An Anonymous Trace-and-Revoke Broadcast Encryption Scheme

Olivier Blazy[1], Sayantan Mukherjee[1], Huyen Nguyen[2(✉)], Duong Hieu Phan[4], and Damien Stehlé[2,3]

[1] XLIM, University of Limoges, CNRS, Limoges, France
csayantan.mukherjee@gmail.com
[2] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France
huyen.nguyen@ens-lyon.fr
[3] Institut Universitaire de France, Paris, France
[4] LTCI, Telecom Paris, Institut Polytechnique de Paris, Paris, France

Abstract. Broadcast Encryption is a fundamental cryptographic primitive, that gives the ability to send a secure message to any chosen target set among registered users. In this work, we investigate broadcast encryption with anonymous revocation, in which ciphertexts do not reveal any information on which users have been revoked. We provide a scheme whose ciphertext size grows linearly with the number of revoked users. Moreover, our system also achieves traceability in the black-box confirmation model.

Technically, our contribution is threefold. First, we develop a generic transformation of linear functional encryption toward trace-and-revoke systems. It is inspired from the transformation by Agrawal *et al.* (CCS'17) with the novelty of achieving anonymity. Our second contribution is to instantiate the underlying linear functional encryptions from standard assumptions. We propose a DDH-based construction which does no longer require discrete logarithm evaluation during the decryption and thus significantly improves the performance compared to the DDH-based construction of Agrawal *et al.*. In the LWE-based setting, we tried to instantiate our construction by relying on the scheme from Wang *et al.* (PKC'19) but finally found an attack to this scheme. Our third contribution is to extend the 1-bit encryption from the generic transformation to n-bit encryption. By introducing matrix multiplication functional encryption, which essentially performs a fixed number of parallel calls on functional encryptions with the same randomness, we can prove the security of the final scheme with a tight reduction that does not depend on n, in contrast to employing the hybrid argument.

Keywords: Anonymity · Trace and revoke · Functional encryption

1 Introduction

Trace-and-revoke systems, introduced in [21,22] have been studied extensively in many works, including [4,11,14,18,24]. A trace-and-revoke system is a multi-recipient encryption scheme in which a content distributor can find malicious

J. Baek and S. Ruj (Eds.): ACISP 2021, LNCS 13083, pp. 214–233, 2021.
https://doi.org/10.1007/978-3-030-90567-5_11

users and revoke their decryption capability. Note that a user might share its secret key with non-legitimate entity. In such a case, it should be possible to identify the user, so that it is revoked from further accessing new content. A traitor tracing system guarantees that if a coalition of users pool their secret keys to construct a pirate decoder box that can decrypt ciphertexts, then there is an efficient trace algorithm to find at least one guilty user provided the algorithm is given access to the decoder. Then the content distributor can use the revocation functionality to prohibit guilty users from accessing the data in the future. A revocation system ensures that if a coalition of illegitimate users pools their secret keys, they still cannot decrypt the ciphertext. A natural question occurs if one can devise a protocol where a revoked user is not able to find out if it has been revoked. One may further request that, given a ciphertext, no legitimate user will get any information about the users who have been revoked.

Anonymity of receivers is important in numerous real-life applications and have been considered in multiple works, such as [7,13,15,19,20]. The standard notion of anonymity requires that the adversary cannot distinguish between ciphertexts of two targeted sets of its choice, even if it can corrupt any user in the intersection of these two sets or outside of the two sets. Unfortunately, it turned out to be extremely difficult to achieve this anonymity level in the general case without any restriction on the size of the target set. The state-of-the-art constructions by Barth *et al.* [7] and Libert *et al.* [20] start from a public-key encryption and result in schemes with ciphertext size which is N times larger, where N denotes the total number of users. Moreover, Kiayias and Samari [17] proved that ciphertext size will be linear in N in the general case.

For revoke systems, the efficiency is often negatively correlated to the upper bound on the number of revoked users. One of the most important applications of broadcast encryption is Pay-TV and it can typically be in the form of a revoke system: the service broadcasts to all users except revoked users who were detected as traitors or who unsubscribed from the system. The state-of-the-art revoke systems [4,11,21,22] have compact ciphertext sizes that grow as $O(r)$ for r the bound of revoked users and which is not dependent in the number of users. None of these schemes is anonymous. An attempt was made to consider outsider adversaries, who can only corrupt users outside of the two targeted sets. In this limited setting, Fazio and Perera [15] showed that one can get key and ciphertext sizes that are sublinear in the number of users. We observe totally different situations for getting anonymity in broadcast encryption and in revoke systems: in broadcast encryption, optimal solutions exist [6,9] but one cannot get the anonymity with sublinear ciphertext size in the total number of users; in revoke systems, no impossibility result has been settled and it does not exclude the possibility to get an anonymous schemes which is as efficient as non-anonymous ones, namely ciphertext size is $O(r)$, independent in the number of users. In this paper, we show that we can design anonymous schemes with $O(r)$ ciphertext size. Moreover, we also handle traceability to achieve anonymous trace-and-revoke systems.

1.1 Contributions

Our primary contribution is to develop the first symmetric-key trace-and-revoke scheme with traceability and anonymous revocation. We give two constructions of trace-and-revoke schemes, namely TR_0 and TR_1 from so-called linear functional encryptions. The former TR_0 is generically constructed from inner product functional encryption (IPFE) and encrypts single bit messages. Similarly, TR_1 is constructed from matrix multiplication functional encryption (MMFE) to support n-bit messages. Interestingly, unlike [4], our DDH instantiations do not require discrete-log evaluation for ciphertext decryption.

Our second contribution is to propose efficient constructions. We give an efficient construction of MMFE in the prime-order groups and prove that our MMFE construction is indeed tightly secure under the standard matDH assumption. As IPFE construction and its security proof follow from those of MMFE, we omit them here and describe them in the full version. This construction can be seen as tweaking Tomida's tightly secure IPFE for the symmetric-key settings [25]. However, we note that our security argument is somewhat different from Tomida's. On top of that, our tightly secure MMFE is more efficient than applying [25] naively.

