collusion RFE can be gained from bounded collusion slotted RFE using the same method.

We adopt the notion of *Q*-bound *L*-slot RFE, i.e., slotted RFE supporting *L* users and against collusion attack from *Q* users. In *Q*-bound *L*-slot RFE for circuits, after collecting all $\{(pk_i, C_i)\}_{i \in [L]}$, the aggregator would publish master public key mpk and helper secret keys $\{hsk_j\}_{j \in [L]}$. Assume the adversary holds the set of secret keys $sk_{c_1}, \ldots, sk_{c_Q}$ (where $c_1, \ldots, c_Q \in [L]$), SIM security requires that it cannot distinguish the challenge ciphertext ct* that is either

normally generated from message x^* , or simulated using (mpk, {hsk_j}_{j\in[L]}, {sk_{c_j}}_{j\in[Q]}, {C_{c_j}(x^*)}_{j\in[Q]}). If we additionally consider malicious case, ct^{*} should be simulated without {sk_{c_j}}_{j\in[Q]}. Here, we ignore this stringent case. For efficiency, we require mpk and hsk of size poly(*C*, *Q*, log *L*), where *C* denotes the circuit size.

Roadmap. Our technical line somewhat deviates from current RFE for limited functionality where they always start from 1-slot case and then generalize to *L*-slot. We will follow the roadmap:

1-bound 1-slot RFE $\xrightarrow{\text{Step 1}}$ 1-bound *L*-slot RFE $\xrightarrow{\text{Step 2}}$ *Q*-bound *L*-slot RFE

Start Point: 1-Bound 1-Slot RFE. First, we propose a new and straightforward construction for 1-bound 1-slot RFE supporting all polynomial circuits. Initially, Sahai et al. [SS10] built the first 1-bound FE for circuits from standard assumptions, which was later evolved into *Q*-bound FE by Gorbunov et al. [GVW12]. Here, we also start from [SS10], but stand by a new perspective. Our first observation is: the worry-free encryption in [SS10] will yield a 1-bound 1-slot RFE after slight adaptions. An overview is depicted as below.

In 1-bound 1-slot RFE, only single user is going to register his circuit C. Suppose C can be translated into a bit string of length *n*, given public key encryption scheme PKE = (Setup, Enc, Dec) and garbled circuit algorithms (Garble, Eval, Garble) [Yao86,BHR12], the aggregator initially samples a sequence of public keys $\{\widehat{pk}_w\}_{w\in[n]}$ by running algorithm PKE.Setup *n* times. Then it sets crs = $(\{\widehat{pk}_w\}_{w\in[n]})$. To register circuit C, the user samples public key pairs $\{(pk_w, sk_w)\}_{w\in[n]}$. He keeps sk = $(\{sk_w\}_{w\in[n]})$ as decryption key and sends (C, $\{pk_w\}_{w\in[n]})$ to aggregator. Thereafter, the aggregator would produce (mpk, hsk) in the following form:

$$mpk = \left(\frac{\overline{pk}_{1,0} \cdots \overline{pk}_{n,0}}{\overline{pk}_{1,1} \cdots \overline{pk}_{n,1}}\right) \text{ and } hsk = \bot,$$

where for each $w \in [n]$ and $b \in \{0, 1\}$, set $\overline{\mathsf{pk}}_{w,b} = \mathsf{pk}_w$ when $\mathsf{C}[w] = b$; otherwise, set $\overline{\mathsf{pk}}_{w,b} = \widehat{\mathsf{pk}}_w$.

Next, to encrypt data x, let $U(\cdot, \cdot)$ be the universal circuit such that U(C, x) = C(x) for any circuit C and data x. Then run $(\tilde{U}, \{lab_{w,b}\}_{w \in [n], b \in \{0,1\}}) \leftarrow Garble(1^{\lambda}, U[x])$ where U[x] is a universal circuit with x hard-wired. With mpk, the ciphertext is defined as:

$$ct = \left(\tilde{U}, \left(\begin{array}{c} \mathsf{PKE}.\mathsf{Enc}(\overline{\mathsf{pk}}_{1,0},\mathsf{lab}_{1,0}) \cdots \mathsf{PKE}.\mathsf{Enc}(\overline{\mathsf{pk}}_{n,0},\mathsf{lab}_{n,0}) \\ \mathsf{PKE}.\mathsf{Enc}(\overline{\mathsf{pk}}_{1,1},\mathsf{lab}_{1,1}) \cdots \mathsf{PKE}.\mathsf{Enc}(\overline{\mathsf{pk}}_{n,1},\mathsf{lab}_{n,1}) \end{array} \right) \right).$$

For decryption, since $\overline{\mathsf{pk}}_{w,b} = \mathsf{pk}_w$ when $\mathsf{C}[w] = b$, the user can recover labels $\{\mathsf{lab}_{w,\mathsf{C}[w]}\}_{w\in[n]}$ by performing algorithm PKE.Dec *n* times. Finally, he obtains $\mathsf{C}(x) \leftarrow \mathsf{Eval}(\tilde{\mathsf{U}}, \{\mathsf{lab}_{w,\mathsf{C}[w]}\}_{w\in[n]})$. As for security, our analysis is listed as follows:

- In corrupt case, the registered user has colluded with adversary. Then adversary obtains labels $\{lab_{w,C[w]}\}_{w\in[n]}$, whereas he is unable to acquire other labels which are encrypted by public keys issued from aggregator. Thus, following the security of garbled circuits, the adversary cannot learn any information about *x* except for C(x);
- In honest case, the adversary has no idea about sk, so he cannot obtain any label according to the semantic security of PKE. Thus, the privacy of x is preserved.

Actually, above construction would immediately lead to 1-bound FE enduring multiple users, by rendering a trusted authority to generate all public keys $\{\overline{pk}_{w,b}\}$ and then distributing secret key corresponding to each user's circuit. However, in the context of registration, such idea is unrealistic since the aggregator must store no long-term secret. Most importantly, *L* users will generate *L* different public keys by themselves, so our problem is how to adapt above construction to accommodate more than one user. **Step 1: 1-Bound** *L*-**Slot RFE.** Next, we proceed to convert 1-bound 1-slot RFE into 1-bound *L*-slot RFE that allows *L* users to register their circuits C_1, \ldots, C_L . Apparently, public key encryption is insufficient to accommodate all these circuits in mpk, so our idea is to replace it with a more powerful tool, i.e., slotted registered broadcast encryption (RBE). In slotted RBE, each user will register his slot index into mpk, and ciphertext is associated with a broadcast set (that is denoted by a bit string $S \in \{0, 1\}^L$) and a message m. For a user indexed by *i*, the decryption algorithm will recover m properly only when S[i] = 1. As for security, we just need "minimal" IND security, which states that the adversary cannot distinguish the ciphertext encrypted by either m_0 or m_1 given public parameters. The reason why we call minimal security is that the adversary is assumed to be unable to collude with any registered user. Let sRBE = (Setup, Gen, Ver, Agg, Enc, Dec) be a slotted RBE with minimal security, we depict 1-bound *L*-slot RFE as follows.

First, the aggregator initializes 2n instances of sRBE and obtains a sequence of $\{\operatorname{crs}_{w,b}\}_{w \in [n], b \in \{0,1\}}$. For each instance, it runs sRBE.Gen to generate L public keys $\{\widehat{\mathsf{pk}}_{i,w,b}\}_{i \in [L], w \in [n], b \in \{0,1\}}$. Then set

$$\operatorname{crs} = (\{\operatorname{crs}_{w,b}\}_{w \in [n], b \in \{0,1\}}, \{\overline{\mathsf{pk}}_{i,w,b}\}_{i \in [L], w \in [n], b \in \{0,1\}}).$$

For a user with slot index *i*, he samples $(\mathsf{pk}_{i,w,b}, \mathsf{sk}_{i,w,b}) \leftarrow \mathsf{sRBE}.\mathsf{Gen}(\mathsf{crs}_{w,b}, i)$ for each instance. Then set public key and secret key as

$$\mathsf{pk}_i = (\{\mathsf{pk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}}), \ \mathsf{sk}_i = (\{\mathsf{sk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}}).$$

Upon receiving $\{pk_i, C_i\}_{i \in [L]}$, the aggregator will initialize broadcast sets $S_{w,b} \in \{0,1\}^L$ for each $w \in [n]$ and $b \in \{0,1\}$, then define master public key mpk and helper secret key hsk_i (for slot $j \in [L]$) as follows:

$$mpk = \begin{pmatrix} mpk_{1,0} \cdots mpk_{n,0} \\ mpk_{1,1} \cdots mpk_{n,1} \end{pmatrix} \text{ and } hsk_j = \begin{pmatrix} hsk_{j,1,0} \cdots hsk_{j,n,0} \\ hsk_{j,1,1} \cdots hsk_{j,n,1} \end{pmatrix}$$

where for each $w \in [n]$ and $b \in \{0, 1\}$, it involves two steps:

(i) for all $i \in [L]$, set

$$(\overline{\mathsf{pk}}_{i,w,b}, S_{w,b}[i]) := \begin{cases} (\mathsf{pk}_{i,w,b}, 1), \text{ when } \mathsf{C}_i[w] = b, \\ (\widehat{\mathsf{pk}}_{i,w,b}, 0), \text{ otherwise.} \end{cases}$$

(ii) run $(\mathsf{mpk}'_{w,b}, \{\mathsf{hsk}_{j,w,b}\}_{j \in [L]}) \leftarrow \mathsf{sRBE}.\mathsf{Agg}(\mathsf{crs}_{w,b}, \{i, \overline{\mathsf{pk}}_{i,w,b}\}_{i \in [L]}) \text{ and set } \mathsf{mpk}'_{w,b}, \mathsf{smb}).$

The encryption algorithm works in a similar way. Briefly, we run algorithm sRBE.Enc to generate the ciphertext:

$$ct = \left(\tilde{U}, \left(\begin{array}{c} sRBE.Enc(mpk_{1,0}, lab_{1,0}) \cdots sRBE.Enc(mpk_{n,0}, lab_{n,0}) \\ sRBE.Enc(mpk_{1,1}, lab_{1,1}) \cdots sRBE.Enc(mpk_{n,1}, lab_{n,1}) \end{array} \right) \right),$$

where $(\tilde{U}, \{lab_{w,b}\}_{w \in [n], b \in \{0,1\}}) \leftarrow Garble(1^{\lambda}, U[x])$ and note that broadcast set $S_{w,b}$ has been contained in mpk_{w,b}. The decryption follows algorithms sRBE.Dec and Eval. At last, the security analysis is as follows:

– In corrupt case, suppose C^{*} is the unique corrupted circuit, let $b_w = C^*[w]$ and $\overline{b}_w = 1 - C^*[w]$, then we have

$$\begin{split} & \tilde{U}, \left\{ \text{sRBE}.\text{Enc}(\text{mpk}_{w,b_w}|\text{ab}_{w,b_w}) \right\}_{w \in [n]}, \left\{ \text{sRBE}.\text{Enc}(\text{mpk}_{w,\overline{b}_w}, |\text{ab}_{w,\overline{b}_w}) \right\}_{w \in [n]} \\ & \approx \tilde{U}, \left\{ \text{sRBE}.\text{Enc}(\text{mpk}_{w,b_w}, |\text{ab}_{w,b_w}) \right\}_{w \in [n]}, \left\{ \text{sRBE}.\text{Enc}(\text{mpk}_{w,\overline{b}_w}, \text{Random}) \right\}_{w \in [n]} \\ & \approx \tilde{U}, \left\{ \text{sRBE}.\text{Enc}(\text{mpk}_{w,b_w}, |\overline{\text{ab}}_{w,b_w}) \right\}_{w \in [n]}, \left\{ \text{sRBE}.\text{Enc}(\text{mpk}_{w,\overline{b}_w}, \text{Random}) \right\}_{w \in [n]} \end{split}$$

where $(\widetilde{U}, \{\widetilde{lab}_{w,b_w}\}_{w \in [n]}) \leftarrow \widetilde{Garble}(1^{\lambda}, C^*(x))$. The first \approx follows the IND security of slotted RBE, and the second \approx follows the simulation security of garbled circuits.

- In honest case, since the adversary has no idea about the secret key for some honest circuit $C_i \neq C^*$, he cannot acquire all labels $\{lab_{w,C_i}[w]\}_{w \in [n]}$. Thus, it is impossible to learn other information about x, including $C_i(x)$.

Efficiency. It seems that 1-bound *L*-slot RFE is almost accomplished, because slotted RBE with minimal security can be directly obtained from recent works [HLWW23,FWW23,ZZGQ23]. However, we observe above transformation has a vital drawback. Recall that the compactness of slotted RBE requires mpk and hsk of size poly(P, log L) where *P* denotes the size of broadcast space. Considering broadcast space is exactly [*L*] and broadcast set for encryption contains *L* bits, it is completely reasonable that slotted RBE has the following properties:

$$\underbrace{|\mathsf{mpk}| = \mathsf{poly}(L), |\mathsf{hsk}| = \mathsf{poly}(L),}_{\text{Real compactness}}, \underbrace{|\mathsf{ct}| = \mathsf{poly}(L)]}_{\text{Real encryption}}.$$

Unfortunately, applying such slotted RBE will immediately lead to mpk and hsk of size poly(L) in our resulting construction since it does not reach the compactness goal of slotted RFE, i.e.,

$$|\underline{\mathsf{mpk}}| = \mathsf{poly}(C, \log L), \ |\mathsf{hsk}| = \mathsf{poly}(C, \log L).$$

Besides, the encryption algorithm would be extremely inefficient when L is a large number.

To address this issue, we have to severely restrict the efficiency of underlying slotted RBE. Specifically, we expect that the underlying slotted RBE provides

Optimal compactness. It means |mpk| = poly(log L), |hsk| = poly(log L) and ct = poly(log L). Thus, our 1-bound
 L-slot RFE naturally enjoys mpk and hsk of size poly(C, log L), as well as compact ciphertext.

However, it seems rather tough to carry above thought into practice, because such efficiency requirement (especially compact ciphertext) is too restrictive. As an alternative solution, we pay attention to a weaker variant of RBE, called *global slotted RBE*. Concretely, this primitive is identical to slotted RBE except that its encryption always sets $S = 1^L$ as default. This is inspired by the fact that the aggregator is generally assumed to be honest and transparent (implied by common reference string model [HLWW23]). Therefore, it is unnecessary to assign broadcast sets $\{S_{w,b}\}_{w \in [n], b \in \{0,1\}}$ for each component in ct, so we can directly fixed them at 1^L , which relieves us of the difficult task of designing broadcast strategy in highly compact ciphertext.

In summary, a global slotted RBE with optimal compactness will yield a 1-bound *L*-slot RFE for circuits through our transformation (in Section 5). Then the next question is how to obtain a concrete global slotted RBE. We claim that this thing is not technically harder than constructing an RABE scheme. In particular, global slotted RBE can be derived from RABE by applying the generic transformation in [FWW23] which was used to build flexible BE. This reflects the universality of the primitive we proposed because several RABE schemes [ZZGQ23,FWW23] from suitable assumptions have been provided. Nevertheless, we remark that this transformation seems a bit cumbersome, requiring a pair of dummy attribute and policy for functionality and thus causing extra overhead on performance. In this work, we present two global slotted RBE schemes (in Section 3 and Section 4) that do not need any dummy attribute/policy while still achieving optimal compactness and adaptive security.

As a result, we obtain two concrete 1-bound *L*-slot RFE for circuits that are adaptively SIM secure under *k*-Lin assumption and (evasive) LWE assumption, respectively². Comparatively, although [BLM⁺24] has given a concrete 1-bound *L*-slot RFE for circuits, it just achieves weaker selective IND security, relying on *q*-type DDH assumption.

² Our pairing-based construction has the same structure as the *k*-Lin distributed BE in [KMW23], because both of them are based on the BE scheme in [GW09]. Our lattice-based construction can also be seen as a new application of witness encryption.

Step 2: *Q***-Bound** *L***-Slot RFE.** Here, we adopt Gorbunov et al.'s generic transformation [GVW12]. In essence, it exploits a reusable dynamic MPC protocol [AV19] to upgrade 1-bound FE to *Q*-bound FE. This methodology is as well suitable for the conversion from 1-bound *L*-slot RFE to *Q*-bound *L*-slot RFE (without malicious case).

Roughly speaking, we improves 1-bound security to *Q*-bound security by implementing *N* instances of 1-bound slotted RFE in parallel, where *N* is a system parameter dependent on *Q*. To resist the adversary colluding with *Q* users, the encryption algorithm will divide data *x* into *N* secret shares, then use these instances to encrypt each share. In the meantime, we restrict each user only register into a part of *N* instances. For decryption, the user first computes multiple local parts of C(x) using secret keys, then recovers the whole C(x) by aggregating these local parts. In security reduction, *Q*-bound security are based on the security of underlying 1-bound *L*-slot RFE and MPC protocol. Finally, we manage to build a *Q*-bound *L*-slot RFE for circuits (in Section 6) which can be later transformed into a full-fledged *Q*-bound RFE via "power-of-two" [HLWW23,FFM⁺23].

Towards Unbounded Users. As we can see, above generic construction only supports a finite number of users, due to crs of size poly(L). Even so, we point out that it can also be utilized to construct RFE supporting an arbitrary number of users, as long as the underlying global slotted RBE supports unbounded users as well. This can be done in **Step 1** by removing all public keys $\{\widehat{pk}_{i,w,b}\}$ in crs and directly aggregating all public keys from users to generate mpk and hsk. In this way, crs only consists of a limited number of global slotted RBE instances, so the size of crs will naturally not scale with *L* if the crs of global slotted RBE does not grow with *L*. Thereby, we obtain a concrete RFE for circuits enjoying unbounded users property. Considering all parameters of size unavoidably growing with *Q*, our unbounded notion is a bit weaker than earlier works [HLWW23,FWW23], but this will not be an issue due to the fact that $Q \ll L$.

1.3 Disscussion

Malicious Case. The technical barrier to tackle malicious case in *Q*-bound slotted RFE lies on the fact that the challenger cannot ensure adversary generates secret key with right randomness. Although non-interactive zero-knowledge arguments (NIZK) [ZZGQ23,BLM⁺24] would be helpful in simulating challenge ciphertext with only public keys, the adversary can still control the generation of randomness which is essential to the upgradation from 1-bound security to *Q*-bound security. Previously, only *iO*-based solution is known to resist malicious users, and it aims at weak IND security. Therefore, we leave seeking new technology to tackle malicious case in RFE for circuits without *iO* as a future work.

Dynamic Bounded Collusion Model. Recently, Agrawal et al. [AMVY21] and Garg et al. [GGLW22] initiated the notion of *dynamic bounded collusion model*, where *Q* is given in the encryption algorithm (instead of setup algorithm) and hence enable to more flexibly select collusion bound while balancing performance. Comparatively, our RFE is static bounded collusion-resistant. At a high level, it is feasible to spread the concept of dynamic bounded collusionresistance to the registering setting, then there is no need to require all parameters of size relevant to *Q*. However, to our best knowledge, it seems necessary to build a dynamic bounded RFE based on the existence of static bounded RFE [GGL24]. Therefore, we believe this work will motivate the study of dynamic bounded collusionresistant RFE. **Succinctness.** One may want to ask whether it is possible to achieve succinct RFE, i.e., the encryption overhead sublinear in the size of the circuit. Intuitively, we can build a succinct 1-bound slotted RFE from our 1-bound slotted RFE and a *Laconic Function Evaluation* (LFE). It is analogous to Quach et al.'s transformation [QWW18] applying on non-succinct 1-bound FE. Concretely, LFE can be used to deterministically compress the large-sized registered circuit into a short digest, then succinctness is guaranteed by performing RFE encryption with respect to LFE encryption, as the overhead of LFE encryption is small.