Our third contribution is a cryptanalysis on the LWE-based IPFE construction of [26]. This justifies our choice of LWE-based IPFE to instantiate TR_0.

Anonymous Revocation. Before describing our results, we discuss the notion of anonymous revocation in trace-and-revoke schemes. The Enc algorithm of any trace-and-revoke scheme takes a message m and a revoked user set description $\mathcal{R}$ and computes a ciphertext that can only be decrypted by users outside $\mathcal{R}$. The anonymity property intuitively means that no information on $\mathcal{R}$ should be inferred from the ciphertext. A typical multi-challenge security model is defined by polynomially many challenge phases where the adversary adaptively produces $(m^{(t)}, \mathcal{R}_0^{(t)}, \mathcal{R}_1^{(t)})$ on the t-th phase and gets an encryption of $(m^{(t)}, \mathcal{R}_\beta^{(t)})$ for the same $\beta \leftarrow \{0,1\}$ throughout the phases. However, this security model is quite strong and there are practical scenarios that do not require such stronger definition. For example, a typical trace-and-revoke scheme revokes more and more users over time. If a revoked user wants to get access to the system again, it has to contact the broadcaster, which can give the user a new key. In such a scenario, the revoked user set increases with time, such that $\mathcal{R}^{(t-1)} \subseteq \mathcal{R}^{(t)}$ for any timestamp $t > 1$. We model this scenario by introducing the restriction that, for any t, if the adversary produces the challenge $(m^{(t)}, \mathcal{R}_0^{(t)}, \mathcal{R}_1^{(t)})$, then $\mathcal{R}_0^{(t-1)} \subseteq \mathcal{R}_0^{(t)}$ and $\mathcal{R}_1^{(t-1)} \subseteq \mathcal{R}_1^{(t)}$, and call the resulting security property *multi-challenge monotonic anonymity* $\mathsf{mIND\text{-}ID\text{-}CPA}$.

1.2 Technical Overview

We start with a basic description of the trace-and-revoke scheme by Agrawal *et al.* [4] (in the bounded collusion model). Each user id in this scheme is associated with a vector $\mathbf{x}_{\mathsf{id}}$ and, correspondingly, a set $\mathcal{R}$ is associated with $\mathbf{X}_{\mathcal{R}}$, the vector

space spanned by $(\mathbf{x}_{\mathsf{id}})_{\mathsf{id}\in\mathcal{R}}$. Then, the predicate '$\mathsf{id} \notin \mathcal{R}$' can be emulated by testing if '$\langle \mathbf{x}_{\mathsf{id}}, \mathbf{v}_{\mathcal{R}} \rangle = 0$' for $\mathbf{v}_{\mathcal{R}}$ orthogonal to $\mathbf{X}_{\mathcal{R}}$. Using this relation, one encrypts a message m by encrypting $m \cdot \mathbf{v}_{\mathcal{R}}$ using an IPFE. An IPFE key for $\mathbf{x}_{\mathsf{id}}$ is used to evaluate $\mathsf{id} \notin \mathcal{R}$ in the encrypted domain. We now describe the decryption algorithm of [4] to clarify that this construction does not achieve anonymity of the revocation set. Decryption takes a ciphertext ct for $(m, \mathcal{R})$ and a secret key sk for id and runs IPFE decryption to obtain an intermediate $\mathsf{Res} = \langle \mathbf{x}_{\mathsf{id}}, m \cdot \mathbf{v}_{\mathcal{R}} \rangle$. The correctness then follows from the fact that decryption can compute $\langle \mathbf{x}_{\mathsf{id}}, \mathbf{v}_{\mathcal{R}} \rangle$ and divide Res by it to retrieve m. This is the reason why the description of $\mathcal{R}$ is provided as part of the ciphertext. Thus, the Agrawal *et al.* scheme does not achieve revocation set hiding.

Our constructions build on [4], but avoid the above difficulty by exploiting the fact that if we consider the message to be single bit (i.e., $m \in \{0, 1\}$), we have the following four cases:

- $m = 0$, $\mathsf{id} \in \mathcal{R}$: The value of $\langle \mathbf{x}_{\mathsf{id}}, \mathbf{y}_{\mathcal{R}} \rangle = m \cdot \langle \mathbf{x}_{\mathsf{id}}, \mathbf{v}_{\mathcal{R}} \rangle$ is zero.
- $m = 1$, $\mathsf{id} \in \mathcal{R}$: Same as above where the value of $\langle \mathbf{x}_{\mathsf{id}}, \mathbf{y}_{\mathcal{R}} \rangle = m \cdot \langle \mathbf{x}_{\mathsf{id}}, \mathbf{v}_{\mathcal{R}} \rangle$ is zero; therefore, when $\mathsf{id} \in \mathcal{R}$, the message m is hidden.
- $m = 0$, $\mathsf{id} \notin \mathcal{R}$: The value of $\langle \mathbf{x}_{\mathsf{id}}, \mathbf{y}_{\mathcal{R}} \rangle = m \cdot \langle \mathbf{x}_{\mathsf{id}}, \mathbf{v}_{\mathcal{R}} \rangle$ is again zero.
- $m = 1$, $\mathsf{id} \notin \mathcal{R}$: The value of $\langle \mathbf{x}_{\mathsf{id}}, \mathbf{y}_{\mathcal{R}} \rangle = m \cdot \langle \mathbf{x}_{\mathsf{id}}, \mathbf{v}_{\mathcal{R}} \rangle$ is non-zero.

The above list of cases shows that a secret key for $\mathbf{x}_{\mathsf{id}}$ decrypts an IPFE ciphertext for $m \cdot \mathbf{v}_{\mathcal{R}}$ and retrieves $m \in \{0, 1\}$ correctly if $\mathsf{id} \notin \mathcal{R}$. Note that the decryption algorithm no longer requires the description of the revoked set $\mathcal{R}$. Based on this observation, our constructions translate $(m, \mathcal{R})$ into a vector $m \cdot \mathbf{v}_{\mathcal{R}}$ where $\mathbf{v}_{\mathcal{R}}$ is a random vector orthogonal to $\mathbf{X}_{\mathcal{R}}$ and id to a non-zero vector $\mathbf{x}_{\mathsf{id}}$. The monotonic anonymity (in the $\mathsf{mIND\text{-}ID\text{-}CPA}$ security model discussed above) then follows from the fact that the underlying IPFE hides the plaintext vector (here $m \cdot \mathbf{v}_{\mathcal{R}}$). For an n-bit message space, we can run independent and parallel executions of the IPFE that allow bit-by-bit retrieval of the message encrypted.[1] We propose a more efficient alternative, namely, matrix multiplication functional encryption (MMFE). Our generic transformation above ensures that any efficient instantiation of MMFE will result in efficient trace-and-revoke scheme. We discuss constructions of MMFE in both the group-based settings and in the lattice-based settings. We further show that our group-based construction of MMFE is tightly secure under standard assumptions. For lattice-based setting, we suggest to use [4] as we could mount a concrete attack on the state-of-the-art [26], rendering it insecure. Lastly, we note that tracing is performed in a similar fashion to [4].

An Attack on the Wang et al. *IPFE.* Here, we show that the IPFE construction by Wang *et al.* can be broken for the parameters chosen in [26]. Our attack can be thwarted by increasing the parameters, but then the scheme does not

[1] In practice, we use this scheme to send 128-bit session keys or a stream: if an user is in the targeted set then it decrypts correctly and if the user is not in the targeted set then it gets all 0s (and therefore the equivalent of a trivial decryptor which generates 0 all the time).

enjoy great efficiency compared to the one from [4]. Here, we give the overview LWE-based IPFE from [26]. The dimension n of the LWE secrets is proportional to the security parameter λ, the parameters ℓ, m, p, q are polynomial in n. The master secret key is $\mathbf{Z}$, uniform over $\{0,\ldots,p-1\}^{\ell\times m}$. The public key is of the form $\mathsf{pk} = (\mathbf{A} \in \mathbb{Z}_q^{m\times n}, \mathbf{T} = \mathbf{ZA} \in \mathbb{Z}_q^{\ell\times n})$. The secret key for the vector $\mathbf{x} \in \mathbb{Z}_p^\ell$ is $\mathsf{sk}_\mathbf{x} = \mathbf{x}^t \cdot \mathbf{Z}$. The ciphertext for a vector $\mathbf{y} \in \mathbb{Z}_p^\ell$ is of the form $(\mathbf{c}_0 \approx \mathbf{As}, \mathbf{c}_1 \approx \mathbf{Ts}+(q/p)\cdot\mathbf{y})$. The authors state that under the LWE assumption, this IPFE is adaptively secure for chosen message distributions, assuming that the secret key queries are linearly independent. We will give an algorithm that can recover the master key from the public key and ciphertexts (i.e., recover $\mathbf{z}$ from $\mathbf{X}^t$ and $\mathbf{X}^t\mathbf{z}$, where $\mathbf{z} \leftarrow \{0,\ldots,p-1\}^\ell$ and $\mathbf{X} \in \{0,\ldots,p-1\}^{\ell\times(\ell-1)}$ is chosen by the adversary). We remark that $\mathbf{z}$ belongs to a coset of the lattice orthogonal of $\mathbf{X}$ defined by $\mathbf{t}$. The crux of the attack is that for parameters as above, the minimum of this lattice is larger than $\|\mathbf{z}\|$. This means that we have a Bounded Distance Decoding problem instance in a lattice of dimension 1. Finally, we also explain why our attack does not extend to the schemes from [4,5].

Organization of the Paper. In Sect. 2, we present some important definitions. In Sect. 3, we present black-box transformations to convert linear functional encryptions into trace-and-revoke systems with traceability and anonymity of revocation. Before we present group-based MMFE construction, in Sect. 4, we show an attack of a recent LWE-based IPFE construction [26]. Then, in Sect. 5, we present a construction of MMFE in the prime-order groups.

2 Definitions and Preliminaries

For $a, b \in \mathbb{N}$ such that $a \leq b$, we often use $[a, b]$ to denote $\{a,\ldots,b\}$. Given a set of vectors S, we use $\mathsf{Matrix}(S)$ to denote the matrix whose each row is a distinct vector from S. For any two sets S and R, we define $S\Delta R = (S \setminus R) \cup (R \setminus S)$. For a dictionary $\mathsf{D} = (k, v_k)_k$, $\mathsf{D.vals}()$ gives the set $\{v_k : k \in \mathsf{D}\}$. For a vector space $\mathbf{V}$ over a field $\mathbb{K}$, the corresponding orthogonal space is denoted by $\mathbf{V}^\perp$. For a distribution D, we write $x \leftarrow D$ to say that x is sampled from D. The ppt abbreviation stands for probabilistic polynomial time. We denote $\mathcal{G}_{gen}(1^\lambda, p) \rightarrow (g, \mathbb{G})$ such that $\mathbb{G}$ is a cyclic group of prime order p and g generates $\mathbb{G}$. For $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_p^{\beta\times\alpha}$ we denote $[\mathbf{A}] = (g^{a_{ij}}) \in \mathbb{Z}_p^{\beta\times\alpha}$. For $m, k \in \mathbb{N}$ for $m > k$, we use $\mathbf{M} \leftarrow \mathcal{D}_{m,k}$ to get a full rank matrix $\mathbf{M} \in \mathbb{Z}_p^{m\times k}$ where the first k rows are linearly independent.