1.4 Related Work

We mention other works to remove the trusted authority in FE. Chandran et al. [CGJS15] introduced the notion of multi-authority functional encryption (MAFE), then proposed a MAFE for arbitrary polynomial-time function based on subexponentially secure *iO* and injective one-way functions. On the other hand, Chotard et al. [CDG⁺18] formalized the notion of decentralized muliti-client functional encryption (DMCFE) and gave the first instance supporting inner-product computation, afterwards an elegant line of work [ABKW19,ABG19,ACF⁺20] are devoted to this filed, while all of them only focus on linear function. Furthermore, Chotard et al. [CDSG⁺20] formalized a new extension called dynamic decentralized functional encryption (DDFE) that allows multiple users to join the system dynamically and generate secret keys in a decentralized fashion. Beyond linear function, a recent work [ATY23] provided the first DDFE for attributed-weighted sums that includes arithmetic branch programs. In addition, Agrawal et al. [AGT21] initiated the study of multi-party functional encryption (MPFE) that unifies a wide range of FE variants, including but not limited to MAFE, DMCFE and DDFE.

2 Preliminaries

For a finite set *S*, we write $s \leftarrow S$ to denote that *s* is picked uniformly from finite set *S*. Then, we use |S| to denote the size of *S*. Let \approx_s stand for two distributions being statistically indistinguishable, and \approx_c denote two distributions being computationally indistinguishable. For any $x \in \{0, 1\}^n$, we use x[w] to denote the *w*-th bit of *x*.

2.1 Prime-Order Bilinear Groups

A generator \mathcal{G} takes as input a security parameter 1^{λ} and outputs a description $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, where p is a prime, $\mathbb{G}_1, \mathbb{G}_2$ and \mathbb{G}_T are cyclic groups of order p, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a non-degenerate bilinear map. Group operations in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ and bilinear map e are computable in deterministic polynomial time in λ . Let $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ and $g_T = e(g_1, g_2) \in \mathbb{G}_T$ be the respective generators, we employ *implicit representation* of group elements: for a matrix \mathbf{M} over \mathbb{Z}_p , we define $[\mathbf{M}]_s = g_s^{\mathbf{M}}, \forall s \in \{1, 2, T\}$, where exponentiation is carried out componentwise. Given $[\mathbf{A}]_1, [\mathbf{B}]_2$ where \mathbf{A} and \mathbf{B} have proper sizes, we let $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$. We review *matrix decisional Diffie-Hellman (MDDH) assumption*, which is implied by k-Lin [EHK⁺13].

Assumption 1 ((k, ℓ, d) **-MDDH over** \mathbb{G}_s , $s \in \{1, 2\}$ **)** *Let* $k, \ell, d \in \mathbb{N}$ *with* $k < \ell$ *. We say that the* (k, ℓ, d) *-MDDH assumption holds in* \mathbb{G}_s *if for all efficient adversaries* \mathcal{A} *, the following advantage function is negligible in* λ *.*

$$\mathsf{Adv}^{MDDH}_{\mathcal{A},s,k,\ell,d}(\lambda) = \left| \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_s, [\mathbf{SM}]_s) = 1] - \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_s, [\mathbf{U}]_s) = 1] \right|$$

where $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^{\lambda}), \mathbf{M} \leftarrow \mathbb{Z}_p^{k \times \ell}, \mathbf{S} \leftarrow \mathbb{Z}_p^{d \times k} and \mathbf{U} \leftarrow \mathbb{Z}_p^{d \times \ell}.$

2.2 Garbled Circuits

Algorithms. A garbled circuit scheme [Yao86,BHR12] (with input $x \in \{0, 1\}^n$ and circuit family *C*) consists of two efficient algorithms as follows:

- Garble $(1^{\lambda}, C) \rightarrow (\tilde{C}, \{ \mathsf{lab}_{w,b} \}_{w \in [n], b \in \{0,1\}})$. It takes as input security parameter 1^{λ} and a circuit $C \in C$, and then outputs a garbled circuit \tilde{C} and labels $\{ \mathsf{lab}_{w,b} \}_{w \in [n], b \in \{0,1\}}$.
- $\text{Eval}(\tilde{C}, \{\text{lab}_{w,x[w]}\}_{w \in [n]}) \rightarrow z$. It takes as input a garbled circuit \tilde{C} and a sequence of input labels $\{\text{lab}_{w,x[w]}\}_{w \in [n]}$, and then deterministically outputs a value z.

Without loss of generality, we assume that the size of each label $lab_{w,b}$ is $O(\lambda)$. **Correctness.** For all λ , for any circuit C and input $x \in \{0, 1\}^n$, we have

rectiless. For an λ , for any circuit c and input $\lambda \in \{0, 1\}$, we have

 $\Pr[\mathsf{Eval}(\tilde{\mathsf{C}}, \{\mathsf{lab}_{w,x[w]}\}_{w \in [n]}) = \mathsf{C}(x) \mid (\tilde{\mathsf{C}}, \{\mathsf{lab}_{w,b}\}_{w \in [n], b \in \{0,1\}}) \leftarrow \mathsf{Garble}(1^{\lambda}, \mathsf{C})] = 1.$

Security. There exists a simulator Garble such that for any circuit C and input $x \in \{0, 1\}^n$, we have

$$(\tilde{\mathsf{C}}, \{\mathsf{lab}_{w,x[w]}\}_{w \in [n]}) \approx_c \tilde{\mathsf{Garble}}(1^{\lambda}, \mathsf{C}(x))$$

where $(\tilde{C}, \{lab_{w,b}\}_{w \in [n], b \in \{0,1\}}) \leftarrow Garble(1^{\lambda}, C)$.

2.3 Global Slotted Registered Broadcast Encryption

Algorithms. A global slotted registered broadcast encryption (global slotted RBE for short) consists of six efficient algorithms as follows:

- Setup $(1^{\lambda}, 1^{L}) \rightarrow$ crs. It takes as input the security parameter 1^{λ} , the upper bound 1^{L} of the number of slots, outputs a common reference string crs.
- Gen(crs, i) \rightarrow (pk_i, sk_i). It takes as input crs and $i \in [L]$, outputs a key pair (pk_i, sk_i).
- Ver(crs, *i*, pk_i) \rightarrow 0/1. It takes as input crs, *i*, pk_i , outputs a bit indicating whether pk_i is valid.
- − Agg(crs, $\{i, pk_i\}_{i \in [L]}$) → (mpk, $\{hsk_j\}_{j \in [L]}$). It takes as input crs and a series of pk_i with slot index *i* for all $i \in [L]$, outputs master public key mpk and a series of helper keys hsk_j for all $j \in [L]$.
- $\mathsf{Enc}(\mathsf{mpk},\mathsf{m})\to\mathsf{ct}.$ It takes as input mpk and a message $\mathsf{m},$ outputs a ciphertext ct.
- $Dec(hsk_{i^*}, sk_{i^*}, ct) \rightarrow m/\bot$. It takes as input hsk_{i^*}, sk_{i^*}, ct , outputs m or an empty symbol \bot .

Completeness. For all $\lambda, L \in \mathbb{N}$, and all $i \in [L]$, we have

$$\Pr\left[\operatorname{Ver}(\operatorname{crs}, i, \operatorname{pk}_i) = 1 | \operatorname{crs} \leftarrow \operatorname{Setup}(1^{\lambda}, 1^L); (\operatorname{pk}_i, \operatorname{sk}_i) \leftarrow \operatorname{Gen}(\operatorname{crs}, i) \right] = 1.$$

Correctness. For all $\lambda, L \in \mathbb{N}$, and all $i^* \in [L]$, all crs \leftarrow Setup $(1^{\lambda}, 1^L)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i \in [L] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, and all m, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{hsk}_{i^*},\mathsf{sk}_{i^*},\mathsf{ct}) = \mathsf{m} \left| (\mathsf{mpk},\{\mathsf{hsk}_j\}_{j \in [L]}) \leftarrow \mathsf{Agg}(\mathsf{crs},\{i,\mathsf{pk}_i\}_{i \in [L]}) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk},m) \right| = 1.$$

Optimal Compactness. For all $\lambda, L \in \mathbb{N}$, and all $i \in [L]$, it holds that

 $|mpk| = poly(\lambda, \log L)$ and $|hsk_i| = poly(\lambda, \log L)$.

In addition, it requires $|ct| = poly(\lambda, \log L)$.

Indistinguishability-Based (IND) Security. For all $\lambda \in \mathbb{N}$ and all efficient adversaries \mathcal{A} , the indistinguishability-based security requires the advantage

$$\Pr\left[b' = b \begin{vmatrix} L \leftarrow \mathcal{A}(1^{\lambda}); \operatorname{crs} \leftarrow \operatorname{Setup}(1^{\lambda}, 1^{L}) \\ (\{i, \mathsf{pk}_{i}^{*}\}_{i \in [L]}, \mathsf{m}_{0}^{*}, \mathsf{m}_{1}^{*}) \leftarrow \mathcal{A}^{\operatorname{OGen}(\cdot).\operatorname{OCor}(\cdot)}(\operatorname{crs}) \\ (\mathsf{mpk}, \{\mathsf{hsk}_{j}\}_{j \in [L]}) \leftarrow \operatorname{Agg}(\operatorname{crs}, \{i, \mathsf{pk}_{i}^{*}\}_{i \in L}) \\ b \leftarrow \{0, 1\}; \operatorname{ct}^{*} \leftarrow \operatorname{Enc}(\mathsf{mpk}, \mathsf{m}_{b}^{*}); b' \leftarrow \mathcal{A}(\operatorname{ct}^{*}) \end{vmatrix}\right] - \frac{1}{2}$$

is negligible in λ , where oracles OGen, OCor work with initial setting $\{\mathcal{D}_i = \emptyset\}_{i \in [L]}, C = \emptyset$ as follows:

- OGen(*i*): run (pk, sk) \leftarrow Gen(crs, *i*), set $\mathcal{D}_i[pk] =$ sk and return pk.

- OCor(*i*, pk): return $\mathcal{D}_i[pk]$ and update $C = C \cup \{(i, pk)\}$.

and for all $i \in [L]$, we require $\mathcal{D}_i[\mathsf{pk}_i^*] \neq \perp$ and $(i, \mathsf{pk}_i^*) \notin C$.

Indeed, global slotted RBE can be seen as a plain slotted RBE which always set broadcast set as 1^{*L*} and achieves the minimal security, i.e., IND security only under honest case.

2.4 Q-Bound Slotted Registered Functional Encryption

Algorithms. A *Q*-bound slotted registered functional encryption (*Q*-bound slotted RFE for short) for circuit family $C: X \rightarrow Z$ consists of six efficient algorithms as follows:

- Setup $(1^{\lambda}, 1^{L}, 1^{Q}, C) \rightarrow$ crs. It takes as input the security parameter 1^{λ} , upper bound 1^{L} of the number of slots, collusion bound 1^{Q} and circuit family *C*, outputs a common reference string crs.
- Gen(crs, i) \rightarrow (pk_i, sk_i). It takes as input crs and slot index $i \in [L]$, outputs a key pair (pk_i, sk_i).
- Ver(crs, *i*, pk_i) \rightarrow 0/1. It takes as input crs, *i*, pk_i , outputs a bit indicating whether pk_i is valid.
- Agg(crs, $\{pk_i, C_i\}_{i \in [L]}$) \rightarrow (mpk, $\{hsk_j\}_{j \in [L]}$). It takes as input crs and a series of pk_i with $C_i \in C$ for all $i \in [L]$, outputs master public key mpk and a series of helper keys hsk_j for all $j \in [L]$. This algorithm is deterministic.
- $Enc(mpk, x) \rightarrow ct$. It takes as input mpk, $x \in X$, outputs a ciphertext ct.
- $Dec(hsk_{i^*}, sk_{i^*}, ct) \rightarrow z/\bot$. It takes as input hsk_{i^*}, sk_{i^*}, ct , outputs $z \in Z$ or an empty symbol \bot .

Completeness. For all $\lambda, L \in \mathbb{N}$, all $Q \ll L$ and all C, and all $i \in [L]$, we have

$$\Pr\left[\operatorname{Ver}(\operatorname{crs}, i, \mathsf{pk}_i) = 1 | \operatorname{crs} \leftarrow \operatorname{Setup}(1^{\lambda}, 1^L, 1^Q, C); (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \operatorname{Gen}(\operatorname{crs}, i)\right] = 1$$

Correctness. For all $\lambda, L \in \mathbb{N}$, all $Q \ll L$ and all C, and all $i^* \in [L]$, all crs \leftarrow Setup $(1^{\lambda}, 1^L, 1^Q, C)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow$ Gen (crs, i^*) , all $\{\mathsf{pk}_i\}_{i \in [L] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, all $x \in X$ and $\mathsf{C}_1, \ldots, \mathsf{C}_L \in C$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{hsk}_{i^*},\mathsf{sk}_{i^*},\mathsf{ct}) = \mathsf{C}_{i^*}(x) \middle| (\mathsf{mpk},\{\mathsf{hsk}_j\}_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs},\{\mathsf{pk}_i,\mathsf{C}_i\}_{i\in[L]}) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk},x) \right] = 1$$

Compactness. For all $\lambda, L \in \mathbb{N}$, all $Q \ll L$ and all C, and all $i \in [L]$, it holds that

$$|mpk| = poly(\lambda, C, Q, log L)$$
 and $|hsk_i| = poly(\lambda, C, Q, log L)$.

Simulation-Based (SIM) Security. For all $\lambda \in \mathbb{N}$ and all efficient adversaries \mathcal{A} , the adaptive simulation-based security requires that there exists simulator $\widetilde{\mathsf{Enc}}$ such that:

where oracles OGen, OCor work with initial setting $\{\mathcal{D}_i = \emptyset\}_{i \in [L]}, C = \emptyset$ and $\mathcal{K} = \emptyset$ as follows:

- OGen(*i*): run (pk, sk) \leftarrow Gen(crs, *i*), set $\mathcal{D}_i[pk] =$ sk and return pk.

- OCor(*i*, pk): return $\mathcal{D}_i[pk]$ and update $C = C \cup \{(i, pk)\}$.

Here, We consider the notion of *Q*-bound SIM security without malicious case. More concretely, it requires (i) $\mathcal{D}_i[\mathsf{pk}_i^*] \neq \perp$ for all $i \in [L]$; (ii) for each $(i, \mathsf{pk}_i^*) \in C$ where $|C| \leq Q^3$, set $\mathcal{K} = \mathcal{K} \cup \{(i, \mathsf{C}_i^*, \mathsf{C}_i^*(x^*), \mathcal{D}_i[\mathsf{pk}_i^*])\}$.

³ Here, we consider the bounded collusion model in a weak sense, i.e., the number of corruption queries is restricted. Nevertheless, our 1-bound RFE construction is still secure, even allowing arbitrary polynomial number of corruption queries and the existence of malicious user.

2.5 Q-Bound Registered Functional Encryption

Algorithms. A *Q*-bound registered functional encryption (*Q*-bound RFE for short) for circuit family $C : X \to Z$ consists of six efficient algorithms as follows:

- Setup $(1^{\lambda}, 1^{L}, 1^{Q}, C) \rightarrow$ crs. It takes as input the security parameter 1^{λ} , the maximum number of users 1^{L} , collusion bound 1^{Q} and circuit family *C*, outputs a common reference string crs.
- Gen(crs, aux) \rightarrow (pk, sk). It takes as input crs and state aux, outputs key pair (pk, sk).
- Reg(crs, aux, pk, C) \rightarrow (mpk, aux'). It takes as input crs, aux, pk along with C \in C, outputs master public key mpk and updated state aux'.
- Upd(crs, aux, pk) \rightarrow hsk. It takes as input crs, aux, pk, outputs a helper key hsk.
- $Enc(mpk, x) \rightarrow ct$. It takes as input mpk, $x \in X$, outputs a ciphertext ct.
- Dec(hsk, sk, ct) $\rightarrow z/\perp$ /getupd. It takes as input hsk, sk, ct, outputs $z \in Z$ or an empty symbol \perp to indicate a decryption failure, or a symbol getupd to indicate the need of an updated helper key.

Correctness. For all stateful adversary \mathcal{A} , the following advantage function is negligible in λ :

$$\Pr[b = 1 | \mathsf{crs} \leftarrow \mathsf{Setup}(1^{\lambda}, 1^L, 1^Q, C); b = 0; \mathcal{A}^{\mathsf{ORegNT}(\cdot, \cdot), \mathsf{ORegT}(\cdot), \mathsf{OEnc}(\cdot, \cdot), \mathsf{ODec}(\cdot)}(\mathsf{crs})]$$

where the oracles work as follows with initial setting aux = \bot , $\mathcal{E} = \emptyset$, $\mathcal{R} = \emptyset$ and $t = \bot$:

- ORegNT(pk, C): run (mpk, aux') ← Reg(crs, aux, pk, C), update aux = aux', append (mpk, aux) to R and return (|R|, mpk, aux);
- ORegT(C*): run (pk*, sk*) \leftarrow Gen(crs, aux), (mpk, aux') \leftarrow Reg(crs, aux, pk*, C*), update aux = aux', compute hsk* \leftarrow Upd(crs, aux, pk*), append (mpk, aux) to \mathcal{R} , return ($t = |\mathcal{R}|$, mpk, aux, pk*, sk*, hsk*);
- OEnc(i, x): let $\mathcal{R}[i] = (mpk, \cdot)$ and run ct $\leftarrow Enc(mpk, x)$, append (x, ct) to \mathcal{E} and return $(|\mathcal{E}|, ct)$;
- ODec(j): let $\mathcal{E}[j] = (x_j, ct_j)$, compute $z_j \leftarrow Dec(hsk^*, sk^*, ct_j)$. If $z_j = getupd$, run $hsk^* \leftarrow Upd(crs, aux, pk^*)$ and recompute $z_j \leftarrow Dec(hsk^*, sk^*, ct_j)$. Set b = 1 when $z_j \neq C^*(x_j)$.

with the following restrictions:

- there exists one query to ORegT;
- for query (i, x) to OEnc, it holds that $t \ge i, \mathcal{R}[i] \ne \bot$;
- for query (j) to ODec, it holds that $\mathcal{E}[j] \neq \bot$.

Compactness and Update Efficiency. For all $\lambda, L \in \mathbb{N}$, all $Q \ll L$ and all *C*, it holds that

$$|mpk| = poly(\lambda, C, Q, log L)$$
 and $|hsk| = poly(\lambda, C, Q, log L)$.

Furthermore, the number of invocations of Upd in ODec is at most $O(\log |\mathcal{R}|)$ and each invocation costs poly $(\log |\mathcal{R}|)$ time.