2.1 Linear Functional Encryption

A functional encryption scheme [10] allows a user, having a secret key sk_f corresponding to a function f, to evaluate $f(z)$ securely given a ciphertext ct_z for a plaintext z. The inner product function, being one of the simplest functionalities, has received a tremendous amount of exposure [1–3,5,12,25]. We here define an

extended version for IPFE in symmetric-key settings called Matrix Multiplication Functional Encryption (MMFE). Informally speaking, having a secret key $\mathsf{sk}_{\mathbf{x}}$ for $\mathbf{x} \in \mathbb{Z}_p^{\ell}$, given a ciphertext $\mathsf{ct}_{\mathbf{M}}$ for for $\mathbf{M} \in \mathbb{Z}_p^{n \times \ell}$, MMFE outputs a binary vector of length n where the i^{th} component indicates if $\mathbf{M}_i\mathbf{x} = 0$ for $i \in [n]$ in terms of a predicate $f : \mathbb{Z}_p \to \{0,1\}$. Precisely, $\mathcal{MMFE}.\mathsf{Dec}(\mathsf{sk}_{\mathbf{x}}, \mathsf{ct}_{\mathbf{M}})$ outputs $(f(\mathbf{M}_1\mathbf{x}), \ldots, f(\mathbf{M}_n\mathbf{x}))$ where $f(z) = \begin{cases} 0 & \text{if } z = 0 \\ 1 & \text{otherwise} \end{cases}$. We say that an MMFE scheme $\mathcal{MMFE}$ is IND-CPA-secure if no polynomial adversary can distinguish a ciphertext $\mathsf{ct}_{\mathbf{M}^{(0)}}$ from another ciphertext $\mathsf{ct}_{\mathbf{M}^{(1)}}$ for distinct $\mathbf{M}^{(0)}, \mathbf{M}^{(1)} \in \mathbb{Z}_p^{n \times \ell}$. Thus, IPFE scheme $\mathcal{IPFE}$ is basically $\mathcal{MMFE}$ with $n = 1$. We present the definitions more formally in the full version of the paper due to page limitation.

2.2 Trace-and-Revoke Systems

A symmetric key traitor tracing encryption scheme is a multi-recipient encryption system in which a broadcasting office has the master secret key for encryption and there are many users with decryption capabilities, each having its own secret key. Additionally, the encryption scheme provides a feature to let the broadcaster identify at least one user from a coalition $\mathcal{T}$ of malicious users (traitors) that built an unauthorized decryption device $\mathcal{D}$. The following is the blackbox confirmation model [8], in which an efficient tracing algorithm Trace is given oracle access to $\mathcal{D}$, which we denote by $\mathcal{O}^{\mathcal{D}}$. The oracle $\mathcal{O}^{\mathcal{D}}$ takes as input any message-ciphertext pair (m, C) and returns 1 if $\mathcal{D}(C) = m$ and 0 otherwise. Given as input a set $\mathcal{S}$ of suspected users containing $\mathcal{T}$, the Trace algorithm should disclose the identity of at least one user from the set $\mathcal{T}$. For security, a traitor coalition should not be able to design a useful box that escapes tracing, i.e., such that the Trace algorithm replies $\perp$ or frames an innocent user in $\mathcal{S} \setminus \mathcal{T}$.

Following [4], the probability of decryption of decoder $\mathcal{D}$, can be estimated by repeatedly querying the oracle $\mathcal{O}^{\mathcal{D}}$ with plaintext-ciphertext pairs. Therefore, we assume the decryption device $\mathcal{D}$ correctly decrypts a properly generated ciphertext with significant probability. The following is a description of $\mathcal{D}$, reproduced from [4] and modified for the symmetric-key setting. Let $\mathcal{R}$ be any set of revoked users, of size $\leq r$. Let the message m be sampled uniformly at random from the message space $\mathcal{M}$ and let $C_{\mathcal{R}}$ be the output of the encryption algorithm Enc using the master secret key msk and $\mathcal{R}$ as the set of revoked users. With $C_{\mathcal{R}}$ as input, the device $\mathcal{D}$ is assumed to output m with probability significantly more than $1/|\mathcal{M}|$:

$$\Pr_{\substack{m \leftarrow U(\mathcal{M}) \\ C_{\mathcal{R}} \leftarrow \mathsf{Enc}(\mathsf{msk}, \mathsf{pp}, \mathcal{R}, m)}} \left[\mathcal{O}^{\mathcal{D}}(C_{\mathcal{R}}, m) = 1\right] \geq \frac{1}{|\mathcal{M}|} + \frac{1}{\lambda^c}, \tag{1}$$

for some constant $c > 0$.

We let the identity space ID and the message space $\mathcal{M}$ be implicit arguments to the setup algorithm below. We let the secret key space $\mathcal{K}$, the ciphertext space $\mathcal{C}$ (along with ID and $\mathcal{M}$) and the descriptions of mathematical tools that

are used be part of the public parameters output by the setup algorithm. We adapt the definition from [4] to the symmetric-key setting.

Definition 1. *A dynamic trace-and-revoke scheme* TR *in the black-box confirmation model is a tuple* $\mathsf{TR} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Trace})$ *of five* ppt *algorithms with the following specifications.*

- $\mathsf{Setup}(1^\lambda, 1^r, 1^t)$ *takes as input the security parameter* λ*, the bound* t *on the size of traitor coalitions and the bound* r *on the number of revoked users. It outputs* $(\mathsf{msk}, \mathsf{pp}, \mathsf{dir})$ *containing the master secret key* msk*, the public parameters* pp *and the initially empty user directory* dir*. Here, unlike* [4]*,* dir *is kept secret.*
- $\mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathsf{id})$ *takes as input the public parameters* pp*, the master secret* msk*, the user directory* dir *and an identity* $\mathsf{id} \in \mathsf{ID}$ *of a user. It outputs the corresponding secret key* $\mathsf{sk}_{\mathsf{id}}$ *and some information* u_{id} *for the given identity* id*. It also updates* dir *to include* u_{id}*.*
- $\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, m)$ *takes as input the public parameters* pp*, the master secret* msk*, the user directory* dir*, a set* $\mathcal{R}$ *of size* $\leq r$ *which contains the* u_{id} *of each revoked user in* dir*, and a plaintext message* $m \in \mathcal{M}$*. It outputs a ciphertext* $C_{\mathcal{R}} \in \mathcal{C}$*.*
- $\mathsf{Dec}(\mathsf{pp}, \mathsf{sk}_{\mathsf{id}}, C_{\mathcal{R}})$ *takes as input the public parameters* pp*, a secret key* $\mathsf{sk}_{\mathsf{id}}$ *of a user with identity* id *and a ciphertext* $C_{\mathcal{R}} \in \mathcal{C}$*. It outputs a plaintext* $m' \in \mathcal{M}$*.*
- $\mathsf{Trace}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, \mathcal{S}, \mathcal{O}^{\mathcal{D}})$ *is a tracing algorithm in the black-box confirmation model that takes as input the public parameters* pp*, the master secret key* msk*, the user directory* dir*, a set* $\mathcal{R}$ *of* $\leq r$ *revoked users, a set* $\mathcal{S}$ *of* $\leq t$ *suspect users, and has black-box access to the pirate decoder* $\mathcal{D}$ *through the oracle* $\mathcal{O}^{\mathcal{D}}$*. It outputs an identity* id *or* $\perp$*.*