Simulation-Based (SIM) Security. For all $\lambda \in \mathbb{N}$ and all efficient adversaries \mathcal{A} , the adaptive simulation-based security requires that there exists simulator $\widetilde{\mathsf{Enc}}$ such that:

$$\begin{vmatrix} \operatorname{crs} \leftarrow \operatorname{Setup}(1^{\lambda}, 1^{L}, 1^{Q}, C) \\ x^{*} \leftarrow \mathcal{A}^{\operatorname{ORegHK}(\cdot), \operatorname{OCorHK}(\cdot)}(\operatorname{crs}) \\ \operatorname{ct}^{*} \leftarrow \operatorname{Enc}(\operatorname{mpk}, x^{*}) \\ \mathcal{A}^{\operatorname{OCorHK}(\cdot)}(\operatorname{ct}^{*}); \alpha \leftarrow \mathcal{A}(\operatorname{ct}^{*}) \end{vmatrix} \approx_{c} \begin{vmatrix} \operatorname{crs} \leftarrow \operatorname{Setup}(1^{\lambda}, 1^{L}, 1^{Q}, C) \\ x^{*} \leftarrow \mathcal{A}^{\operatorname{ORegHK}(\cdot), \operatorname{OCorHK}(\cdot)}(\operatorname{crs}) \\ \widetilde{\operatorname{ct}}^{*} \leftarrow \operatorname{Enc}(\operatorname{mpk}, \mathcal{K}); \\ \mathcal{A}^{\operatorname{OCorHK}(\cdot)}(\operatorname{ct}^{*}); \alpha \leftarrow \mathcal{A}(\operatorname{ct}^{*}) \end{vmatrix}$$

where oracles ORegHK, OCorHK work with initial setting mpk = \perp , aux = \perp , $\mathcal{R} = \emptyset$, $\mathcal{C} = \emptyset$, $\mathcal{K} = \emptyset$ and \mathcal{D} being a dictionary with $\mathcal{D}[pk] = \emptyset$ for all possible pk:

- ORegHK(C): run (pk, sk) \leftarrow Gen(crs, aux) and (mpk', aux') \leftarrow Reg(crs, aux, pk, C), update mpk = mpk', aux = aux', $\mathcal{D}[pk] = \mathcal{D}[pk] \cup \{C\}$, append (pk, sk) to \mathcal{R} and return ($|\mathcal{R}|$, mpk, aux, pk);
- OCorHK(*i*): let $\mathcal{R}[i] = (pk, sk)$ and $C = \mathcal{D}[pk]$, append pk to *C* and return sk.

Similarly, we require the *Q*-bound SIM security without malicious case. More concretely, it requires (i) $\mathcal{R}[i] \neq \perp$ for each query *i* to OCorHK; (ii) for each $(i, \mathsf{pk}_i^*) \in C$ where $|C| \leq Q$, let $\mathcal{R}[i] = (\mathsf{pk}_i^*, \mathsf{sk}_i^*)$ and $\mathsf{C}_i = \mathcal{D}[\mathsf{pk}_i^*]$, set $\mathcal{K} = \mathcal{K} \cup \{(i, \mathsf{C}_i^*, \mathsf{C}_i^*(x^*), \mathsf{sk}_i^*)\}$.

3 Pairing-Based Global Slotted RBE

In this section, we present a global slotted RBE relying on MDDH assumption.

3.1 Construction

Our construction works as follows:

- Setup $(1^{\lambda}, 1^{L})$: Generate $\mathbb{G} := (p, \mathbb{G}_{1}, \mathbb{G}_{2}, \mathbb{G}_{T}, e) \leftarrow \mathcal{G}(1^{\lambda})$ and sample

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (k+1)}, \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1) \times k}, \mathbf{k} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}.$$

For all $i \in [L]$, sample $\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(k+1) \times (k+1)}$, $\mathbf{r}_i \leftarrow \mathbb{Z}_p^{1 \times k}$. Output

$$\operatorname{crs} = \begin{pmatrix} [\mathbf{A}]_1, \{ [\mathbf{A}\mathbf{V}_i]_1, [\mathbf{B}\mathbf{r}_i^{\mathsf{T}}, \mathbf{V}_i\mathbf{B}\mathbf{r}_i^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_2 \}_{i \in [L]}, \\ \{ [\mathbf{V}_i\mathbf{B}\mathbf{r}_j^{\mathsf{T}}]_2 \}_{j \in [L], i \in [L] \setminus \{j\}}, [\mathbf{A}\mathbf{k}^{\mathsf{T}}]_T \end{pmatrix}$$

- Gen(crs, *i*) : Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1) \times (k+1)}$, output $\mathsf{pk}_i = ([\mathbf{AU}_i]_1, \{[\mathbf{U}_i \mathbf{Br}_i^{\mathsf{T}}]_2\}_{j \in [L] \setminus \{i\}})$ and $\mathsf{sk}_i = \mathbf{U}_i$.

- Ver(crs, *i*, pk_i) : Parse the public key pk_i = ([AU_i]₁, {[U_iBr_i]₂}_{j \in [L] \ {i}}). For each $j \in [L] \setminus \{i\}$, check

$$e([\mathbf{A}]_1, [\mathbf{U}_i \mathbf{B} \mathbf{r}_j^{\mathsf{T}}]_2) \stackrel{?}{=} e([\mathbf{A} \mathbf{U}_i]_1, [\mathbf{B} \mathbf{r}_j^{\mathsf{T}}]_2).$$

If above checks pass, output 1; otherwise, output 0.

- Agg(crs, $\{i, pk_i\}_{i \in [L]}$): For all $i \in [L]$, parse $pk_i = ([\mathbf{AU}_i]_1, \{[\mathbf{U}_i \mathbf{Br}_i^{\mathsf{T}}]_2\}_{j \in [L] \setminus \{i\}})$. Output

$$\mathsf{mpk} = \left([\mathbf{A}]_1, [\mathbf{Ak}^{\mathsf{T}}]_T, \left[\sum_{j \in [L]} (\mathbf{AV}_j + \mathbf{AU}_j) \right]_1 \right),$$

and for all $i \in [L]$, output

$$\mathsf{hsk}_{i} = \left(\underbrace{[\mathbf{Br}_{i}^{\mathsf{T}}]_{2}, [\mathbf{V}_{i}\mathbf{Br}_{i}^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_{2}, [\underbrace{\sum_{j \in [L] \setminus \{i\}} (\mathbf{V}_{j}\mathbf{Br}_{i}^{\mathsf{T}} + \mathbf{U}_{j}\mathbf{Br}_{i}^{\mathsf{T}})}_{\mathbf{k}_{2}^{\mathsf{T}}}\right]_{2}}_{\mathbf{k}_{2}^{\mathsf{T}}}\right)$$

- Enc(mpk, m) : Parse mpk = $([\mathbf{A}]_1, [\mathbf{Ak}^T]_T, [\sum_{j \in [L]} (\mathbf{AV}_j + \mathbf{AU}_j)]_1)$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$, output

$$\mathsf{ct} = \left(\underbrace{[\mathbf{SA}]}_{\mathbf{c}_0} \right)_1, \left[\underbrace{\sum_{j \in [L]} (\mathbf{SAV}_j + \mathbf{SAU}_j)}_{\mathbf{c}_1} \right]_1, \underbrace{[\mathbf{SAk}^{\mathsf{T}}]_T \cdot \mathsf{m}}_C \right)_1$$

- Dec(hsk_{i*}, sk_{i*}, ct) : Parse sk_{i*} = \mathbf{U}_{i*} , hsk_{i*} = ($[\mathbf{k}_0^T]_2$, $[\mathbf{k}_1^T]_2$, $[\mathbf{k}_2^T]_2$) and ct = ($[\mathbf{c}_0]_1$, $[\mathbf{c}_1]_1$, C). Compute

$$[z_1]_T = e([\mathbf{c}_1]_1, [\mathbf{k}_0^{\mathsf{T}}]_2), \quad [z_2]_T = e([\mathbf{c}_0]_1, [\mathbf{k}_2^{\mathsf{T}}]_2),$$

$$[z_3]_T = e([\mathbf{c}_0\mathbf{U}_{i^*}]_1, [\mathbf{k}_0^{\mathsf{T}}]_2), \quad [z_4]_T = e([\mathbf{c}_0]_1, [\mathbf{k}_1^{\mathsf{T}}]_2),$$

$$[z_5]_T = [z_1 - z_2 - z_3 - z_4]_T,$$

and output $z = C \cdot [z_5]_T$.

Completeness and Optimal Compactness. For completeness, it just follows the definition of bilinear map *e* and the fact $\mathbf{A} \cdot \mathbf{U}_i \mathbf{B} \mathbf{r}_j^{\mathsf{T}} = \mathbf{A} \mathbf{U}_i \cdot \mathbf{B} \mathbf{r}_j^{\mathsf{T}}$. As for optimal compactness, it is easy to see that the above construction satisfies our requirements, i.e., $|\mathsf{mpk}| = \mathsf{poly}(\lambda, \log L)$, $|\mathsf{hsk}_i| = \mathsf{poly}(\lambda, \log L)$ and $|\mathsf{ct}| = \mathsf{poly}(\lambda, \log L)$.

Correctness. For all $\lambda, L \in \mathbb{N}$, all P, all $i^* \in [L]$, all crs \leftarrow Setup $(1^{\lambda}, 1^L)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i \in [L] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, for all m , we have

$$hsk_{i^*} = ([\mathbf{k}_0^T]_2, [\mathbf{k}_1^T]_2, [\mathbf{k}_2^T]_2), ct = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1, C).$$

We obtain

$$z_1 = \sum_{i \in [L]} (\mathbf{sAV}_i \mathbf{Br}_{i^*}^{\mathsf{T}} + \mathbf{sAU}_i \mathbf{Br}_{i^*}^{\mathsf{T}}),$$

$$z_2 = \sum_{i \in [L] \setminus \{i^*\}} (\mathbf{sAV}_i \mathbf{Br}_{i^*}^{\mathsf{T}} + \mathbf{sAU}_i \mathbf{Br}_{i^*}^{\mathsf{T}}),$$

$$z_3 = \mathbf{sAU}_{i^*} \mathbf{Br}_{i^*}^{\mathsf{T}},$$

$$z_4 = \mathbf{sAV}_{i^*} \mathbf{Br}_{i^*}^{\mathsf{T}} + \mathbf{sAk}^{\mathsf{T}},$$

and then

$$z_5 = z_1 - z_2 - z_3 - z_4 = -\mathbf{s}\mathbf{A}\mathbf{k}^{\mathsf{T}}.$$

Finally, we have $z = C \cdot [z_5]_T = m$. This proves the correctness.

3.2 Security

Theorem 1. Assume MDDH assumption holds, our pairing-based global slotted RBE achieves the IND security in the standard model as defined in Section 2.3.

Game Sequence. We prove Theorem 1 via the following game sequences. Let *L* be the number of slots, i^* be the challenge slot, and m^{*} be the challenge message; Suppose $\{pk_i^*\}_{i \in [L]}$ are challenge public keys to be registered. For all $i \in [L]$, $\mathcal{D}_i = \{pk_i : \mathcal{D}_i[pk_i] = sk_i \neq \bot\}$ stores the response to OGen(i); $C_i = \{pk_i : (i, pk_i) \in C\}$ stores the response to $OCor(i, \cdot)$.

– Game₀ : Real Game. Recall that:

the common reference string is that

$$\operatorname{crs} = \begin{pmatrix} [\mathbf{A}]_1, \{ [\mathbf{A}\mathbf{V}_i]_1, [\mathbf{B}\mathbf{r}_i^{\mathsf{T}}, \mathbf{V}_i\mathbf{B}\mathbf{r}_i^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_2 \}_{i \in [L]}, \\ \{ [\mathbf{V}_i\mathbf{B}\mathbf{r}_j^{\mathsf{T}}]_2 \}_{j \in [L], i \in [L] \setminus \{j\}}, [\mathbf{A}\mathbf{k}^{\mathsf{T}}]_T \end{pmatrix}$$

• For each $i \in [L]$, each public key $pk_i \in \mathcal{D}_i$ is that

$$\mathsf{pk}_i = ([\mathbf{A}\mathbf{U}_i]_1, \{[\mathbf{U}_i\mathbf{B}\mathbf{r}_j^{\mathsf{T}}]_2\}_{j\in[L]\setminus\{i\}}).$$

It corresponds to secret key $sk_i = U_i$.

• The challenge ciphertext is

$$\mathsf{ct}^* = \left(\underbrace{[\mathbf{SA}]}_{\mathbf{c}_0}]_1, \left[\underbrace{\sum_{j \in [L]} (\mathbf{sAV}_j + \mathbf{sAU}_j)}_{\mathbf{c}_1}\right]_1, \underbrace{[\mathbf{SAk}^{\mathsf{T}}]_T \cdot m}_C\right),$$

where $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$.

- Game₁ : Identical to Game₀ except that we replace **sA** in challenge ciphertext with $\mathbf{c} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}$. Then the challenge ciphertext is

$$\mathsf{c}\mathsf{t}^* = \left(\underbrace{[\mathbf{c}]_{1,c}}_{\mathbf{c}_0} \right]_{1,c} \left[\underbrace{\sum_{j \in [L]} (\mathbf{c} \mathbf{V}_j + \mathbf{c} \mathbf{U}_j)}_{\mathbf{c}_1} \right]_{1,c} \underbrace{[\mathbf{c} \mathbf{k}^{\mathsf{T}}]_T \cdot m}_{C} \right)$$

Observe that we have $Game_0 \approx_c Game_1$, which follows the MDDH assumption, ensuring that $([\mathbf{A}]_1, [\mathbf{sA}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (k+1)}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$ and $\mathbf{c} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}$. See Lemma 1 for more details.

- Game_{2, $\ell,1$}($\ell \in [L]$) : Identical to Game_{2, $\ell-1,3$} except that we replace $[\mathbf{Br}_{\ell}^{\mathsf{T}}, \mathbf{V}_{\ell}\mathbf{Br}_{\ell}^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_2$ in crs with the following form

$$[\mathbf{d}_{\ell}^{\scriptscriptstyle \mathsf{T}},\mathbf{V}_{\ell}\mathbf{d}_{\ell}^{\scriptscriptstyle \mathsf{T}}+\mathbf{k}^{\scriptscriptstyle \mathsf{T}}]_2,$$

where $\mathbf{d}_{\ell} \leftarrow \mathbb{Z}_{p}^{1 \times (k+1)}$. We have $\mathsf{Game}_{2,\ell-1,3} \approx_{c} \mathsf{Game}_{2,\ell,1}$, which follows the MDDH assumption $([\mathbf{B}]_{2}, [\mathbf{Br}_{\ell}^{\mathsf{T}}]_{2}) \approx_{c} ([\mathbf{B}]_{2}, [\mathbf{d}_{\ell}^{\mathsf{T}}]_{2})$, where $\mathbf{B} \leftarrow \mathbb{Z}_{p}^{(k+1) \times k}$, $\mathbf{r}_{\ell} \leftarrow \mathbb{Z}_{p}^{1 \times (k+1)}$ and $\mathbf{d}_{\ell} \leftarrow \mathbb{Z}_{p}^{1 \times k}$. See Lemma 2 for more details.

- Game_{2, $\ell,2$} : Identical to Game_{2, $\ell,1$} except that we change replace $[\mathbf{d}_{\ell}^{\mathsf{T}}, \mathbf{V}_{\ell}\mathbf{d}_{\ell}^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_2$ in crs with the following form

$$[\mathbf{d}_{\ell}^{\mathsf{T}}, \mathbf{V}_{\ell}\mathbf{d}_{\ell}^{\mathsf{T}} + \boldsymbol{\alpha}\mathbf{c}^{\perp} + \mathbf{k}^{\mathsf{T}}]_{2},$$

where $\alpha_{\ell} \leftarrow \mathbb{Z}_p$ and $\mathbf{c}^{\perp} \leftarrow \mathbb{Z}_p^{2k+1}$ such that $\mathbf{Ac}^{\perp} = 0$, $\mathbf{cc}^{\perp} = 1$. Note that $\mathsf{Game}_{2,0}$ is identical to Game_1 ; we have $\mathsf{Game}_{2,\ell,1} \approx_s \mathsf{Game}_{2,\ell,2}$, see Lemma 3 for more details.

- Game_{2, ℓ ,3} : Identical to Game_{2, ℓ ,2} except that we change replace $[\mathbf{d}_{\ell}^{\mathsf{T}}, \mathbf{V}_{\ell}\mathbf{d}_{\ell}^{\mathsf{T}} + \alpha \mathbf{c}^{\perp} + \mathbf{k}^{\mathsf{T}}]_2$ in crs with the following form

$$[\mathbf{B}\mathbf{r}_{\ell}^{\mathsf{T}},\mathbf{V}_{\ell}\mathbf{B}\mathbf{r}_{\ell}^{\mathsf{T}}+\alpha\mathbf{c}^{\perp}+\mathbf{k}^{\mathsf{T}}]_{2}.$$

Notice that we can prove $Game_{2,\ell,2} \approx_c Game_{2,\ell,3}$ via Lemma 2 as well.

- Game₃ : Identical to Game_{2,L} except that we replace the ciphertext into the following form:

$$\mathsf{ct}^* = \left(\underbrace{[\mathbf{c}]_{1, c_0}}_{\mathbf{c}_0} \right]_1, \left[\underbrace{\sum_{j \in [L]} (\mathbf{cV}_j + \mathbf{cU}_j)}_{\mathbf{c}_1} \right]_1, \underbrace{g_T^*}_{C} \right).$$

where g_T^* is sampled uniformly over G_T . We claim that $Game_{2,L} \approx_s Game_3$ which follows the following the statistical argument:

$$(\mathbf{A}\mathbf{k}^{\mathsf{T}},\mathbf{k}^{\mathsf{T}}+\alpha\mathbf{c}^{\perp},\mathbf{c}\mathbf{k}^{\mathsf{T}})\approx_{s}(\mathbf{A}\mathbf{k}^{\mathsf{T}},\mathbf{k}^{\mathsf{T}},\mathbf{c}\mathbf{k}^{\mathsf{T}}-\alpha)$$

where $[\mathbf{ck}^{T} - \alpha]_{T}$ is uniform, namely g_{T}^{*} .

In the following, we use $\mathsf{Adv}^i_{\mathcal{A}}(\lambda)$ to denote the advantage of \mathcal{A} in Game_i .