The correctness requirement is that, with overwhelming probability over the randomness used by the algorithms, for $(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}) \leftarrow \mathsf{Setup}(1^\lambda, 1^r, 1^t)$*, for any set* $\mathcal{R}$ *of* $\leq r$ *revoked users:*

$$\forall m \in \mathcal{M},\ \forall \mathsf{id} \in \mathsf{ID} \setminus \mathcal{R} :\ \mathsf{Dec}(\mathsf{pp}, \mathsf{sk}_{\mathsf{id}}, \mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, m)) = m.$$

In this work, we consider three security properties for a trace-and-revoke scheme: message hiding, revocation set hiding, and traceability.

2.2.1 Message Hiding

The IND-CPA security of a trace-and-revoke scheme TR is defined based on the following game. Informally speaking, neither a system outsider nor a revoked user must be able to get any information about the encrypted message.

- The challenger runs $\mathsf{Setup}(1^\lambda, 1^r, 1^t)$ and gives the produced public parameters pp to the adversary $\mathcal{A}$. The adversary may ask the challenger to add polynomially many users in the system (these user addition queries can be adaptive and take place at any time in the game). The challenger updates dir accordingly.

- The adversary can adaptively make up to r secret key queries and a single challenge ciphertext query, of the following form:
  - Given a key generation query id, the challenger provides the corresponding $\mathsf{sk}_{\mathsf{id}}$ to $\mathcal{A}$.
  - Given the challenge ciphertext query $(m_0, m_1, \mathcal{R})$ with $\mathcal{R} \subset \mathsf{ID}$ of size $\leq r$, the challenger samples $\beta \leftarrow \{0,1\}$ and provides $C^{(\beta)} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, m_\beta)$ to $\mathcal{A}$.

  These queries are subject to the restriction that every queried id belongs to $\mathcal{R}$.
- Finally, the adversary returns its guess $\beta' \in \{0,1\}$ for the bit β chosen by the challenger. The adversary wins this game if $\beta = \beta'$.

The advantage of the adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{TR},\mathcal{A}} = |\Pr[\beta = \beta'] - 1/2|.$$

A trace-and-revoke scheme TR is said to be $\mathsf{IND\text{-}CPA}$ secure if $\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{TR},\mathcal{A}}$ is negligible for all ppt adversary $\mathcal{A}$.

2.2.2 Revocation Set Hiding

The anonymity of a trace-and-revoke scheme TR captures the idea of hiding the *revocation set* in the ciphertext: if t^{th} challenge ciphertext is created for one of the two adversarially chosen revoked sets $(\mathcal{R}_0^{(t)}, \mathcal{R}_1^{(t)})$ on the t^{th} challenge phase, then the adversary cannot distinguish if $\mathcal{R}_0^{(t)}$ or $\mathcal{R}_1^{(t)}$ was used for the encryption for all of t.

As we already have mentioned in the Introduction, we aim for a multi-challenge security settings that properly emulates the following scenario: A typical trace-and-revoke scheme traces and revokes more and more users over the time. In such a scenario, each new ciphertext is created for growing revoked user sets. We call this setting as *monotonic anonymity* security model ($\mathsf{mIND\text{-}ID\text{-}CPA}$) and define it as following.

- The challenger runs $\mathsf{Setup}(1^\lambda, 1^r, 1^t)$ and gives the produced public parameter pp to the adversary $\mathcal{A}$. The adversary may ask the challenger to add polynomially many users in the system (these user addition queries can be adaptive and take place at any time in the game). The challenger updates dir accordingly.
- The adversary can adaptively make up to $(r + t)$ secret key queries and polynomially many anonymity challenge queries, of the following form:
  - Given a key generation query id, the challenger provides the corresponding $\mathsf{sk}_{\mathsf{id}}$ to $\mathcal{A}$.
  - Given a challenge anonymity query $(m, \mathcal{R}_0, \mathcal{R}_1)$ with $\mathcal{R}_0, \mathcal{R}_1 \subset \mathsf{ID}$ of size $\leq r$, the challenger samples $\beta \leftarrow \{0,1\}$ and provides $C^{(\beta)} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}_\beta, m)$ to $\mathcal{A}$.

  These queries are subject to the restriction that for every queried id, either $\mathsf{id} \in \mathcal{R}_0 \cap \mathcal{R}_1$ or $\mathsf{id} \in \mathsf{ID} \setminus (\mathcal{R}_0 \cup \mathcal{R}_1)$. Among all the key queries that have been made, at most t of them could be satisfying $\mathsf{id} \in \mathsf{ID} \setminus (\mathcal{R}_0 \cup \mathcal{R}_1)$ and at most

r of them could be satisfying $\mathsf{id} \in \mathcal{R}_0 \cap \mathcal{R}_1$. The challenge anonymity queries also have a natural restriction that $\mathcal{R}_0^{(i)} \subseteq \mathcal{R}_0^{(j)}$ and $\mathcal{R}_1^{(i)} \subseteq \mathcal{R}_1^{(j)}$ for all $i \leq j$ where the t^{th} challenge anonymity query was made on $(m^{(t)}, \mathcal{R}_0^{(t)}, \mathcal{R}_1^{(t)})$.
- Finally, the adversary returns its guess $\beta' \in \{0,1\}$ for the bit β chosen by the challenger. The adversary wins this game if $\beta = \beta'$.

The advantage of the adversary $\mathcal{A}$ is defined as

$$\mathrm{Adv}^{\mathsf{mIND\text{-}ID\text{-}CPA}}_{\mathsf{TR},\mathcal{A}} = |\Pr[\beta = \beta'] - 1/2|.$$

A trace-and-revoke scheme TR is said to be $\mathsf{mIND\text{-}ID\text{-}CPA}$ secure if $\mathrm{Adv}^{\mathsf{mIND\text{-}ID\text{-}CPA}}_{\mathsf{TR},\mathcal{A}}$ is negligible for all ppt adversary $\mathcal{A}$.

2.2.3 Traceability

The notion of traceability considers a suspected set $\mathcal{S}$ of users who might have produced the pirate decoder $\mathcal{D}$. Then the tracing algorithm Trace outputs an $\mathsf{id} \in \mathcal{S} \setminus \mathcal{T}$ where $\mathcal{T}$ is the set of traitors who are already detected. This requirement is formalized using the following game, denoted by $\mathsf{AD\text{-}TT}$, between an adversary $\mathcal{A}$ and a challenger. We reproduce the security model from [4] for sake of completeness.[2] More precisely, the authors of [4] achieved *public-traceability*: for this purpose, the public-key Enc algorithm was used to construct so-called probe ciphertexts to query $\mathcal{O}^{\mathcal{D}}$ and identify a traitor. Our trace-and-revoke scheme relies on a symmetric key Enc algorithm, and hence tracing relies on the master secret key msk (in particular, tracing is not public).

- The challenger runs $\mathsf{Setup}(1^\lambda, 1^r, 1^t)$ and gives pp to $\mathcal{A}$. The adversary may ask the challenger to add polynomially many users in the system (these user addition queries can be adaptive and take place at any time in the game). The challenger updates dir accordingly.
- Adversary $\mathcal{A}$ makes adaptive traitor key queries on at most t distinct users. For every id queried, the challenger checks to find $\mathsf{u_{id}} \leftarrow \mathsf{dir}[\mathsf{id}]$. If available, records id in $\mathcal{T}$ and returns $\mathsf{sk_{id}}$. Otherwise, adds $\mathsf{u_{id}}$ to $\mathsf{dir}[\mathsf{id}]$, records id in $\mathcal{T}$ and returns $\mathsf{sk_{id}} \leftarrow \mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathsf{id})$.
- Adversary $\mathcal{A}$ sends an adaptively chosen revocation set $\mathcal{R} \subset \mathsf{ID}$ of size $\leq r$ and gets back all the secret keys $\{\mathsf{sk_{id}} \leftarrow \mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathsf{id})\}_{\mathsf{id} \in \mathcal{R}}$.
- Adversary $\mathcal{A}$ then produces a pirate decoder $\mathcal{D}$ and gives the challenger its access in terms of an oracle $\mathcal{O}^{\mathcal{D}}$. $\mathcal{A}$ also produces a suspect set $\mathcal{S}$ of size $\leq t$ containing $\mathcal{T}$ and sends it to the challenger.

[2] Recently, a more general model of pirate, called *pirate distinguisher*, have been introduced and considered in [16,24]. However, as proven in [13], in the bit-encryption setting, such a notion of pirate distinguisher is equivalent to the pirate decoder. In this section, we consider bit-encryption and in the next section about multi-bit encryption, the tracing is reduced to the tracing in the bit-encryption sub schemes. Therefore, we keep using the definition from [4] (adapted to the symmetric-key setting).

- The challenger then runs $\mathsf{Trace}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, \mathcal{S}, \mathcal{O}^{\mathcal{D}})$. The adversary wins if both of the following hold:
  - Equation (1) is satisfied for the set of revoked users $\mathcal{R}$ chosen by the adversary (i.e., decoder $\mathcal{D}$ is useful),
  - the execution of Trace outputs $\perp$ or outputs an $\mathsf{id} \in \mathcal{S} \setminus \mathcal{T}$ with probability $\geq 1/\lambda^c$.

We define the tracing advantage $\mathrm{Adv}^{\mathsf{AD\text{-}TT}}_{\mathsf{TR},\mathcal{A}}$ as the probability of $\mathcal{A}$'s win. A trace-and-revoke scheme TR is said to be $\mathsf{AD\text{-}TT}$ secure if the advantage $\mathrm{Adv}^{\mathsf{AD\text{-}TT}}_{\mathsf{TR},\mathcal{A}}$ is negligible for all ppt adversary $\mathcal{A}$.

3 Trace-and-Revoke from Linear Functional Encryption

In this section, we construct a trace-and-revoke system from a linear functional encryption scheme that achieves traceability and anonymous revocation. This is achieved in two steps. First, a trace-and-revoke system for single-bit messages is constructed from inner product functional encryption. Then we extend such a trace-and-revoke system to support arbitrary fixed length strings.

We first define a generic transformation similar to the one of [4], which converts an $\mathsf{IND\text{-}CPA}$ secure inner product functional encryption scheme IPFE into a trace-and-revoke system TR_0 for the restricted message space $\mathcal{M} = \{0,1\}$ that enjoys anonymous revocation. Note that this transformation converts an $\mathsf{IND\text{-}CPA}$ secure IPFE in the bounded collusion model to a trace-and-revoke system TR_0 that supports an exponential number of users like [4]. Then we provide another generic transformation that converts an $\mathsf{IND\text{-}CPA}$ secure matrix multiplication functional encryption scheme (MMFE) into a trace-and-revoke system TR_1 for the message space $\mathcal{M} = \{0,1\}^n$ for n as large as $\mathsf{poly}(\lambda)$. This transformation also ensures that TR_1 achieves anonymous revocation along with supporting an exponential number of users.

As, our primary contribution in this paper, is to introduce trace-and-revoke schemes with anonymous revocation, our presentation mainly focuses on the construction and the anonymity security of TR_0 and TR_1. Nevertheless, in Sect. 3.1, we have provided a complete description of the TR_0 that includes an explicit description of the Trace function. For the sake of simplicity, we however have presented the general trace-and-revoke systems TR_1 in Sect. 3.2 without a Trace. Note that, TR_1 can use the Trace algorithm of TR_0.