Lemma 1 (Game₀ \approx_c Game₁). For any efficient adversary \mathcal{A} , there exists algorithm \mathcal{B}_1 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}^0_{\mathcal{A}}(\lambda) - \mathsf{Adv}^1_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{MDDH}_{\mathcal{B}_1}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. Recall that the difference between two games is that we replace $[\mathbf{sA}]_1$ in Game_0 with $[\mathbf{c}]_1$, where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (k+1)}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$ and $\mathbf{c} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}$. This follows from (k, k+1, 1)-MDDH assumption, which ensures that:

$$([\mathbf{A}]_1, [\mathbf{s}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$$

On input $([A]_1, [t]_1)$ where $\mathbf{t} = \mathbf{s}\mathbf{A}$ or $\mathbf{t} = \mathbf{c}$, algorithm \mathcal{B}_1 works as follows:

Setup. Sample

$$\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1) \times k}, \mathbf{k} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}, \{\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(k+1) \times (k+1)}, \mathbf{r}_i \leftarrow \mathbb{Z}_p^{1 \times k}\}_{i \in [L]}$$

Output

$$\operatorname{crs} = \begin{pmatrix} [\mathbf{A}]_1, \{ [\mathbf{A}\mathbf{V}_i]_1, [\mathbf{B}\mathbf{r}_i^{\mathsf{T}}, \mathbf{V}_i\mathbf{B}\mathbf{r}_i^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_2 \}_{i \in [L]}, \\ \{ [\mathbf{V}_i\mathbf{B}\mathbf{r}_j^{\mathsf{T}}]_2 \}_{j \in [L], i \in [L] \setminus \{j\}}, [\mathbf{A}\mathbf{k}^{\mathsf{T}}]_T \end{pmatrix}.$$

Query. Here, for all $i \in [L]$ and each $(pk_i, sk_i) \in \mathcal{D}_i$ is generated honestly as :

$$\mathsf{pk}_i = ([\mathbf{A}\mathbf{U}_i]_1, \{[\mathbf{U}_i\mathbf{B}\mathbf{r}_j^{\mathsf{T}}]_2\}_{j \in [L] \setminus \{i\}})$$

and $\mathsf{sk}_i = \mathbf{U}_i$ where $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1) \times (k+1)}$. **Challenge.** On input challenge m^{*}, output

$$\mathsf{c}\mathsf{t}^* = \left([\mathsf{t}]_1, \left[\sum_{j\in[L]}(\mathsf{t}\mathsf{V}_j + \mathsf{t}\mathsf{U}_j)\right]_1, [\mathsf{t}\mathsf{k}^{\mathsf{T}}]_T \cdot \mathsf{m}^*\right).$$

Observe that when $\mathbf{t} = \mathbf{sA}$, the simulation is identical to $Game_0$; when $\mathbf{t} = \mathbf{c}$, the simulation is identical to $Game_1$. This readily proves the lemma.

Lemma 2 (Game_{2, ℓ -1,3} \approx_c Game_{2, ℓ ,1}). For any efficient adversary \mathcal{A} , there exists algorithm \mathcal{B}_2 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}_{\mathcal{A}}^{2,\ell-1,3}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2,\ell,1}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_2}^{MDDH}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. This follows from the (k, k + 1, 1)-MDDH assumption:

$$([\mathbf{B}]_2, [\mathbf{Br}_{\ell}^{\mathsf{T}}]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}_{\ell}^{\mathsf{T}}]_2)$$

where $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1) \times k}$, $\mathbf{r}_{\ell} \leftarrow \mathbb{Z}_p^{1 \times k}$ and $\mathbf{d}_{\ell} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}$. On input $[\mathbf{B}]_2$, $[\mathbf{t}^{\mathsf{T}}]_2$ where $\mathbf{t}^{\mathsf{T}} = \mathbf{B}\mathbf{r}_{\ell}^{\mathsf{T}}$ or $\mathbf{t}^{\mathsf{T}} = \mathbf{d}_{\ell}^{\mathsf{T}}$, the algorithm \mathcal{B}_2 works as follow:

Setup. Sample

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (k+1)}, \ \mathbf{k} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}, \ \mathbf{c} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}, \ \alpha \leftarrow \mathbb{Z}_p,$$
$$\{\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(k+1) \times (k+1)}, \ \mathbf{r}_i \leftarrow \mathbb{Z}_p^{1 \times k}\}_{i \in [L]}.$$

Output

$$\operatorname{crs} = \begin{pmatrix} [\mathbf{A}\mathbf{k}^{\mathsf{T}}]_{T}[\mathbf{A}]_{1}, \{[\mathbf{A}\mathbf{V}_{i}]_{1}\}_{i\in[L]}, \{[\mathbf{V}_{i}\mathbf{B}\mathbf{r}_{j}^{\mathsf{T}}]_{2}\}_{j\in[L],i\in[L]\setminus\{j\}}, \\ \{[\mathbf{B}\mathbf{r}_{i}^{\mathsf{T}}, \mathbf{V}_{i}\mathbf{B}\mathbf{r}_{i}^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}} + \alpha \mathbf{c}^{\perp}]_{2}\}_{i<\ell}, \begin{bmatrix} [\mathbf{t}_{\ell}, \mathbf{V}_{\ell}\mathbf{t}_{\ell}^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_{2}, \\ \{[\mathbf{B}\mathbf{r}_{i}^{\mathsf{T}}, \mathbf{V}_{i}\mathbf{B}\mathbf{r}_{i}^{\mathsf{T}} + \mathbf{k}^{\mathsf{T}}]_{2}\}_{i>\ell} \end{pmatrix}$$

Query. Here, for all $i \in [L]$ and each $(pk_i, sk_i) \in \mathcal{D}_i$ is generated honestly as:

- if $i \neq \ell$, the pk_i is that

 $([\mathbf{A}\mathbf{U}_i]_1, \{[\mathbf{U}_i\mathbf{B}\mathbf{r}_i^{\mathsf{T}}]_2\}_{j\in[L]\setminus\{i,\ell\}}, [\mathbf{U}_i\mathbf{t}^{\mathsf{T}}]_2);$

- if $i = \ell$, the pk_{ℓ} is that

$$([\mathbf{A}\mathbf{U}_{\ell}]_1, \{[\mathbf{U}_{\ell}\mathbf{B}\mathbf{r}_j^{\mathsf{T}}]_2\}_{j\in[L]\setminus\{\ell\}}).$$

where $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1) \times (k+1)}$.

Challenge. On input challenge m*, output ct* as

$$\mathsf{ct}^* = \left([\mathbf{c}]_1, \left[\sum_{j \in [L]} (\mathbf{c} \mathbf{V}_j + \mathbf{c} \mathbf{U}_j) \right]_1, [\mathbf{c} \mathbf{k}^{\mathsf{T}}]_T \cdot \mathsf{m}^* \right).$$

Observe that when $\mathbf{t}^{\mathsf{T}} = \mathbf{B}\mathbf{r}_{\ell}^{\mathsf{T}}$, the simulation is identical to $\mathsf{Game}_{2,\ell-1,3}$; when $\mathbf{t}^{\mathsf{T}} = \mathbf{d}_{\ell}^{\mathsf{T}}$, the simulation is identical to $\mathsf{Game}_{2,\ell,1}$.

Lemma 3 (Game_{2, $\ell,1$} \approx_s Game_{2, $\ell,2$}). For any efficient adversary \mathcal{A} , there exists algorithm \mathcal{B}_3 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}_{\mathcal{A}}^{2,\ell,1}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2,\ell,2}(\lambda)| \le \mathsf{negl}(\lambda).$$

Proof. Here, it only considers honest case, then we have $Game_{2,\ell,1} \approx_s Game_{2,\ell,2}$ by the following argument:

$$\begin{cases} \mathbf{A}, \mathbf{B}_{\ell}, \mathbf{c}^{\perp}, \mathbf{d}_{\ell}^{\mathsf{T}}, \mathbf{AV}_{\ell}, \mathbf{V}_{\ell} \mathbf{B}, \mathbf{V}_{\ell} \mathbf{d}_{\ell}^{\mathsf{T}} + b\mathbf{c}^{\perp}\alpha; & //crs \\ \mathbf{AU}_{\ell}; \quad \mathbf{c}, \mathbf{cV}_{\ell} + \mathbf{cU}_{\ell} & //pk_{i}; ct^{*} \\ \approx_{s} \begin{cases} \mathbf{A}, \mathbf{B}_{\ell}, \mathbf{c}^{\perp}, \mathbf{d}_{\ell}^{\mathsf{T}}, \mathbf{AV}_{\ell}, \mathbf{V}_{\ell} \mathbf{B}, \mathbf{V}_{\ell} \mathbf{d}_{\ell}^{\mathsf{T}} + v_{\ell} \mathbf{c}^{\perp} + b\mathbf{c}^{\perp}\alpha; \\ \mathbf{AU}_{\ell}; \quad \mathbf{c}, \mathbf{cV}_{\ell} + \mathbf{cU}_{\ell} + v_{\ell} \mathbf{c}^{\perp} + u_{\ell} \mathbf{c}^{\perp} \\ \approx_{s} \begin{cases} \mathbf{A}, \mathbf{B}_{\ell}, \mathbf{c}^{\perp}, \mathbf{d}_{\ell}^{\mathsf{T}}, \mathbf{AV}_{\ell}, \mathbf{V}_{\ell} \mathbf{B}, \mathbf{V}_{\ell} \mathbf{d}_{\ell}^{\mathsf{T}} + v_{\ell} \mathbf{c}^{\perp} + b\mathbf{c}^{\perp}\alpha; \\ \mathbf{AU}_{\ell}; \quad \mathbf{c}, \mathbf{cV}_{\ell} + \mathbf{cU}_{\ell} + v_{\ell} \mathbf{c}^{\perp} + u_{\ell} \mathbf{c}^{\perp} \end{cases} \end{cases}$$

where $b \in \{0, 1\}$. Here, we have

– The first \approx_s follows that:

 $\mathbf{V}_{\ell} \mapsto \mathbf{V}_{\ell} + \mathbf{c}^{\perp} v_{\ell} \mathbf{d}^{\perp}$ and $\mathbf{U}_{\ell} \mapsto \mathbf{U}_{\ell} + \mathbf{c}^{\perp} u_{\ell} \mathbf{d}^{\perp}$

where $\mathbf{c}^{\perp} \in \mathbb{Z}_p^{k+1}$ and $\mathbf{d}^{\perp} \in \mathbb{Z}_p^{1 \times (k+1)}$ such that $\mathbf{A}\mathbf{c}^{\perp} = 0$, $\mathbf{c}\mathbf{c}^{\perp} = 1$, $\mathbf{d}^{\perp}\mathbf{B} = 0$, $\mathbf{d}^{\perp}\mathbf{d}_{\ell} = 1$.

- The second \approx_s holds by the fact that v_ℓ in crs also seems to be sampled randomly because u_ℓ hides extra v_ℓ in challenge ciphertext.

This readily proves the lemma.

4 Lattice-Based Global Slotted RBE

In this section, we give a global slotted RBE construction based on function-binding hash function (relying on LWE assumption) [FWW23] and witness encryption (relying on evasive LWE assumption) [Wee22]. This construction is adapted from slotted RABE (with a public randomized aggregation procedure) in [FWW23]. Concretely, we initially construct a global slotted RBE construction that achieves adaptive security subject to the restriction that adversary does not make any corruption queries. Then we use the "two-key" technology [GW09] to remove this restriction and obtain a global slotted RBE that achieves the adaptive security (as defined in Section 2) in the random oracle.

4.1 Construction without Corruption

Assume a public key encryption PKE = (Setup, Enc, Dec) with all parameters of size $poly(\lambda)$, a function-binding hash function FBH = (Setup, Hash, Open, Ver) with block size $m_{in} = \lambda + \log L$ [FWW23], and a witness encryption WE = (Enc, Dec) for a NP language \mathcal{L} with witness relation \mathcal{R} [VWW22,Tsa22] defined as follows:

$$\mathcal{R}((\mathsf{hk},\mathsf{pk},\mathsf{dig}),(i,\mathsf{ct},r,\pi)) = 1$$

$$\Leftrightarrow \mathsf{ct} = \mathsf{PKE}.\mathsf{Enc}(\mathsf{pk},1;r) \land \mathsf{FBH}.\mathsf{Ver}(\mathsf{hk},\mathsf{dig},\{i\},\{(i,(i,\mathsf{ct}))\},\pi) = 1$$

our construction is as follows:

- Setup $(1^{\lambda}, 1^{L})$: Run (pk, sk) \leftarrow PKE.Setup (1^{λ}) and hk \leftarrow FBH.Setup $(1^{\lambda}, L)$, and output the common reference string crs = (pk, hk).
- Gen(crs, *i*) : Parse crs = (pk, hk). Sample $r \leftarrow \{0, 1\}^{\lambda}$ and run ct \leftarrow PKE.Enc(pk, 1; *r*), then output pk_i = ct and sk_i = *r*.
- Ver(crs, i, pk_i) : Check whether pk_i is a valid ciphertext of PKE. If so, output 1; otherwise, output 0.
- Agg(crs, $\{i, pk_i\}_{i \in [L]}$) : Parse crs = (pk, hk). Then run

dig
$$\leftarrow$$
 FBH.Hash(hk, ((1, pk₁), ..., (L, pk_L))),
 $\pi_i \leftarrow$ FBH.Open(hk, ((1, pk₁), ..., (L, pk_L)), {i}), $\forall i = 1, ..., L$.

Output the master public key mpk = (crs, dig) and the helper secret key hsk_i = (j, π_i , pk_i) for all $j \in [L]$.

- Enc(mpk, m) : Parse mpk = ((pk, hk), dig). Output the ciphertext

ct ← WE.Enc
$$(1^{\lambda}, (hk, pk, dig), m).$$

- Dec(hsk_{*i**}, sk_{*i**}, ct) : Parse hsk_{*i**} = (i^* , π_{i^*} , pk_{*i**}). Output

m = WE.Dec(ct,
$$(i^*, pk_{i^*}, sk_{i^*}, \pi_{i^*}))$$
.

Optimal Compactness and Unbounded Users. Note that $|crs| = |pk| + |hk| = poly(\lambda, \log L)$, $|mpk| = |crs| + |dig| = poly(\lambda, \log L)$, $|hsk_j| = |j| + |\pi_j| + |pk_j| = poly(\lambda, \log L)$, and the runtime for algorithms PKE.Enc and FBH.Ver are at most poly(λ , log L), so above construction supports optimal compactness and unbounded users.

Correctness. For all $\lambda, L \in \mathbb{N}$, all C, and all $i^* \in [L]$, all crs \leftarrow Setup $(1^{\lambda}, 1^L, C)$ where crs = (pk, hk), all (pk_{i*}, sk_{i*}) \leftarrow Gen(crs, i^*), all {pk_i}_{i \in [L] \{i*}} such that Ver(crs, i, pk_i) = 1, and all message m, we have mpk = (crs, dig) and hsk_{i*} = $(i^*, \pi_{i^*}, pk_{i^*})$, where

dig
$$\leftarrow$$
 FBH.Hash(hk, ((1, pk₁), ..., (*L*, pk_{*L*}))),
 $\pi_{i^*} \leftarrow$ FBH.Open(hk, ((1, pk₁), ..., (*L*, pk_{*L*})), {*i*^{*}}).

Then the ciphertext is computed as

 $ct \leftarrow WE.Enc(1^{\lambda}, (hk, pk, dig), m).$

For decryption, we state that $hsk_{i^*} = (i^*, \pi_{i^*}, pk_{i^*})$ along with sk_{i^*} is a valid witness for the statement (hk, pk, dig), because $pk_{i^*} = PKE.Enc(pk, 1; sk_{i^*})$, and FBH.Ver(hk, dig, $\{i^*\}, \{(i^*, (i^*, pk_{i^*}))\}, \pi_{i^*}) = 1$ by the completeness of FBH. Thus, by the correctness of witness encryption, we have

WE.Dec(ct,
$$(i^*, pk_{i^*}, sk_{i^*}, \pi_{i^*})) = m_i$$

4.2 Security

Theorem 2. Assume PKE = (Setup, Enc, Dec) is a public key encryption with semantic security, FBH = (Setup, Hash, Open, Ver) is a function-binding hash function with function hiding and function bind properties, and WE = (Enc, Dec) is a secure witness encryption, our global slotted RBE achieves the adaptive IND security without corruption.

Game Sequence. We prove Theorem 2 via a sequence of games as follows:

- H₀: Real Game.
- H_1 : this game is identical to H_0 except that for each query to oracle OGen(crs, *i*) where crs = (pk, hk), the challenger generates (pk_i, sk_i) as follows:

$$pk_i = PKE.Enc(pk, 0; r), sk_i = r$$

where $r \leftarrow \{0, 1\}^{\lambda}$. We can prove $H_0 \approx_c H_1$ via Lemma 4.

- H₂: this game is identical to H₁ except that we replace FBH.Setup $(1^{\lambda}, 1^{L})$ with FBH.SetupBind $(1^{\lambda}, 1^{L}, f_{g})$. Here, the function f_{g} is defined as

$$f_g((1, \operatorname{ct}_1), \ldots, (L, \operatorname{ct}_L)) = \bigvee_{i \in [L]} g(i, \operatorname{ct}_i),$$

where

$$g(i, \mathsf{ct}_i) = \begin{cases} 1, \text{ when PKE.Dec}(\mathsf{sk}, \mathsf{ct}_i) = 1, \\ 0, \text{ otherwise.} \end{cases}$$

sk is the secret key corresponding to public key pk of PKE. We can prove H₁ \approx_c H₂ via Lemma 5.

- H₃: this game is identical to H₂ except that the challenge ciphertext is defined as

$$\mathsf{ct}^* \leftarrow \mathsf{WE}.\mathsf{Enc}(1^\lambda, (\mathsf{hk}, \mathsf{pk}, \mathsf{dig}), \mathsf{m}^*),$$

where m^{*} is a random message. This can be proved via Lemma 6.

Lemma 4 (H₀ \approx_c H₁). For any adversary \mathcal{A} , there exists algorithm \mathcal{B}_1 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}^{0}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{1}_{\mathcal{A}}(\lambda)| \leq q \cdot \mathsf{Adv}^{\mathsf{PKE}}_{\mathcal{B}_{1}}(\lambda) + \mathsf{negl}(\lambda).$$

where q is the bound of the number of quires to oracle OGen.

Proof. The proof follows the semantic security of public-key encryption PKE. Roughly speaking, since the adversary has no idea about the secret key sk, the challenger is able to change all ciphertexts in a one-by-one fashion, without raising any doubt. Here, we omit details.

Lemma 5 ($H_1 \approx_c H_2$). For any adversary \mathcal{A} , there exists algorithm \mathcal{B}_2 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}^{1}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{2}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{FBH-CFH}}_{\mathcal{B}_{2}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. The proof follows the computational function hiding property of FBH. The challenger can replace algorithm FBH.Setup with FBH.SetupBind without raising any doubt.

Lemma 6 (H₂ \approx_c H₃). For any adversary \mathcal{A} , there exists algorithm \mathcal{B}_3 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}^{1}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{2}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{WE}}_{\mathcal{B}_{3}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. The proof follows the security of witness encrytion WE and the statistical function binding property of FBH. Recall the witness relation \mathcal{R} :

$$\mathcal{R}((\mathsf{hk},\mathsf{pk},\mathsf{dig}),(i,\mathsf{ct},r,\pi)) = 1$$

$$\Leftrightarrow \mathsf{ct} = \mathsf{PKE}.\mathsf{Enc}(\mathsf{pk},1;r) \land \mathsf{FBH}.\mathsf{Ver}(\mathsf{hk},\mathsf{dig},\{i\},\{(i,(i,\mathsf{ct}))\},\pi) = 1$$

If some witness (i, ct, r, π) corresponding to instance (hk, pk, dig), it must hold that PKE.Dec $(sk, \mathsf{ct}) = 1$, then we have $f_g((1, \mathsf{ct}_1), \ldots, (L, \mathsf{ct}_L)) = 1$. However, since $g(i, \mathsf{ct}_i) = 0$ for all $i \in [L]$ in H₂, it means $f_g((1, \mathsf{ct}_1), \ldots, (L, \mathsf{ct}_L)) = 0$. Combining with statistical function binding property, it is clear that adversary is able to pass the relation \mathcal{R} with only negligible probability. Therefore, the challenger can exploit the security of WE to replace the challenge ciphertext ct^{*} \leftarrow WE.Enc $(1^{\lambda}, (hk, pk, dig), m_b)$ with ct^{*} \leftarrow WE.Enc $(1^{\lambda}, (hk, pk, dig), m^*)$.

4.3 Final Construction

Assume a hash function $H : \{0, 1\}^* \to \{0, 1\}^L$ that can be modeled as random oracle, a global slotted RBE without corruption gsRBE_{wc} = (Setup, Gen, Ver, Agg, Enc, Dec) that all parameters are of size poly(λ), our final construction is as follows:

- Setup $(1^{\lambda}, 1^{L})$: Run crs \leftarrow gsRBE_{wc}.Setup (1^{λ}) and output the common reference string crs.
- Gen(crs, *i*) : Sample two pairs of public key and secret

 $(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{gsRBE}_{wc}.\mathsf{Gen}(\mathsf{crs}, i), \ (\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{gsRBE}_{wc}.\mathsf{Gen}(\mathsf{crs}, i).$

Then sample a random bit $\beta \leftarrow \{0, 1\}$ and $s \leftarrow \{0, 1\}^{\lambda}$, output $pk_i = (pk_0, pk_1, s), sk_i = (\beta, sk_{\beta})$.

- Ver(crs, *i*, pk_i) : Parse pk_i = (pk_{i,0}, pk_{i,1}, s_i). If both pk_{i,0} and pk_{i,1} pass the check of algorithm gsRBE_{wc}.Ver, and $s_i \in \{0, 1\}^{\lambda}$, output 1; otherwise, output 0.
- Agg(crs, $\{i, \mathsf{pk}_i\}_{i \in [L]}$) : Parse $\mathsf{pk}_i = (\mathsf{pk}_{i,0}, \mathsf{pk}_{i,1}, s_i)$. Compute $(h_1, \ldots, h_L) \leftarrow \mathsf{H}(\mathsf{crs}, (1, \mathsf{pk}_1), \ldots, (L, \mathsf{pk}_L))$ and let $\overline{h}_i = 1 h_i$ for all $i \in [L]$. Then run

$$\begin{aligned} (\mathsf{mpk}_0, \{\mathsf{hsk}_{j,0}\}_{j \in [L]}) &\leftarrow \mathsf{gsRBE}_{\mathsf{wc}}.\mathsf{Agg}(\mathsf{crs}, ((1, \mathsf{pk}_{1,h_1}), \dots, (L, \mathsf{pk}_{L,h_L}))), \\ (\mathsf{mpk}_1, \{\mathsf{hsk}_{j,1}\}_{j \in [L]}) &\leftarrow \mathsf{gsRBE}_{\mathsf{wc}}.\mathsf{Agg}(\mathsf{crs}, ((1, \mathsf{pk}_{1,\overline{h_1}}), \dots, (L, \mathsf{pk}_{L,\overline{h_L}}))). \end{aligned}$$

Output the master public key mpk = (mpk_0, mpk_1) and the helper secret key $hsk_j = (h_j, hsk_{j,0}, hsk_{j,1})$ for all $j \in [L]$.

- Enc(mpk, m) : Parse mpk = (mpk_0, mpk_1) , output ct = (ct_0, ct_1) , where $ct_0 \leftarrow gsRBE_{wc}$. $Enc(mpk_0, m)$ and $ct_1 \leftarrow gsRBE_{wc}$. $Enc(mpk_1, m)$.
- Dec(hsk_{i*}, sk_{i*}, ct) : Parse hsk_{i*} = (h_{i*} , hsk_{i*,0}, hsk_{i*,1}), sk_{i*} = (β_{i*} , sk_{β_{i*}}) and ct = (ct₀, ct₁). If $\beta_{i*} = h_{i*}$, output m = gsRBE_{wc}.Dec(hsk_{i*,0}, sk_{i*, β_{i*}}, ct₀); otherwise, output m = gsRBE_{wc}.Dec(hsk_{i*,1}, sk_{i*, β_{i*}}, ct₁).

Optimal Compactness and Unbounded Users. Note that the final construction consists of two instances for $gsRBE_{wc}$, so it will meet optimal compactness (resp., unbounded users) as long as $gsRBE_{wc}$ meets optimal compactness (resp., unbounded users).

Correctness. Informally, the public key $pk_{i^*,\beta_{i^*}}$ corresponding to secret key $sk_{i^*,\beta_{i^*}}$ is either registered into mpk_0 (when $\beta_{i^*} = h_{i^*}$) or mpk_1 (when $\beta_{i^*} = \overline{h_{i^*}}$), then it can recover message m properly following the correctness of $gsRBE_{wc}$.

As for security, this construction achieves the adaptive IND security in random oracle model and it allows the query to corruption oracle OCor. The proof strategy is analogous to [FWW23]. The difference lies on the fact that we do not require any challenge policy, so our construction is naturally adaptively IND secure.

Finally, we obtain an *Q*-bound slotted RFE for circuits via the compiler in Section 5 and Section 6, and we can modify the compiler to achieve unbounded users by eliminating all $\{\widehat{pk}_{i,w,b}\}$ of crs and just setting $\overline{pk}_{i,w,b} = pk_{i,w,b}$ only when $C_i[w] = b$. Here, due to the good traits of FBH, algorithm sRBE.Agg still works as usual when the number of registered public keys is less than *L*.

5 1-Bound Slotted RFE for Circuits

With global slotted RBE, we present a slotted RFE scheme for circuits with adaptive 1-bound SIM security.

5.1 Construction

For some circuit family $C : X \to Z$, let $U(\cdot, \cdot)$ be the universal circuit such that U(C, x) = C(x) for any circuit $C \in C$ and input $x \in X$. Assume a garbled circuit scheme GC = (Garble, Eval) where *n* is the input length of the circuit, and a global slotted registered broadcast encryption gsRBE = (Setup, Gen, Ver, Agg, Enc, Dec), then our 1-bound slotted RFE for circuits (set Q = 1 as default) works as follows:

- Setup $(1^{\lambda}, 1^{L}, C)$: Run gsRBE.Setup $(1^{\lambda}, 1^{L})$ 2*n* times and obtain $\{\operatorname{crs}_{w,b}\}_{w \in [n], b \in \{0,1\}}$. For all $w \in [n]$ and $b \in \{0, 1\}$, run gsRBE.Gen $(\operatorname{crs}_{w,b}, i)$ for all $i \in [L]$, omit secret keys and obtain valid public keys $\{\widehat{\mathsf{pk}}_{i,w,b}\}_{i \in [L], w \in [n], b \in \{0,1\}}$. Output

$$crs = ({crs_{w,b}}_{w \in [n], b \in \{0,1\}}, {pk_{i,w,b}}_{i \in [L], w \in [n], b \in \{0,1\}}).$$

- Gen(crs, *i*) : For all $w \in [n]$ and $b \in \{0, 1\}$, run $(\mathsf{pk}_{i,w,b}, \mathsf{sk}_{i,w,b}) \leftarrow \mathsf{gsRBE}.\mathsf{Gen}(\mathsf{crs}_{w,b}, i)$. Output

 $\mathsf{pk}_i = (\{\mathsf{pk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}}), \ \mathsf{sk}_i = (\{\mathsf{sk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}}).$

- Ver(crs, *i*, pk_{*i*}) : For all $w \in [n]$ and $b \in \{0, 1\}$, run $\beta_{w,b} \leftarrow gsRBE.Ver(crs_{w,b}, i, pk_{i,w,b})$, and if $\beta_{w,b} = 0$, output 0 and abort. Otherwise, output 1.
- Agg(crs, { $\mathsf{pk}_i, \mathsf{C}_i$ }_{$i \in [L]$}) : Parse $\mathsf{C}_i = (\mathsf{C}_i[1], \dots, \mathsf{C}_i[n]) \in \{0, 1\}^n$ and $\mathsf{pk}_i = (\{\mathsf{pk}_{i,w,b}\}_{w \in [n], b \in \{0, 1\}})$. For all $i \in [L]$ and all $w \in [n], b \in \{0, 1\}$, set

$$\overline{\mathsf{pk}}_{i,w,b} := \begin{cases} \mathsf{pk}_{i,w,b}, \text{ when } \mathsf{C}_i[w] = b, \\ \widehat{\mathsf{pk}}_{i,w,b}, \text{ otherwise.} \end{cases}$$

Then run $(\mathsf{mpk}_{w,b}, \{\mathsf{hsk}_{j,w,b}\}_{j \in [L]}) \leftarrow \mathsf{gsRBE}.\mathsf{Agg}(\mathsf{crs}_{w,b}, \{i, \overline{\mathsf{pk}}_{i,w,b}\}_{i \in [L]})$. Output

$$mpk = (\{mpk_{w,b}\}_{w \in [n], b \in \{0,1\}}), \ hsk_j = (C_j, \{hsk_{j,w,b}\}_{w \in [n], b \in \{0,1\}}).$$

- Enc(mpk, x): Let U[x] be the universal circuit with x hard-wired. Run

$$(\tilde{\mathsf{U}}, \{\mathsf{lab}_{w,b}\}_{w \in [n], b \in \{0,1\}}) \leftarrow \mathsf{GC}.\mathsf{Garble}(1^{\lambda}, \mathsf{U}[x]).$$

For all $w \in [n], b \in \{0, 1\}$, run

$$ct_{w,b} \leftarrow gsRBE.Enc(mpk_{w,b}, lab_{w,b}).$$

Output ct = $(\tilde{U}, \{ct_{w,b}\}_{w \in [n], b \in \{0,1\}}).$

- Dec(hsk_i*, sk_i*, ct) : Parse hsk_i* = (C_i*, {hsk_i*, w, b}_{w \in [n], b \in \{0,1\}) and sk_i* = ({sk_i*, w, b}_{w \in [n], b \in \{0,1\}). For all $w \in [n]$, let $b_w = C_{i^*}[w]$ and run}}

$$\mathsf{m}_{w,b_w} \leftarrow \mathsf{gsRBE}.\mathsf{Dec}(\mathsf{hsk}_{i^*,w,b_w},\mathsf{sk}_{i^*,w,b_w},\mathsf{ct}_{w,b_w}).$$

Thus, we output

$$z \leftarrow \text{GC.Eval}(\tilde{U}, \{\mathsf{m}_{w,b_w}\}_{w \in [n]}).$$

Remark. The above generic construction can be instantiated by any global slotted RBE scheme, but it does not support unbounded users, i.e., crs not scaling with *L*. Indeed, if we adopt the construction in Section 4, we can improve it into the one supporting unbounded users by removing all public keys $\{\widehat{pk}_{i,w,b}\}$ in algorithm Setup and directly letting $\overline{pk}_{i,w,b} = pk_{i,w,b}$ when $C_i[w] = b$.

Completeness and Compactness. For completeness, it follows the underlying slotted RBE. In other words, if slotted RBE in above construction meets completeness, then it holds that

$$\Pr\left[\mathsf{gsRBE}.\mathsf{Ver}(\mathsf{crs}_{w,b}, i, \mathsf{pk}_i) = 1\right] = 1$$

for all $w \in [n]$ and all $b \in \{0, 1\}$. Thus, the completeness of our construction follows readily.

For compactness, thanks to the optimal compactness of gsRBE, our 1-bound slotted RFE scheme has the following properties:

$$|mpk| = 2n \cdot poly(\lambda, \log L), |hsk_i| = 2n \cdot poly(\lambda, \log L)$$

where *n* is related to circuit family *C*. Thus, our construction meets the compactness requirement.

Correctness. For all $\lambda, L \in \mathbb{N}$, all C, and all $i^* \in [L]$, all crs \leftarrow Setup $(1^{\lambda}, 1^L, C)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i \in [L] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, all $x \in X$ and $\mathsf{C}_1, \ldots, \mathsf{C}_L \in C$, we have $\mathsf{sk}_{i^*} = (\{\mathsf{sk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}})$ and

$$ct = \left(\tilde{U}, \left(\begin{array}{c} gsRBE.Enc(mpk_{1,0}, lab_{1,0}) \cdots gsRBE.Enc(mpk_{n,0}, lab_{n,0}) \\ gsRBE.Enc(mpk_{1,1}, lab_{1,1}) \cdots gsRBE.Enc(mpk_{n,1}, lab_{n,1}) \end{array} \right) \right)$$

Here, each mpk_{*w*,*b*} is generated from $\{i, \overline{\mathsf{pk}}_{i,w,b}\}_{i \in [L]}$. Note that in algorithm Enc, we have

$$\overline{\mathsf{pk}}_{i,w,b} := \begin{cases} \mathsf{pk}_{i,w,b}, \text{ when } \mathsf{C}_i[w] = b, \\ \widehat{\mathsf{pk}}_{i,w,b}, \text{ otherwise.} \end{cases}$$

Here, $sk_{i^*,w,b}$ is the secret key of $\overline{pk}_{i^*,w,b}$ only when $C_{i^*}[w] = b$. Thus, after computing all $m_{w,b}$, nothing else can be obtained except for $\{lab_{i^*,w,b_w}\}_{w \in [n]}$. Then it follows the correctness of garbled circuits to compute $z = U(C_{i^*}, x) = C_{i^*}(x)$. Therefore, the correctness follows readily.

5.2 Security

Theorem 3. Assume GC = (Garble, Eval) is a secure garbled circuits scheme and gsRBE = (Setup, Gen, Ver, Agg, Enc, Dec) is a global slotted RBE scheme with optimal compactness which achieves the IND security defined in Section 2.3, our construction achieves the 1-bound SIM security defined in Section 2.4.

Proof. let C^{*} be the circuit corresponding to the unique corrupted user. Just as the security analysis presented in Section 1.2, our proof strategy follows the security of underlying global slotted RBE and garbled circuits. Concretely, we randomize all labels $\{\widetilde{lab}_{w,1-C^*[w]}\}_{w\in[n]}$ one by one (from $Game_{1,\kappa-1}$ to $Game_{1,\kappa}$), via the IND security of global slotted RBE. Then we can simulate rest labels (from $Game_{1,n}$ to $Game_2$) via the security of garbled circuits. In final game, the challenge ciphertext will only disclose C^{*}(x^{*}) and nothing else. Here, we define the simulator Enc that works as follows:

- $\widetilde{\text{Enc}}(\text{mpk}, (i^*, \mathsf{C}^*, \mathsf{C}^*(x^*), \mathsf{sk}_{i^*}))$: Parse mpk = $(\{\text{mpk}_{w,b}\}_{w \in [n], b \in \{0,1\}})$. Run

$$\tilde{\mathsf{C}}^*, \{\widetilde{\mathsf{lab}}_{w,\mathsf{C}^*[w]}\}_{w\in[n]}\} \leftarrow \widetilde{\mathsf{Garble}}(1^{\lambda},\mathsf{C}^*(x)).$$

Then sample $\widetilde{\mathsf{lab}}_{w,1-C^*[w]} \leftarrow \{0,1\}^{\lambda}$ for all $w \in [n]$. Set

$$ct^{*} = \left(\tilde{C}^{*}, \begin{pmatrix} ct_{1,0}^{*} \cdots ct_{n,0}^{*} \\ ct_{1,1}^{*} \cdots ct_{n,1}^{*} \end{pmatrix}\right)$$
$$= \left(\tilde{C}^{*}, \begin{pmatrix} gsRBE.Enc(mpk_{1,0}, \widetilde{lab}_{1,0}) \cdots gsRBE.Enc(mpk_{n,0}, \widetilde{lab}_{n,0}) \\ gsRBE.Enc(mpk_{1,1}, \widetilde{lab}_{1,1}) \cdots gsRBE.Enc(mpk_{n,1}, \widetilde{lab}_{n,1}) \end{pmatrix}\right)$$

The algorithm \widetilde{Enc} actually does not need sk_i, so our resulting construction can resist single malicious user.

Game Sequence. We prove Theorem 3 via a sequence of games as follows:

- Game₀: this game is identical to the real experiment of adaptive 1-SIM security. Recall that
 - crs has the form:

$$\operatorname{crs} = (\{\operatorname{crs}_{w,b}\}_{w \in [n], b \in \{0,1\}}, \{\widehat{\mathsf{pk}}_{i,w,b}\}_{i \in [L], w \in [n], b \in \{0,1\}}).$$

where $crs_{w,b}$ and $\widehat{pk}_{i,w,b}$ are generated from the underlying slotted RBE algorithms gsRBE.Setup and gsRBE.Gen, respectively.

• For each $i \in [L]$, (pk_i, sk_i) are in the form:

$$\mathsf{pk}_i = (\{\mathsf{pk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}}), \ \mathsf{sk}_i = (\{\mathsf{sk}_{i,w,b}\}_{w \in [n], b \in \{0,1\}}).$$

where $(pk_{i,w,b}, sk_{i,w,b})$ are sampled from algorithm gsRBE.Gen.

• The master public key mpk and helper secret key hsk_i has the form

$$\mathsf{mpk} = \begin{pmatrix} \mathsf{mpk}_{1,0} \cdots \mathsf{mpk}_{n,0} \\ \mathsf{mpk}_{1,1} \cdots \mathsf{mpk}_{n,1} \end{pmatrix}, \ \mathsf{hsk}_j = \begin{pmatrix} \mathsf{C}_j, \begin{pmatrix} \mathsf{hsk}_{j,1,0} \cdots \mathsf{hsk}_{j,n,0} \\ \mathsf{hsk}_{j,1,1} \cdots \mathsf{hsk}_{j,n,1} \end{pmatrix} \end{pmatrix},$$

where for each $w \in [n], b \in \{0, 1\}$, mpk_{*w*,*b*} is computed as

$$\overline{\mathsf{pk}}_{i,w,b} := \begin{cases} \mathsf{pk}_{i,w,b}, \text{ when } \mathsf{C}_i[w] = b\\ \widehat{\mathsf{pk}}_{i,w,b}, \text{ otherwise.} \end{cases}$$

Then obtain $(\mathsf{mpk}_{w,b}, \{\mathsf{hsk}_{j,w,b}\}_{j \in [L]}) \leftarrow \mathsf{gsRBE}.\mathsf{Agg}(\mathsf{crs}_{w,b}, \{i, \overline{\mathsf{pk}}_{i,w,b}\}_{i \in [L]}).$

• The challenge ciphertext ct* has the form

$$\begin{aligned} \mathsf{ct}^* &= \left(\tilde{\mathsf{U}}, \begin{pmatrix} \mathsf{ct}_{1,0}^* \cdots \mathsf{ct}_{n,0}^* \\ \mathsf{ct}_{1,1}^* \cdots \mathsf{ct}_{n,1}^* \end{pmatrix} \right) \\ &= \left(\tilde{\mathsf{U}}, \begin{pmatrix} \mathsf{gsRBE.Enc}(\mathsf{mpk}_{1,0}, \mathsf{lab}_{1,0}) \cdots \mathsf{gsRBE.Enc}(\mathsf{mpk}_{n,0}, \mathsf{lab}_{n,0}) \\ \mathsf{gsRBE.Enc}(\mathsf{mpk}_{1,1}, \mathsf{lab}_{1,1}) \cdots \mathsf{gsRBE.Enc}(\mathsf{mpk}_{n,1}, \mathsf{lab}_{n,1}) \end{pmatrix} \right), \end{aligned}$$

where $(\tilde{U}, \{ \mathsf{lab}_{w,b} \}_{w \in [n], b \in \{0,1\}}) \leftarrow \mathsf{GC.Garble}(1^{\lambda}, \mathsf{U}[x^*]).$

- Game_{1. κ} ($\kappa \in [n]$): Game_{1. κ} is identical to Game₀ except that for each $w \leq \kappa$, set $b_w = C^*[w]$ and $\overline{b}_w = 1 - C^*[w]$, we have

$$\begin{aligned} \mathsf{ct}^*_{w,b_w} &\leftarrow \mathsf{gsRBE}.\mathsf{Enc}(\mathsf{mpk}_{w,b_w},s_{w,b_w},\mathsf{lab}_{w,b_w}),\\ \mathsf{ct}^*_{w,\overline{b}_w} &\leftarrow \mathsf{gsRBE}.\mathsf{Enc}(\mathsf{mpk}_{w,\overline{b}_w},s_{w,\overline{b}_w},\overline{\mathsf{lab}}_{w,\overline{b}_w}), \end{aligned}$$

where $\widetilde{lab}_{w,\overline{b}_w}$ is randomly sampled from $\{0,1\}^{\lambda}$.