3.1 Trace-and-Revoke for Single Bit Messages

We construct a trace-and-revoke scheme TR_0 following the specifications of Definition 1 for the message space $\mathcal{M} = \{0,1\}$. TR_0 relies on a user directory dir which contains the identities of all the users that have been assigned keys in the system. This user directory is initially empty. Unlike [4], we assume that dir can only be accessed by the central authority, which is the sender as well as the key generator. TR_0 relies on an inner product functional encryption scheme IPFE for

the ℓ-dimensional vector space on $\mathbb{Z}_p$, where the value ℓ is a function of r and t. Recall that, in a typical trace-and-revoke scheme, the bound on the number of revoked users r and the bound on the number of suspected users (traitors) t are given as the system parameters. Our description of $\mathcal{IPFE}$ (simpler form of $\mathcal{MMFE}$ as noted in Sect. 2.1) comes with an injective map f whose description is included in the public parameters pp. To define the trace-and-revoke scheme TR_0, we define a special element in the range of the map $\mathit{elem}^* = f(0)$. Concretely, in case of a group-based construction of $\mathcal{IPFE}$, we take the exponentiation map $f : x \mapsto [x]$ and have $\mathit{elem}^* = [0]$. In case of a lattice-based construction, we take the identity map $f : x \mapsto x$ and have $\mathit{elem}^* = 0$.

1. $\mathsf{Setup}(1^\lambda, 1^r, 1^t)$. Upon input the security parameter λ, the bound t on the number of the suspected users, and the bound r on the number of revoked users, set $p = \lambda^{\omega(1)}$ and proceed as follows:
   (a) Let $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathcal{IPFE}.\mathsf{Setup}(1^\lambda, 1^\ell, p)$, where we set $\ell = 2r + t + 1$. The key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$ are the $\mathcal{IPFE}$ key space and ciphertext space, respectively.
   (b) Create an empty directory dir.
   (c) Output the public parameter pp, master secret key msk and the (empty) user directory dir.
2. $\mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathsf{id})$. Upon input the public parameters pp, the master secret key msk, the user directory dir and a user identity $\mathsf{id} \in \mathsf{ID}$, proceed as follows:
   (a) Sample $\mathbf{x}_{\mathsf{id}} \leftarrow \mathbb{Z}_p^\ell$. The pair $\mathsf{u}_{\mathsf{id}} = (\mathsf{id}, \mathbf{x}_{\mathsf{id}})$ is then appended to dir.
   (b) Let $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathcal{IPFE}.\mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathbf{x}_{\mathsf{id}})$.
   (c) Output $(\mathsf{sk}_{\mathsf{id}}, \mathbf{x}_{\mathsf{id}})$.
3. $\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, m)$. Upon input the public parameters pp, the master secret key msk, the user directory dir, a set of revoked users $\mathcal{R}$ of size $\leq r$ and a plaintext message $m \in \mathcal{M} = \{0, 1\}$, proceed as follows:
   (a) Sample $\mathbf{v}_{\mathcal{R}} \leftarrow \mathbf{X}_{\mathcal{R}}^\perp$ where $\mathbf{X}_{\mathcal{R}} = \{\mathbf{x}_{\mathsf{id}} \ : \ \mathsf{id} \in \mathcal{R}\}$.
   (b) Compute $\mathbf{y}_{\mathcal{R}} = m \cdot \mathbf{v}_{\mathcal{R}}$.
   (c) Output $C_{\mathcal{R}} = \mathcal{IPFE}.\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathbf{y}_{\mathcal{R}})$.
4. $\mathsf{Dec}(\mathsf{pp}, (\mathsf{sk}_{\mathsf{id}}, \mathbf{x}_{\mathsf{id}}), C_{\mathcal{R}})$. Upon input the public parameters pp, the secret key $\mathsf{sk}_{\mathsf{id}}$ for user id and a ciphertext $C_{\mathcal{R}}$, proceed as follows:
   (a) Compute $\mathsf{Res} = \mathcal{IPFE}.\mathsf{Dec}(\mathsf{pp}, (\mathsf{sk}_{\mathsf{id}}, \mathbf{x}_{\mathsf{id}}), C_{\mathcal{R}})$.
   (b) If $\mathsf{Res} = \mathit{elem}^*$, then output 0. Otherwise output 1.
5. $\mathsf{Trace}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, \mathcal{S}, \mathcal{O}^{\mathcal{D}})$. Upon input the master secret key msk, the user directory dir, a revoked set of users $\mathcal{R}$, a suspect set of users $\mathcal{S}$ and given access to the oracle $\mathcal{O}^{\mathcal{D}}$, proceed as follows:
   (a) Suppose the users in the suspect set $\mathcal{S}$ can distinguish between the messages $m = 0$ and $m' = 1$ except with negligible probability provided these users can access the oracle $\mathcal{O}^{\mathcal{D}}$.[3]
   (b) Set $\mathcal{S}_1 = \{\mathsf{id}_1, \mathsf{id}_2, \ldots\} = \mathcal{S} \setminus \mathcal{R}$.
   (c) Sample $\mathbf{v}_{\mathcal{R}} \leftarrow \mathbf{X}_{\mathcal{R}}^\perp$ where $\mathbf{X}_{\mathcal{R}} = \{\mathbf{x}_{\mathsf{id}} \ : \ \mathsf{id} \in \mathcal{R}\}$.

[3] Note that [4] used Hoeffding's inequality to ensure that one can efficiently find such distinguishable m and m'. In our case, it is simpler, as $\mathcal{M} = \{0, 1\}$.