 Game₂: this game is identical to Game_{1,n} except that it replaces Enc with Enc to generate the challenge ciphertext ct*.

Lemma 7 (Game_{1, κ -1} \approx_c Game_{1, κ}). For any efficient adversary \mathcal{A} , there exists an algorithm \mathcal{B}_1 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}_{\mathcal{A}}^{1,\kappa-1}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{1,\kappa}(\lambda)| \leq 2 \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{gsRBE}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. Initially, \mathcal{B}_1 receives upper bound *L* from \mathcal{A} . Then \mathcal{B}_1 flips a coin $\beta \leftarrow \{0, 1\}$ and sends *L* to the challenger of gsRBE. Then \mathcal{B}_1 proceeds following phases:

Setup. After receiving the $\operatorname{crs}_{\kappa,\beta}$ from the challenger of gsRBE, initialize 2n - 1 slotted RBE instances by itself, and obtain $\{\operatorname{crs}_{w,b}\}_{w \in [n], b \in \{0,1\}}$. For all $w \in [n]$ and all $b \in \{0,1\}$, if $w = \kappa$ and $b = \beta$, query the oracle OGen(i) of gsRBE to obtain $\widehat{\operatorname{pk}}_{i,\kappa,\beta}$ for all $i \in [L]$; otherwise, run gsRBE.Gen $(\operatorname{crs}_{w,b}, i)$ by itself for all $i \in [L]$. Then omit all secret keys and obtain public keys $\{\widehat{\operatorname{pk}}_{i,w,b}\}_{i \in [L], w \in [n], b \in \{0,1\}}$. Output

 $\operatorname{crs} = (\{\operatorname{crs}_{w,b}\}_{w \in [n], b \in \{0,1\}}, \{\widehat{\mathsf{pk}}_{i,w,b}\}_{i \in [L], w \in [n], b \in \{0,1\}}).$

Query. Here, \mathcal{A} can query oracles as below:

- OGen(*i*) : For all $w \in [n]$ and all $b \in \{0, 1\}$, if $w = \kappa$ and $b = \beta$, query the oracle OGen(*i*) of gsRBE to obtain $pk_{i,\kappa,\beta}$; otherwise, run $(pk_{i,w,b}, sk_{i,w,b}) \leftarrow gsRBE.Gen(crs_{w,b}, i)$ by itself. Output $pk = (\{pk_{i,w,b}\}_{w \in [n], b \in \{0,1\}})$ and set $\mathcal{D}_i[pk] = \{sk_{i,w,b}\}_{w \in [n] \setminus \{\kappa\}, b \in \{0,1\}} \cup \{sk_{i,\kappa,1-\beta}\}.$
- − OCor(*i*, pk) : Parse pk = ({pk_{*i*,*w*,*b*}}_{*w*∈[*n*],*b*∈{0,1}}). Query the oracle OCor(*i*, pk_{*κ*,*β*}) of gsRBE to obtain sk_{*i*,*κ*,*β*}. Then return $\mathcal{D}_i[pk] \cup \{sk_{i,\kappa,\beta}\}$. Update $C = C \cup \{(i, pk)\}$.}
- **Challenge.** \mathcal{B}_1 receives challenge public keys $\{pk_i^*\}_{i \in [L]}$ where $pk_i^* = \{pk_{i,w,b}^*\}_{w \in [n], b \in \{0,1\}}$. Combining with challenge circuits $\{C_i^*\}_{i \in [L]}$, we assume that the unique corrupted user registering the circuit $C^* \in \{C_i^*\}_{i \in [L]}$, and C^* is linked to the public key $pk^* \in \{pk_i^*\}_{i \in [L]}$. If $C^*[\kappa] = \beta$, then abort the experiment immediately; otherwise, it means that all public keys that has registered in gsRBE are not corrupted. Thus, for all $i \in [L]$ and all $w \in [n], b \in \{0, 1\}$, set

$$\overline{\mathsf{pk}}_{i,w,b} := \begin{cases} \mathsf{pk}_{i,w,b}^*, \text{ when } \mathsf{C}_i[w] = b, \\ \widehat{\mathsf{pk}}_{i,w,b}, \text{ otherwise.} \end{cases}$$

After that, run (\tilde{U} , {lab_{*w*,*b*}}_{*w*\in[*n*],*b*\in{0,1}}) \leftarrow GC.Garble(1^{λ}, U[*x*^{*}]) and for each *w* $\leq \kappa$, pick lab_{*w*,1-C^{*}[*w*]} \leftarrow {0, 1}^{λ}. For all *w* \in [*n*], *b* \in {0, 1}, if *w* = κ and *b* = β , send ({*i*, $\overline{\mathsf{pk}}_{i,\kappa,\beta}$ }_{*i*\in[*L*]}, lab_{*\karkallem,\beta\)}) to the challenger, and obtain (mpk_{<i>\karkallem,\beta\)*}, {hsk_{*j*,*w*,*b*}}_{*j*\in[*L*]}) \leftarrow gsRBE.Agg(crs_{*w*,*b*}, {*i*, $\overline{\mathsf{pk}}_{i,w,b}$ }_{*i*\in[*L*]}). Set}</sub>

$$mpk = (\{mpk_{w,b}\}_{w \in [n], b \in \{0,1\}}), \ hsk_j = (C_j^*, \{hsk_{j,w,b}\}_{w \in [n], b \in \{0,1\}}).$$

Then \mathcal{B}_1 receives the challenge ciphertext $\mathsf{ct}^*_{\kappa,\beta}$ and computes other $\mathsf{ct}^*_{w,b}$ as follows:

$$ct_{w,b}^* = \begin{cases} gsRBE.Enc(mpk_{w,b}, \widetilde{lab}_{w,b}), & when w < \kappa \land C^*[w] = 1 - b, \\ gsRBE.Enc(mpk_{w,b}, lab_{w,b}), & otherwise. \end{cases}$$

Finally, return the challenge ciphertext

$$\mathsf{ct}^* = \left(\tilde{\mathsf{U}}, \, \begin{pmatrix} \mathsf{ct}_{1,0}^* \cdots \mathsf{ct}_{n,0}^* \\ \mathsf{ct}_{1,1}^* \cdots \mathsf{ct}_{n,1}^* \end{pmatrix} \right).$$

Observe that if $ct^*_{\kappa,\beta}$ is generated under message $\widetilde{lab}_{\kappa,\beta}$, \mathcal{B}_1 simulates $Game_{1,\kappa}$; otherwise, it simulates $Game_{1,\kappa-1}$. Thus, this readily proves the lemma.

Lemma 8 (Game_{1,n} \approx_c Game₂). For any efficient adversary \mathcal{A} , there exists an algorithm \mathcal{B}_2 with close running time to \mathcal{A} such that

$$|\mathsf{Adv}_{\mathcal{A}}^{1,n}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_{2}}^{\mathsf{GC}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. The only difference between $Game_{1,n}$ and $Game_2$ is the generation of ct*. Obviously, if the underlying garbled circuits scheme is secure, the output of algorithm Enc in $Game_{1,n}$ is indistinguishable from the output of algorithm Enc in $Game_2$ from the view of \mathcal{A} .

Analysis for Honest and Corrupt Cases. Without loss of generality, we assume that all challenge circuits are different from each other. Let C^{*} be the corrupted circuit for slot *i*^{*}. For some honest slot *i*, there must exist at least a different bit (assume index w') between C^{*}_i and C^{*}. In this way, even if \mathcal{A} owns the secret key of slot *i*^{*}, it will only obtain $\{\overline{lab}_{w,C^*_i[w]}\}_{w\in[n]\setminus\{w'\}} \cup \{\overline{lab}_{w',C^*_i[w']}\}$. Here, $\{\overline{lab}_{w,C^*_i[w]}\}_{w\in[n]\setminus\{w'\}}$ are simulated using 1^{λ} and C^{*}(x^{*}), while $\overline{lab}_{w',C^*_i[w']}$ is a random string independent from other labels. According to the privacy of garbled circuits, \mathcal{A} cannot extract any useful information about $C^*_i(x^*)$.

For corrupt case, \mathcal{A} can only obtain $(\tilde{C}^*, \{\tilde{lab}_{w,C^*[w]}\}_{w \in [n]})$ that are simulated using just 1^{λ} and $C^*(x^*)$. Thus, only $C^*(x^*)$ is revealed. At last, the proof of Theorem 3 is completed.

6 Q-Bound Slotted RFE for Circuits

In this section, we roughly follow the approach of [GVW12] in order to upgrade the construction in Section 5 from 1bound security to *Q*-bound security. Here, we only present an *Q*-bound secure RFE for NC1 circuits because it can be trivially bootstrapped into RFE for all polynomial-sized circuits using computational randomized encodings [AIK06]. With slotted RFE for circuits, we can convert it into a full-fledged RFE construction via "power-of-two" approach (presented in the full version).

6.1 Construction

Let C := NC1 be a circuit family with circuits of degree D and size n. Our construction is additionally parameterized with S, N, t and v. For any circuit $C \in C$ and set $\Delta \subseteq [S]$, we define a new circuit $G \in G$ takes as input $\mathbf{x} = (x, r_1, ..., r_S)$ as follows:

$$G(\mathbf{x}) = C(x) + \sum_{j \in \Delta} r_j.$$
 (1)

Assume a 1-bound slotted registered function encryption osRFE = (Setup, Gen, Ver, Agg, Enc, Dec), our *Q*-bound slotted RFE for circuit family *C* works as follows:

- Setup $(1^{\lambda}, 1^{L}, 1^{Q}, C)$: Initialize *N* 1-bound slotted RFE instances by running osRFE.Setup $(1^{\lambda}, 1^{L}, G)$ for *N* times, and obtain {crs_k}_{k \in [N]}. Output

$$\operatorname{crs} = (\{\operatorname{crs}_k\}_{k \in [N]}).$$

- Gen(crs, *i*) : Parse crs = ({crs_k}_{k \in [N]}), then it proceeds as follows:

• Sample uniformly random set $\Gamma_i \subseteq [N]$ of size tD + 1 and random set $\Delta_i \subseteq [S]$ of size v, where Δ_i can be translated into a bit string δ_i of length $v \log S$. Set $n' = n + v \log S$;

• For all $k \in [N]$, run $(pk_{k,i}, sk_{k,i}) \leftarrow osRFE.Gen(crs_k, i)$. Here, based on the construction presented in Section 5, for each $k \in [N]$, we have $pk_{k,i} = (\{pk_{k,i,w,b}\}_{w \in [n'], b \in \{0,1\}})$ and $sk_{k,i} = (\{sk_{k,i,w,b}\}_{w \in [n'], b \in \{0,1\}})$, where $(pk_{k,i,w,b}, sk_{k,i,w,b})$ are sampled from the key-generation algorithm of global slotted RBE. Then omit secret keys $sk_{k,i}$ for all $k \notin \Gamma_i$, and for all $k \in \Gamma_i$, update

$$\mathsf{sk}_{k,i} = (\{\mathsf{sk}_{k,i,w,b}\}_{w \le n} \cup \{\mathsf{sk}_{k,i,w,\delta_i[w]}\}_{w > n}).$$

Output

$$\mathsf{pk}_i = (\{\mathsf{pk}_{k,i}\}_{k \in [N]}), \ \mathsf{sk}_i = (\{\mathsf{sk}_{k,i}\}_{k \in \Gamma_i}, \Gamma_i, \Delta_i).$$

- Ver(crs, *i*, pk_i) : For all $k \in [N]$, run $\beta_k \leftarrow \text{osRFE.Ver}(\text{crs}_k, i, \text{pk}_{k,i})$, and if $\beta_k = 0$, output 0 and abort; otherwise, output 1.
- Agg(crs, {pk_i, C_i}_{i \in [L]}) : Parse pk_i = ({pk_{k,i}}_{k \in [N]}) for each $i \in [L]$. For all $k \in [N]$, run (mpk_k, {hsk_{k,j}}_{j \in [L]}) \leftarrow osRFE.Agg(crs_k, {pk_{k,i}, G_i}_{i \in [L]}), where G_i is defined as in (1) given constant C_i and Δ_i . Here, algorithm osRFE.Agg works as in construction 5.1 except that all submitted public keys associated with Δ_i are directly registered into {mpk_k}_{k \in [N]} to ensure the cover freeness. Then output

$$mpk = (\{mpk_k\}_{k \in [N]}), hsk_j = (\{hsk_{k,j}\}_{k \in [N]})$$

- Enc(mpk, *x*) : It proceeds as follows:
 - Sample a random degree *t* polynomial $\mu(\cdot)$ whose constant term is *x*;
 - For all $j \in [S]$, sample a random degree *Dt* polynomial $\zeta_i(\cdot)$ whose constant term is 0;
 - For all $k \in [N]$, compute $\mathbf{x}_k = (\mu(k), \zeta_1(k), \dots, \zeta_S(k))$ and run $ct_k \leftarrow osRFE.Enc(mpk_k, \mathbf{x}_k)$. Then output

$$ct = (ct_1, \ldots, ct_N).$$

- $\text{Dec}(\text{hsk}_{i^*}, \text{sk}_{i^*}, \text{ct})$: Parse $\text{hsk}_{i^*} = (\{\text{hsk}_{k,i^*}\}_{k \in [N]}), \text{sk}_{i^*} = (\{\text{sk}_{k,i^*}\}_{k \in \Gamma_{i^*}}, \Gamma_{i^*}, \Delta_{i^*}).$ For all $k \in \Gamma_{i^*}$, run

$$z_k \leftarrow \text{osRFE.Dec}(\text{hsk}_{k,i^*}, \text{sk}_{k,i^*}, \text{ct}_k).$$

Then use $\{z_k\}_{k \in \Gamma_{i^*}}$ to recover a degree *Dt* polynomial $\psi(\cdot)$ such that $\psi(k) = z_k$. Output $\psi(0)$.

Remark. For the range of parameters *S*, *N*, *t* and *v*, we let $v = O(\lambda)$. Suppose there are *Q* corrupted users whose slot numbers are collected in set $\{c_1, \ldots, c_Q\} \subseteq [L]$, then we set $t = O(Q^2\lambda)$ and $N = O(D^2Q^2t)$ to ensure small pairwise intersections [GVW12]. In other words, for all $\Gamma_{c_1}, \ldots, \Gamma_{c_Q}$, it holds that

$$\Pr\left[\left|\bigcup_{i\neq j}(\Gamma_{c_i}\cap\Gamma_{c_j})\right|>t\right]\leq \operatorname{negl}(\lambda).$$

Besides, we set $S = O(Q^2 v)$ to ensure cover freeness [GVW12]. In other words, for all $\Delta_{c_1}, \ldots, \Delta_{c_Q}$ and all $i \in [Q]$, it holds that

$$\Pr\left[\Delta_{c_i} \setminus \left(\bigcup_{j \neq i} \Delta_{c_j}\right) = \emptyset\right] \le \operatorname{negl}(\lambda).$$

On the other hand, we can trivially bootstrap above construction into RFE for all polynomial-sized circuits instead of NC1 circuits. For any polynomial-sized circuit C_i , this can be done by modifying the definition of circuit G_i into generating a randomized encoding of C_i that is computable by a constant-degree circuit with fresh randomness generated from weak pseudo-random function. Here, we omit more details and only discuss the NC1 case. **Completeness and Compactness.** For completeness, it follows the underlying 1-bound slotted RFE. For compactness, combining the compactness analysis of osRFE, it holds that

$$|mpk| = N \cdot 2n \cdot poly(\lambda, \log L), |hsk_j| = N \cdot 2n \cdot poly(\lambda, \log L)$$

where *N* depends on the corruption bound *Q*, and *n* is related to circuit family *C*. Thus, our construction meets the compactness requirement.

Correctness. By the correctness of underlying 1-bound slotted RFE, for all $k \in \Gamma_{i^*}$ we have

$$\psi(k) = \mathsf{G}_{i^*}(\mathbf{x}_k) = \mathsf{C}_{i^*}(\mu(k)) + \sum_{j \in \Delta_{i^*}} \zeta_j(k).$$

Since $|\Gamma_{i^*}| = Dt + 1$, we can recover the polynomial $\psi(\cdot)$ of degree Dt, and then evaluate $\psi(0) = C_{i^*}(\mu(0)) = C_{i^*}(x)$. Indeed, above computation exactly corresponds to BGW MPC protocol [WOG88]. Therefore, the correctness follows readily.

6.2 Security

Theorem 4. Assume osRFE = (Setup, Gen, Ver, Agg, Enc, Dec) is a slotted RFE scheme which achieves the 1-bound SIM security, the above construction achieves the Q-bound SIM security.

Proof. Our proof strategy is analogous to [GVW12]. Suppose the adversary \mathcal{A} colludes with Q corrupted users whose slot indices are collected in set $\{c_1, \ldots, c_Q\} \subseteq [L]$. Let \mathcal{T} denote the set $\bigcup_{i \neq j} (\Gamma_{c_i} \cap \Gamma_{c_j})$, and note that \mathcal{A} has no idea about other $\Gamma_i \notin \{\Gamma_{c_1}, \ldots, \Gamma_{c_Q}\}$ under honest slots. With challenge ciphertext $ct^* = (ct_1^*, \ldots, ct_N^*)$ and secret key $\mathsf{sk}_i = (\{\mathsf{sk}_{k,i}\}_{k \in \Gamma_i}, \Gamma_i, \Delta_i)$ for $k \in [N]$, then the proof strategy is organized as follows:

- If $k \notin \mathcal{T}$, it means there exists at most a set Γ_{c_i} such that $k \in \Gamma_{c_i}$ and $k \notin \Gamma_{c_j}$ for other *j*. In particular, ct_k^* can be just decrypted correctly by a corrupted user with slot *i*. Thus, it can rely on the 1-bound SIM security of underlying construction;
- Otherwise, it means that A holds more than one secret keys that are used to decrypt ct^{*}_k correctly. In this way, 1-bound SIM security would be broken, and the security would in turn rely on the underlying MPC protocol. In this case, A will obtain no valid information about the challenge message x* as long as small pairwise intersections and cover freeness hold.

Then we define the simulator \widetilde{Enc} that works as follows:

- $\widetilde{\mathsf{Enc}}(\mathsf{mpk},\mathcal{K})$: Parse $\mathcal{K} = \{(c_i, \mathsf{C}^*_{c_i}, \mathsf{C}^*_{c_i}, \mathsf{sk}_{c_i})\}_{i \in [Q]}$. Here, we obtain $\Gamma_{c_1}, \ldots, \Gamma_{c_Q}, \Delta_{c_1}, \ldots, \Delta_{c_Q}$ from sk_i . Then it proceeds as follows:
 - Sample a uniformly random degree *t* polynomial $\mu(\cdot)$ whose constant term is 0;
 - For all $j \in [Q]$, fix some $a_j^* \in \Delta_{c_j} \setminus (\bigcup_{j \neq k} \Delta_{c_k})$ based on the cover freeness. For other $a \in (\Delta_{c_1} \cup \cdots \cup \Delta_{c_Q}) \setminus \{a_j^*\}_{j \in [Q]}$, sample a uniformly random degree Dt polynomial $\zeta_a(\cdot)$ whose constant term is 0. For all $j \in [Q]$, pick a random degree Dt polynomial $\psi_{c_j}(\cdot)$ whose constant term is $C_{c_j}(x^*)$ and adjust the evaluation of $\zeta_{a_j^*}$ such that for all $k \in \mathcal{T}$, we have

$$\psi_{c_j}(k) = \mathsf{C}_{c_j}(\mu(k)) + \sum_{a \in \Delta_{c_i}} \zeta_a(k).$$

• For all $k \notin \mathcal{T}$, suppose there is at most a set Γ_{c_i} such that $k \in \Gamma_{c_i}$ and $k \notin \Gamma_{c_j}$ for all $j \neq i$, then we simulate ct_k^* as follows:

$$\mathsf{ct}_{k}^{*} \leftarrow \mathsf{osRFE}.\widetilde{\mathsf{Enc}}(\mathsf{mpk}_{k}, (c_{i}, \mathsf{G}_{c_{i}}, \psi_{c_{i}}(k), \mathsf{sk}_{c_{i}}))$$

• For all $k \in \mathcal{T}$, we generate ct_k^* as in real experiment:

$$\mathsf{ct}_k^* \leftarrow \mathsf{osRFE}.\mathsf{Enc}(\mathsf{mpk}_k, (\mu(k), \zeta_1(k), \dots, \zeta_S(k))).$$

Finally, output

$$\mathsf{ct}^* = (\mathsf{ct}_1^*, \dots, \mathsf{ct}_N^*).$$

Game Sequence. We prove Theorem 4 via a sequence of games as follows:

- Game₀: Real Game.
- Game₁: this game is identical to Game₀ except that it samples $\zeta_1, \ldots, \zeta_S, \psi_1, \ldots, \psi_Q$ as in Enc and simulates all $\{\mathsf{ct}_k^*\}_{k\notin \mathcal{T}}$ as in algorithm Enc.
- Game₂: this game is identical to Game₁ except that it replaces Enc with Enc to generate the challenge ciphertext ct*.

Lemma 9 (Game₀ \approx_c Game₁). For any adversary \mathcal{A} , there exists an algorithm \mathcal{B} with close running time to \mathcal{A} such that

$$|\mathsf{Adv}^{0}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{1}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{osRFE}}_{\mathcal{B}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. Informally, thanks to cover freeness, we observe that the distribution of $\zeta_1, \ldots, \zeta_S, \psi_1, \ldots, \psi_Q$ in Enc are essentially identical to those in Enc, and then we can follow the 1-bound SIM security of underlying slotted RFE scheme to simulate all $\{ct_k^*\}_{k\notin T}$ as in Enc. Thus, it holds that $Game_0$ is computationally indistinguishable from $Game_1$.

Lemma 10 (Game₁ \approx_s Game₂). For any adversary \mathcal{A} , we have

$$|\operatorname{Adv}_{\mathcal{A}}^{1}(\lambda) - \operatorname{Adv}_{\mathcal{A}}^{2}(\lambda)| \leq \operatorname{negl}(\lambda).$$

Proof. The only difference between Game₁ and Game₂ is the distributions of μ . We claim that the distributions of $\{\mu(k)\}_{k\in\mathcal{T}}$ in Game₁ are essentially identical to those in Game₂ as long as small pairwise intersections holds, i.e., $|\mathcal{T}| \leq t$. Thus, this readily proves the lemma.

Acknowledgements. Thank Yin Zhu for his useful advice. We also thank all anonymous reviewers for their helpful comments. This work was supported in part by National Natural Science Foundation of China (62372180, 62325209, U2336203), Innovation Program of Shanghai Municipal Education Commission (2021-01-07-00-08-E00101), the "Digital Silk Road" Shanghai International Joint Lab of Trustworthy Intelligent Software (22510750100), the Australian Research Council Discovery Early Career Researcher Award DE240100282, the Major Program (JD) of Hubei Province (No. 2023BAA027), and the Key Research and Development Science and Technology of Hainan Province (GHYF2022010).

References

- ABG19. Michel Abdalla, Fabrice Benhamouda, and Romain Gay. From single-input to multi-client inner-product functional encryption. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 552–582. Springer, Heidelberg, December 2019. 8
- ABKW19. Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner. Decentralizing inner-product functional encryption. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 128–157. Springer, Heidelberg, April 2019. 8

- ACF⁺20. Shweta Agrawal, Michael Clear, Ophir Frieder, Sanjam Garg, Adam O'Neill, and Justin Thaler. Ad hoc multi-input functional encryption. In Thomas Vidick, editor, *ITCS 2020*, volume 151, pages 40:1–40:41. LIPIcs, January 2020. 8
- AFNV19. Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi. Match me if you can: Matchmaking encryption and its applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 701–731. Springer, Heidelberg, August 2019. 2
- AGT21. Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-party functional encryption. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part II*, volume 13043 of *LNCS*, pages 224–255. Springer, Heidelberg, November 2021. 8
- AIK06. Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Computationally private randomizing polynomials and their applications. *computational complexity*, 15(2):115–162, 2006. 24
- AJ15. Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 308–326. Springer, Heidelberg, August 2015. 2
- ALS16. Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 333–362. Springer, Heidelberg, August 2016. 2
- AMVY21. Shweta Agrawal, Monosij Maitra, Narasimha Sai Vempati, and Shota Yamada. Functional encryption for turing machines with dynamic bounded collusion from LWE. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part IV*, volume 12828 of *LNCS*, pages 239–269, Virtual Event, August 2021. Springer, Heidelberg. 7
- AR17. Shweta Agrawal and Alon Rosen. Functional encryption for bounded collusions, revisited. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 173–205. Springer, Heidelberg, November 2017. 2
- ATY23. Shweta Agrawal, Junichi Tomida, and Anshu Yadav. Attribute-based multi-input fe (and more) for attribute-weighted sums. In *Annual International Cryptology Conference*, pages 464–497. Springer, 2023. 8
- AV19. Prabhanjan Ananth and Vinod Vaikuntanathan. Optimal bounded-collusion secure functional encryption. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 174–198. Springer, Heidelberg, December 2019. 2, 7
- AW17. Shashank Agrawal and David J. Wu. Functional encryption: Deterministic to randomized functions from simple assumptions. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 30–61. Springer, Heidelberg, April / May 2017. 2
- BHR12. Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In Ting Yu, George Danezis, and Virgil D. Gligor, editors, *ACM CCS 2012*, pages 784–796. ACM Press, October 2012. 4, 8
- BLM⁺24. Pedro Branco, Russell WF Lai, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, and Ivy KY Woo. Traitor tracing without trusted authority from registered functional encryption. *Cryptology ePrint Archive*, 2024. 2, 3, 6, 7
- BSW11. Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Heidelberg, March 2011. 1, 2
- BV15.Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In Venkatesan
Guruswami, editor, 56th FOCS, pages 171–190. IEEE Computer Society Press, October 2015. 2
- CDG⁺18. Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. Decentralized multiclient functional encryption for inner product. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 703–732. Springer, Heidelberg, December 2018. 8
- CDSG⁺20. Jérémy Chotard, Edouard Dufour-Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. Dynamic decentralized functional encryption. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 747–775. Springer, Heidelberg, August 2020. 8
- CGJS15. Nishanth Chandran, Vipul Goyal, Aayush Jain, and Amit Sahai. Functional encryption: Decentralised and delegatable. Cryptology ePrint Archive, Report 2015/1017, 2015. https://eprint.iacr.org/2015/1017. 8
- DKL⁺23. Nico Döttling, Dimitris Kolonelos, Russell WF Lai, Chuanwei Lin, Giulio Malavolta, and Ahmadreza Rahimi. Efficient laconic cryptography from learning with errors. In *Annual International Conference on the Theory and Applications* of Cryptographic Techniques, pages 417–446. Springer, 2023. 2
- DP23. Pratish Datta and Tapas Pal. Registration-based functional encryption. *IACR Cryptol. ePrint Arch.*, 2023:457, 2023. 1, 2, 3, 34

- EHK⁺13. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013. 8
- FFM⁺23. Danilo Francati, Daniele Friolo, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, and Daniele Venturi. Registered (inner-product) functional encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 98–133. Springer, 2023. 1, 2, 3, 7, 34
- FWW23. Cody Freitag, Brent Waters, and David J Wu. How to use (plain) witness encryption: Registered abe, flexible broad-cast, and more. In *Annual International Cryptology Conference*, pages 498–531. Springer, 2023. 2, 4, 6, 7, 16, 17, 19, 31
- GGL24. Rachit Garg, Rishab Goyal, and George Lu. Dynamic collusion functional encryption and multi-authority attributebased encryption. In *IACR International Conference on Public-Key Cryptography*, pages 69–104. Springer, 2024. 7
- GGLW22. Rachit Garg, Rishab Goyal, George Lu, and Brent Waters. Dynamic collusion bounded functional encryption from identity-based encryption. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 736–763. Springer, Heidelberg, May / June 2022. 7
- GGSW13. Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In *Proceedings* of the forty-fifth annual ACM symposium on Theory of computing, pages 467–476, 2013. 32
- GHMR18. Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ahmadreza Rahimi. Registration-based encryption: Removing private-key generator from IBE. In Amos Beimel and Stefan Dziembowski, editors, TCC 2018, Part I, volume 11239 of LNCS, pages 689–718. Springer, Heidelberg, November 2018. 1
- GKMR23. Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, and Ahmadreza Rahimi. Efficient registration-based encryption. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, pages 1065–1079, 2023. 2
- GV20. Rishab Goyal and Satyanarayana Vusirikala. Verifiable registration-based encryption. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 621–651. Springer, Heidelberg, August 2020. 2
- GVW12. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption with bounded collusions via multi-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 162–179. Springer, Heidelberg, August 2012. 2, 4, 7, 24, 25, 26
- GW09. Craig Gentry and Brent Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 171–188. Springer, Heidelberg, April 2009. 6, 16
- HLWW23. Susan Hohenberger, George Lu, Brent Waters, and David J. Wu. Registered attribute-based encryption. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 511–542. Springer, Heidelberg, April 2023. 2, 3, 6, 7, 32, 34
- JLLW23. Aayush Jain, Huijia Lin, Ji Luo, and Daniel Wichs. The pseudorandom oracle model and ideal obfuscation. In *Annual International Cryptology Conference*, pages 233–262. Springer, 2023. 2
- KMW23. Dimitris Kolonelos, Giulio Malavolta, and Hoeteck Wee. Distributed broadcast encryption from bilinear groups. In International Conference on the Theory and Application of Cryptology and Information Security, pages 407–441. Springer, 2023. 6
- KW17. Sam Kim and David J. Wu. Access control encryption for general policies from standard assumptions. In Tsuyoshi Takagi and Thomas Peyrin, editors, ASIACRYPT 2017, Part I, volume 10624 of LNCS, pages 471–501. Springer, Heidelberg, December 2017. 2
- QWW18. Willy Quach, Hoeteck Wee, and Daniel Wichs. Laconic function evaluation and applications. In Mikkel Thorup, editor, *59th FOCS*, pages 859–870. IEEE Computer Society Press, October 2018. 7
- SS10. Amit Sahai and Hakan Seyalioglu. Worry-free encryption: functional encryption with public keys. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 2010*, pages 463–472. ACM Press, October 2010. 2, 4
- Tsa22. Rotem Tsabary. Candidate witness encryption from lattice techniques. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 535–559. Springer, Heidelberg, August 2022. 17

- VWW22. Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Witness encryption and null-IO from evasive LWE. In Shweta Agrawal and Dongdai Lin, editors, ASIACRYPT 2022, Part I, volume 13791 of LNCS, pages 195–221. Springer, Heidelberg, December 2022. 17
- Wee22. Hoeteck Wee. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 217–241. Springer, Heidelberg, May / June 2022. 3, 16
- WOG88. Avi Wigderson, MB Or, and S Goldwasser. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *Proceedings of the 20th Annual Symposium on the Theory of Computing (STOC'88)*, pages 1–10, 1988.
 26
- Yao86. Andrew Chi-Chih Yao. How to generate and exchange secrets. In 27th annual symposium on foundations of computer science (Sfcs 1986), pages 162–167. IEEE, 1986. 4, 8
- ZLZ⁺24. Ziqi Zhu, Jiangtao Li, Kai Zhang, Junqing Gong, and Haifeng Qian. Registered functional encryptions from pairings. In *EUROCRYPT*, 2024. 2, 3
- ZZGQ23. Ziqi Zhu, Kai Zhang, Junqing Gong, and Haifeng Qian. Registered abe via predicate encodings. In International Conference on the Theory and Application of Cryptology and Information Security, pages 66–97. Springer, 2023. 2, 4, 6,

7

Appendices

A Other Cryptographic Tools

A.1 Public-Key Encryption

Algorithms. A public-key encryption (PKE for short) scheme consists of three efficient algorithms as follows:

- Setup $(1^{\lambda}) \rightarrow (pk, sk)$. It takes as input security parameter 1^{λ} , outputs public key pk and secret key sk.
- Enc(pk, m; r) \rightarrow ct. It takes as input public key pk and a message m. Then sample randomness $r \leftarrow \{0, 1\}^{\lambda}$ to generate a ciphertext ct. Output ct;
- $Dec(sk, ct) \rightarrow m/\perp$. It takes as input secret key sk and ciphertext ct, outputs a message m or an empty symbol \perp .

Correctness. For all λ and all m, we have

$$Pr[Dec(sk, Enc(pk, m)) = m | (pk, sk) \leftarrow Setup(1^{\lambda})] = 1.$$

Semantic Security. For all λ and all efficient adversaries \mathcal{A} , the advantage

$$\Pr\left[b' = b \begin{vmatrix} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^{\lambda}) \\ (\mathfrak{m}_0^*, \mathfrak{m}_1^*) \leftarrow \mathcal{A}(1^{\lambda}, \mathsf{pk}) \\ b \leftarrow \{0, 1\}; \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathfrak{m}_b^*) \\ b' \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{vmatrix} - \frac{1}{2} \end{vmatrix}$$

is negligible in λ .

A.2 Function-Binding Hash Function

Algorithms. A function-binding hash function [FWW23] (FBH for short) consists of four efficient algorithms as follows:

- Setup $(1^{\lambda}, n) \rightarrow$ hk. It takes as input security parameter 1^{λ} and the bound of input block number *n*, then outputs a hash key hk where $|hk| = poly(\lambda, m_{in}, \log n)$. Here, $m_{in} = m_{in}(\lambda)$ is the size of the input block, and set digest size $d = d(\lambda)$ and opening size $p = p(\lambda)$.
- SetupBind $(1^{\lambda}, n, f) \rightarrow$ hk. It takes as input security parameter 1^{λ} , the number of input blocks n and a function $f: (\{0, 1\}^{m_{\text{in}}})^* \rightarrow \{0, 1\}^{m_{\text{out}}}$, then outputs a hash key hk. Here, $m_{\text{out}} = m_{\text{out}}(\lambda)$ is the size of function output and f is implementable by a circuit of size at most $s(\lambda) \cdot \text{poly}(k)$.
- Hash(hk, (blk₁,..., blk_k)) → dig. It takes as input the hash key hk and a sequence of input blocks (blk₁,..., blk_k) ∈ $(\{0, 1\}^{m_{in}})^k$ where $k \le n$, then deterministically outputs a digest dig $\in \{0, 1\}^d$.
- Open(hk, (blk₁,..., blk_k), S) → π . It takes as input the hash key hk, a sequence of input blocks (blk₁,..., blk_n) and a subset S ⊆ [k], then outputs an opening proof $\pi \in \{0, 1\}^p$.
- Ver(hk, dig, S, $\{(i, b|k_i)\}_{i \in S}, \pi) \rightarrow 0/1$. It takes as input hk, dig, S, $\{(i, b|k_i)\}_{i \in S}$ and π , then outputs a bit indicating whether it accepts or rejects.

Efficiency. For all λ , all n, k satisfying $k \leq n$, all f, all $hk \leftarrow \text{Setup}(1^{\lambda}, n)$, all tuple of inputs $(\text{blk}_1, \dots, \text{blk}_k) \in (\{0, 1\}^{m_{\text{in}}})^k$, all dig $\leftarrow \text{Hash}(hk, (\text{blk}_1, \dots, \text{blk}_k))$, all subset $S \subseteq [k]$ and all opening proof $\pi \leftarrow \text{Open}(hk, (\text{blk}_1, \dots, \text{blk}_k), S)$, it is required that

Time(Setup(
$$1^{\lambda}$$
, n)) = Time(SetupBind(1^{λ} , n , f)) = poly(λ , $s(\lambda)$, log n),
|dig| = poly(λ , $m_{out}(\lambda)$, log k), and $|\pi| = |S| \cdot poly(\lambda, m_{out}(\lambda), \log k)$.

Perfect Completeness. For all λ , all n, k satisfying $k \leq n$, and all input blocks $(blk_1, ..., blk_k) \in (\{0, 1\}^{m_{in}})^k$ and subset $S \subseteq [k]$, we have

$$\Pr\left[\operatorname{Ver}(\mathsf{hk}, \mathsf{dig}, \mathcal{S}, \{(i, \mathsf{blk}_i)\}_{i \in \mathcal{S}}, \pi) = 1 \middle| \begin{array}{l} \mathsf{hk} \leftarrow \operatorname{Setup}(1^{\lambda}, n) \\ \mathsf{dig} \leftarrow \operatorname{Hash}(\mathsf{hk}, (\mathsf{blk}_1, \dots, \mathsf{blk}_k)) \\ \pi \leftarrow \operatorname{Open}(\mathsf{hk}, (\mathsf{blk}_1, \dots, \mathsf{blk}_k), \mathcal{S}) \end{array} \right] = 1.$$

Computational Function Hiding. For all efficient adversaries \mathcal{A} , it is required that the advantage

$$\Pr\left[b' = b \begin{vmatrix} f \leftarrow \mathcal{R}(1^{\lambda}) \\ hk_0 \leftarrow \text{Setup}(1^{\lambda}, n) \\ hk_1 \leftarrow \text{SetupBind}(1^{\lambda}, n, f) \\ b \leftarrow \{0, 1\}; b' \leftarrow \mathcal{R}(hk_b) \end{vmatrix} - \frac{1}{2}\right]$$

is negligible in λ .

Statistical Function Binding. For all stateful unbounded adversaries \mathcal{A} , it is required that the advantage

$$\Pr \begin{bmatrix} (\exists \{(j, \mathsf{blk}_j^*)\}_{j \in [k] \setminus S}, \\ \text{s.t. } f(\mathsf{blk}_1^*, \dots, \mathsf{blk}_k^*) = f(\mathsf{blk}_1, \dots, \mathsf{blk}_k)) \\ \land (\mathsf{Ver}(\mathsf{hk}, \mathsf{dig}, S, \{(i, \mathsf{blk}_i^*)\}_{i \in S}, \pi) = 1) \end{bmatrix} \begin{bmatrix} f \leftarrow \mathcal{A}(1^\lambda) \\ \mathsf{hk} \leftarrow \mathsf{SetupBind}(1^\lambda, n, f) \\ (\{\mathsf{blk}_i\}_{i \in [k]}, S, \{(i, \mathsf{blk}_i^*)\}_{i \in S}, \pi) \leftarrow \mathcal{A}(\mathsf{hk}) \\ \mathsf{dig} \leftarrow \mathsf{Hash}(\mathsf{hk}, (\mathsf{blk}_1, \dots, \mathsf{blk}_k)) \end{bmatrix}$$

is negligible in λ .

A.3 Witness Encryption

Algorithms. A witness encryption [GGSW13] (WE for short) for a NP language \mathcal{L} with witness relation $\mathcal{R} : X \times W \rightarrow \{0, 1\}$ consists of four efficient algorithms as follows:

- $Enc(1^{\lambda}, x, m) \rightarrow ct$. It takes as input the security parameter 1^{λ} , an instance $x \in X$ for the language \mathcal{L} , and a message m, then outputs a ciphertext ct.
- Dec(ct, w) $\rightarrow m/\perp$. It takes as input a ciphertext ct and a witness $w \in W$, then outputs a message m or an empty symbol \perp .

Correctness. For all $\lambda \in \mathbb{N}$, all (x, w) such that x is a valid instance of L (namely $\mathcal{R}(x, w) = 1$) and all messages m, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{Enc}(1^{\lambda}, x, \mathsf{m}), w) = \mathsf{m}\right] = 1.$$

Security. For all $\lambda \in \mathbb{N}$ and all efficient adversaries \mathcal{A} , the security requires the advantage

$$\Pr\left[b' = b \begin{vmatrix} (x^*, \mathsf{m}_0^*, \mathsf{m}_1^*) \leftarrow \mathcal{A}(1^{\lambda}) \\ b \leftarrow \{0, 1\}; \mathsf{ct}^* \leftarrow \mathsf{Enc}(1^{\lambda}, x^*, \mathsf{m}_b^*); \\ b' \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{vmatrix} - \frac{1}{2}\right]$$

is negligible in λ when $x^* \in X$ is an invalid instance of language *L*.

B Q-Bound RFE for Circuits

We exploit the "power-of-two" approach from [HLWW23] to generically convert *Q*-bound slotted RFE to *Q*-bound RFE.

Construction. Suppose a full-fledged RFE mostly supports $L = 2^{\ell}$ users and endures $Q \ll L$ corrupted users, this approach needs $\ell + 1$ copies of slotted RFE with 1, 2, 4, \cdots , 2^{ℓ} slots. And the public state aux = $(\mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk})$ consists of the following terms:

- $\mathcal{D}_1[k, i] = (pk, y)$: where $k \in [0, \ell]$ and $i \in [2^k]$. This dictionary assigns a user's (pk, y) to the slot i of the 2^k -slotted RFE scheme.
- − $\mathcal{D}_2[k, n]$ = hsk: where $k \in [0, \ell]$ and $n \in [L]$. This dictionary assigns a hsk of slotted RFE to the 2^{*k*}-slotted RFE scheme and the user index *n*.
- − mpk = (ctr, mpk₀, · · · , mpk_ℓ) denotes the current master public key. Where {mpk_k}_{k∈[0,ℓ]} denote the master public keys of ℓ + 1 copies of slotted RFE, and ctr denotes the number of currently registered users. When no registered user, we initially set mpk = (0, ⊥, · · · , ⊥).

When no registered user, we initially set aux = $(\emptyset, \emptyset, \bot)$. Assuming a *Q*-bound slotted RFE for circuits sRFE = (Setup, Gen, Ver, Agg, Enc, Dec), a full-fledged RFE for circuits can be constructed as follows:

- Setup $(1^{\lambda}, 1^{L}, 1^{Q}, C)$: Compute $\ell = \log L$. For all $k \in [0, \ell]$, run crs_k \leftarrow sRFE.Setup $(1^{\lambda}, 1^{2^{k}}, 1^{\min(Q, 2^{k})}, C)$. Output

$$crs = (crs_0, \cdots, crs_\ell).$$

- Gen(crs, aux) : Fetch crs = {crs_k}_{k \in [0, ℓ]} and aux = ($\mathcal{D}_1, \mathcal{D}_2, mpk$), where mpk = (ctr, {mpk_k}_{k \in [0, ℓ]}). For all $k \in [0, \ell]$, compute}

$$i_k = (\operatorname{ctr} \operatorname{mod} 2^k) + 1$$

and run $(pk_k, sk_k) \leftarrow sRFE.Gen(crs_k, i_k)$. Set ctr' = ctr and output

$$\mathsf{pk} = (\mathsf{ctr}', \mathsf{pk}_0, \cdots, \mathsf{pk}_\ell)$$
 and $\mathsf{sk} = (\mathsf{ctr}', \mathsf{sk}_0, \cdots, \mathsf{sk}_\ell).$

- Reg(crs, aux, pk, C) : Fetch crs = {crs_k}_{k \in [0, \ell]}, aux = ($\mathcal{D}_1, \mathcal{D}_2, mpk$), and pk = (ctr', {pk_k}_{k \in [0, \ell]}), where mpk = (ctr, {mpk_k}_{k \in [0, \ell]}). For all $k \in [0, \ell]$, do the following operates:
 - Compute $i_k = (\text{ctr mod } 2^k) + 1;$
 - Check if sRFE.Ver(crs_k, i_k, pk_k) = 1 and ctr' = ctr. If the check passes, set ctr = ctr + 1, if the check fails, the algorithm halts and output (mpk, aux);
 - Update $\mathcal{D}_1[k, i_k] = (pk, C);$
 - If $i_k = 2^k$: compute $(\mathsf{mpk}'_k, \{\mathsf{hsk}_{k,j}\}_{j \in [2^k]}) \leftarrow \mathsf{sRFE}.\mathsf{Agg}(\mathsf{crs}_k, \{\mathcal{D}_1[k,i]\}_{i \in [2^k]})$. Update mpk'_k , and for all $j \in [2^k]$, update $\mathcal{D}_2[k, \mathsf{ctr} 2^k + j] = \mathsf{hsk}_{k,j}$.

Update the master public key mpk = (ctr, mpk₀, · · · , mpk_l) and aux = ($\mathcal{D}_1, \mathcal{D}_2, mpk$), output (mpk, aux).

- Upd(crs, aux, pk) : Fetch crs = {crs_k}_{k \in [0, \ell]}, aux = ($\mathcal{D}_1, \mathcal{D}_2, mpk$), and pk = (ctr', {pk_k}_{k \in [0, \ell]}), where mpk = (ctr, {mpk_k}_{k \in [0, \ell]}). Output

$$hsk = \begin{cases} \underbrace{(\mathcal{D}_2[0, ctr'+1], \cdots, \mathcal{D}_2[\ell, ctr'+1])}_{hsk_0} & \text{if } ctr' < ctr \\ \bot & \text{otherwise} \end{cases}$$
(2)

- Enc(mpk, x) : Fetch mpk = $(ctr, \{mpk_k\}_{k \in [0, \ell]})$. For all $k \in [0, \ell]$, compute:

$$ct_{k} = \begin{cases} sRFE.Enc(mpk_{k}, x) & \text{if } mpk_{k} \neq \bot \\ \bot & \text{otherwise} \end{cases}$$
(3)

Output $ct = (ctr, ct_0, \cdots, ct_\ell)$.

- Dec(hsk, sk, ct) : Fetch sk = $(ctr', \{sk_k\}_{k \in [0,\ell]})$, hsk = $\{hsk_k\}_{k \in [0,\ell]}$ and ct = $(ctr, \{ct_k\}_{k \in [0,\ell]})$. Proceed as follows:
 - If $ctr' \ge ctr$: output \perp ;
 - Otherwise, compute ctr = $(a_{\ell}, \dots, a_0)_2$ and ctr' = $(b_{\ell}, \dots, b_0)_2$. We denote k_d as the maximum $k \in [0, \ell]$ such that $a_k \neq b_k$. if mpk_{kd} $\neq \bot$ and hsk_{kd} = \bot , output getupd;
 - Otherwise, output sRFE.Dec(hsk_{k_d}, sk_{k_d}, ct).

Analysis. We would demonstrate the correctness, compactness, efficiency and security of the above construction via a series of theorems.

Theorem 5 (Correctness). Suppose construction sRFE is complete and perfectly correct. Then our construction is perfectly correct.

Proof. Similar to [HLWW23,FFM⁺23,DP23], we omit details here.

Theorem 6 (Compactness). Suppose construction sRFE is compact. Then our construction is compact.

Proof. Observe that $|mpk| = |ctr| + \sum_{i \in [0,\ell]} |mpk_i|$ and $|hsk| = \sum_{i \in [0,\ell]} |hsk_i|$, where ctr is a ℓ -bit number. According to the compactness of sRFE, we have $|mpk_i| = poly(\lambda, C, Q, \log L)$ and $|hsk_i| = poly(\lambda, C, Q, \log L)$ for all $i \in [0, \ell]$. Then it holds that $|mpk| = poly(\lambda, C, Q, \log i)$ and $|hsk| = poly(\lambda, C, Q, \log |\mathcal{R}|)$.

Theorem 7 (Update Efficiency). Suppose construction sRFE is compact. Then our construction meets update efficiency.

Proof. Observe that the number of invocations of Upd is at most $\ell + 1 = O(\log |\mathcal{R}|)$ and Upd is only invoked when one of $\{hsk_k\}_{k \in [0,\ell]}$ is \bot . Thus, the number of invocations of Upd in ODec is at most $O(\log |\mathcal{R}|)$.

On the other hand, $|hsk_k| = poly(\lambda, C, Q, log |\mathcal{R}|)$ for $k \in [0, \ell]$ according to the compactness of sRFE. Since aux maintains a dictionary \mathcal{D}_2 mapping each index slot index k to its set of helper decryption keys, each invocation of Upd runs in poly(log $|\mathcal{R}|$) time (in RAM model).

Theorem 8. Suppose construction sRFE meets the Q-bound SIM security. Then our construction meets the Q-bound SIM security.

Proof. Analogous to [HLWW23], suppose that there exists an adversary \mathcal{A} who breaks the *Q*-bound SIM security of sRFE with non-negligible advantage, we start by defining a sequence of hybrid experiments, each parameterized by an index $v \in [0, \ell]$:

- H_{ν} : This game is identical to the real experiment defined in Section 2.5, except that for the challenge ciphertext $ct^* = (ctr^*, ct^*_0, \dots, ct^*_{\ell})$, the first ν ciphertexts $\{ct^*_k\}_{k \in [0,\nu]}$ are simulated by $\widetilde{Enc}(mpk_k, \mathcal{K})$, while remaining ciphertexts $\{ct^*_k\}_{k \in [\nu+1,\ell]}$ are generated by $Enc(mpk_k, x^*)$. Here, \mathcal{K} is the set of all corrupted slot information in RFE. Concretely, this game proceeds as follows:

Setup. In this phase, \mathcal{A} proceeds as follows:

- \mathcal{A} chooses (L, Q) and send them to the challenger;
- The challenger samples $crs \leftarrow Setup(1^{\lambda}, 1^{L}, 1^{Q}, C);$
- Then it initializes a counter t = 0, master public key mpk = \perp and auxiliary input aux = $(\mathcal{D}_1, \mathcal{D}_2, \text{mpk})$ where $\mathcal{D}_1 = \emptyset, \mathcal{D}_2 = \emptyset$ and mpk = $(0, \perp, ..., \perp)$; Set $\mathcal{R} = \emptyset, C = \emptyset, S = \emptyset$ and a dictionary \mathcal{D} with $\mathcal{D}[pk] = \emptyset$ for all possible pk;
- Finally, it sends crs to \mathcal{A} .

Query. In the query phase, \mathcal{A} can make queries as follows:

- ORegHK(C): \mathcal{A} specifies a circuit C. The challenger sets $t \leftarrow t+1$ and samples $(pk_t, sk_t) \leftarrow Gen(crs, aux)$ and $(mpk', aux') \leftarrow Reg(crs, aux, pk_t, C)$. Then it updates mpk = mpk', aux = aux', $\mathcal{D}[pk_t] = \mathcal{D}[pk_t] \cup \{C\}$, append (pk_t, sk_t) to \mathcal{R} and return (t, mpk, aux, pk_t) ;
- OCorHK(i): A specifies an index i ∈ [t]. let R[i] = (pk, sk) and C = D[pk], append pk to C and return sk. This oracle can be queried at most Q times.

Challenge. In the challenge phase, \mathcal{A} submits the challenge message x^* . The challenger proceeds as follows:

- Let $aux = (ctr, \mathcal{D}_1, \mathcal{D}_2, mpk)$ where $mpk = (ctr, mpk_0, ..., mpk_{\ell})$;
- For each $k \in [0, \ell]$, if mpk_k =1, then set ctr_k =1; otherwise, if $k \le \nu$, compute ct^{*}_k $\leftarrow \operatorname{Enc}(\operatorname{mpk}_k, \mathcal{K})$, and if $k > \nu$, compute ct^{*}_k $\leftarrow \operatorname{Enc}(\operatorname{mpk}_k, x^*)$;
- The challenger replies to \mathcal{A} with $ct^* = (ctr, ct_0, \dots, ct_{\ell})$.

Lemma 11 ($H_{\nu-1} \approx_c H_{\nu}$). Suppose construction sRFE meets the Q-bound SIM security, For any adversary \mathcal{A} , there exists an algorithm \mathcal{B} with close running time to \mathcal{A} such that

$$|\mathsf{Adv}_{\mathcal{A}}^{\nu-1}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\nu}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{sRFE}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. The algorithm \mathcal{B} will simulated $H_{\nu-1}$ or H_{ν} as follows:

Setup. In this phase, \mathcal{B} proceeds as follows:

- When \mathcal{B} receives (L, Q) from \mathcal{A} , it sends $(2^{\nu}, \min(Q, 2^{\nu}))$ to the challenger of 2^{ν} -slotted RFE, then obtains crs_{ν};
- For each $k \in [0, \ell] \setminus \{\nu\}$, the challenger samples $\operatorname{crs}_k \leftarrow \operatorname{Setup}(1^{\lambda}, 1^{2^k}, 1^{\min(Q, 2^{\nu})}, C);$
- Then it initializes a counter t = 0, master public key mpk = \perp and auxiliary input aux = $(\mathcal{D}_1, \mathcal{D}_2, \text{mpk})$ where $\mathcal{D}_1 = \emptyset, \mathcal{D}_2 = \emptyset$ and mpk = $(0, \bot, ..., \bot)$; Set a dictionary \mathcal{D} with $\mathcal{D}[\text{pk}] = \emptyset$ for all possible pk. In addition, \mathcal{B} maintains a dictionary \mathcal{D}_s to track the secret keys associated with each ORegHK query, and initializes two ordered list $\mathcal{S}_1 = \bot, \mathcal{S}_2 = (\bot, ..., \bot)$ to track the public keys and circuits aggregated as part of mpk_v.
- Finally, it sends $crs = (crs_0, \ldots, crs_\ell)$ to \mathcal{A} .
- **Query.** In the query phase, \mathcal{B} can simulated queries \mathcal{A} makes as follows:
 - ORegHK(C): When \mathcal{A} specifies a circuit C, let ctr be the current counter in aux. For each $k \in [0, \ell]$, compute $i_k = (\operatorname{ctr} \mod 2^k) + 1$. Then generate $(\operatorname{pk}_k, \operatorname{sk}_k) \leftarrow \operatorname{sRFE.Gen}(\operatorname{crs}_k, i_k)$ for $k \neq \nu$. Next, \mathcal{B} makes a query i_{ν} to OGen(·), then obtain a public key pk_{ν} . It set $\operatorname{pk} = (\operatorname{ctr}, \operatorname{pk}_0, \dots, \operatorname{pk}_\ell)$. The challenger sets $t \leftarrow t + 1$ and $\mathcal{D}_s[t] = (\operatorname{ctr}, \{\operatorname{sk}_k\}_{k \in [0,\ell] \setminus \{\nu\}})$. Next, \mathcal{B} runs (mpk', aux') $\leftarrow \operatorname{Reg}(\operatorname{crs}, \operatorname{aux}, \operatorname{pk}_t, \mathbb{C})$ and updates mpk = mpk', aux = aux', $\mathcal{D}[\operatorname{pk}_t] = \mathcal{D}[\operatorname{pk}_t] \cup \{\mathsf{C}\}$, append ($\operatorname{pk}_t, \operatorname{sk}_t$) to \mathcal{R} and return (t, mpk, aux, pk_t). In addition, \mathcal{B} updates $\mathcal{S}_2[i_{\nu}] = (t, \mathsf{C})$. Moreover, if $i_{\nu} = 2^{\nu}$, \mathcal{B} set $\mathcal{S}_1 = \mathcal{S}_2$.
 - OCorHK(*i*): When \mathcal{A} specifies an index $i \in [t]$, \mathcal{B} looks up $\mathcal{D}_s[i] = (\mathsf{ctr}, \{\mathsf{sk}_k\}_{k \in [0,\ell] \setminus \{\nu\}})$. let $\mathcal{R}[i] = (\mathsf{pk}, \mathsf{sk})$, then it makes a corrupt query (i, pk) to $\mathsf{OCor}(\cdot, \cdot)$ and obtains sk_{ν} . Next, append pk to C, set $\mathcal{K} = \mathcal{K} \cup \{(i, \mathsf{C}, \mathsf{C}(x^*), \mathsf{sk})\}$ and return $\mathsf{sk}_{\nu} = (\mathsf{ctr}, \mathsf{sk}_0, \dots, \mathsf{sk}_\ell)$. This oracle can be queried at most Q times.
- **Challenge.** In the challenge phase, \mathcal{A} submits the challenge message x^* . Let mpk = (ctr, mpk_0, ..., mpk_ ℓ) be the current master public key. For each $k \in [0, \ell]$, \mathcal{B} proceeds as follows:
 - If $mpk_k = \perp$, then set $ct_k^* = \perp$;
 - If $mpk_k \neq \perp$ and $k < \nu$, then compute $ct_k^* \leftarrow \widetilde{Enc}(mpk_k, \mathcal{K})$;
 - If $mpk_k \neq \perp$ and k = v, \mathcal{B} makes a challenge query to obtain ct_v^* ;
 - If $mpk_k \neq \perp$ and k > v, then compute $ct_k^* \leftarrow Enc(mpk_k, x^*)$;
 - The challenger replies to \mathcal{A} with $ct^* = (ctr, ct_0^*, \dots, ct_{\ell}^*)$.

In above experiment, \mathcal{B} perfectly simulates an execution of Q-bound RFE against \mathcal{A} . Note that if $2^{\nu} \leq Q$, it means that all secret keys in z^{ν} -slotted RFE can be corrupted. This will not influence the simulation of ct_{ν}^{*} , since other corrupt secret keys are not registered in z^{ν} -slotted RFE, which means that adversary still owns at most 2^{ν} corrupted keys and then the simulation security of z^{ν} -slotted RFE will not be broken. Thus, in the case where $ct_{\nu}^{*} \leftarrow$ sRFE.Enc(mpk_{ν}, x^{*}), \mathcal{B} simulates H_{ν -1}, while in the case where $ct_{\nu}^{*} \leftarrow$ sRFE.Enc(mpk_{ν}, \mathcal{K}), \mathcal{B} simulates H_{ν}.