(d) For all $i = 1, 2, \ldots, t$,
- If $i = 1$, set $\mathbf{v}_{\mathcal{S}_i} = \mathbf{0}$. If $\mathcal{S}_i = \emptyset$, set $\mathbf{v}_{\mathcal{S}_i} = (m' - m) \cdot \mathbf{v}_{\mathcal{R}}$.
- Otherwise, sample $\mathbf{v}_{\mathcal{S}_i} \leftarrow \mathbf{X}^{\perp}_{\mathcal{R}\cup\mathcal{S}_i} \cap \left(\mathbf{X}^{\perp}_{\mathcal{S}_1\setminus\mathcal{S}_i} + (m' - m) \cdot \mathbf{v}_{\mathcal{R}}\right)$ where $\mathbf{X}_{\mathcal{R}\cup\mathcal{S}_i} = \{\mathbf{x}_{\mathsf{id}} : \mathsf{id} \in \mathcal{R} \cup \mathcal{S}_i\}$ and $\mathbf{X}_{\mathcal{S}_1\setminus\mathcal{S}_i} = \{\mathbf{x}_{\mathsf{id}} : \mathsf{id} \in \mathcal{S}_1 \setminus \mathcal{S}_i\}$.
- Construct $\mathbf{y}_i = \mathbf{v}_{\mathcal{S}_i} + m \cdot \mathbf{v}_{\mathcal{R}}$;
- Provide the oracle $\mathcal{O}^{\mathcal{D}}$ with $(C_{\mathcal{S}_i}, m)$ as input and get a binary value b_i as output. Suppose the probability of $b_i = 1$ is p_i.
- The probe ciphertext is $C_{\mathcal{S}_i} = \mathit{IPFE}.\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathbf{y}_i)$; We note that, the decryption result of the probe ciphertext $C_{\mathcal{S}_i}$ is m if $\mathsf{id} \in \mathcal{S}_i$ and m' if $\mathsf{id} \in \mathcal{S} \setminus \mathcal{S}_i$.
- If $i > 1$ and $|p_i - p_{i-1}|$ is non-negligible,
  - Output id_{i-1} as the traitor identity and abort;
  - If $\mathcal{S}_i = \phi$, output $\perp$ and abort. Otherwise, set $\mathcal{S}_{i+1} = \mathcal{S}_i \setminus \{\mathsf{id}_i\}$.

We state the following theorems that are essential for the correctness and defer the proofs to the full version of the paper, due to page limitation.

Theorem 1. *Assume that $p = \lambda^{\omega(1)}$. Then, for every set $\mathcal{R}$ of revoked users of size $\leq r$, every $\mathsf{id} \notin \mathcal{R}$ and every $m \in \mathcal{M} = \{0, 1\}$, we have*

$$\mathsf{Dec}(\mathsf{pp}, (\mathsf{sk}_{\mathsf{id}}, \mathbf{x}_{\mathsf{id}}), \mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, m)) = m,$$

with probability $\geq 1 - \lambda^{-\omega(1)}$.

Theorem 2. *Let $\mathcal{R}$ be arbitrary of size $\leq r$ and assume Eq. (1) holds for $\mathcal{O}^{\mathcal{D}}$ and $\mathcal{R}$. Then we have:*

$$\left| \Pr_{C \leftarrow \mathsf{Enc}(\mathsf{pp},\mathsf{msk},\mathsf{dir},\mathcal{R},0)}[\mathcal{O}^{\mathcal{D}}(C, 0) = 1] - \Pr_{C \leftarrow \mathsf{Enc}(\mathsf{pp},\mathsf{msk},\mathsf{dir},\mathcal{R},1)}[\mathcal{O}^{\mathcal{D}}(C, 0) = 1] \right| \geq \frac{2}{\lambda^c},$$

with probability $\geq 1 - \lambda^{-\omega(1)}$ and for some constant $c > 0$.

Security. We prove that the base scheme TR_0 enjoys message hiding, revocation set hiding and traceability. We defer these proofs to the full version.

Theorem 3. *If IPFE is an* IND-CPA *secure inner product functional encryption scheme allowing up to r key extraction queries, then TR_0 is* IND-CPA *secure.*

Theorem 4. *If IPFE is an* IND-CPA *secure inner product functional encryption scheme allowing up to $(t + r)$ key extraction queries, then TR_0 is* mIND-ID-CPA *secure.*

Theorem 5. *If IPFE is an* IND-CPA *secure inner product functional encryption scheme allowing $(r + t)$ queries, then TR_0 is* AD-TT *secure.*

3.2 Efficient Trace-and-Revoke for Bit Strings

We present a trace-and-revoke scheme TR_1 for $\mathcal{M} = \{0,1\}^n$ that does not run parallel independent n executions of TR_0. However, we note that, we omit the description of Trace here as it follows from the Trace algorithm of TR_0. This scheme again assumes the existence of a user directory dir which is initialized to be empty, contains the identities of the users that have been assigned keys in the system. We assume that dir can only be modified by the central authority who is the sender as well as the key generator. Here, we assume existence of an efficient matrix multiplication functional encryption $\mathcal{MMFE}$ that encrypts matrices of $n \times \ell$ dimension. The intuitive idea here is that, we utilize n copies of inner product of ℓ dimensional vectors as a linear system of equations $\mathbf{Mx}$ where $\mathbf{M} \in \mathbb{Z}_p^{n \times \ell}$ and $\mathbf{x} \in \mathbb{Z}_p^{\ell}$. Each of the rows of $\mathbf{M}$ is used to encrypt each message bit.

1. $\mathsf{Setup}(1^\lambda, 1^n, 1^r, 1^t)$. Upon input the security parameter λ, the message bit-length n, the bound t on the number of the suspected users and the bound r on the number of revoked users, set $p = \lambda^{\omega(1)}$ and proceed as follows:
   (a) Let $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathcal{MMFE}.\mathsf{Setup}(1^\lambda, 1^\ell, 1^n, p)$, where we set $\ell = 2r+t+n+1$.
   (b) Output the public parameter pp, master secret key msk and an empty user directory dir.
2. $\mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathsf{id})$. Upon input the public parameters pp, the master secret key msk, the user directory dir and a user identity $\mathsf{id} \in \mathsf{ID}$, proceed as follows:
   (a) Sample $\mathbf{x}_{\mathsf{id}} \leftarrow \mathbb{Z}_p^{\ell}$. The pair $\mathsf{u}_{\mathsf{id}} = (\mathsf{id}, \mathbf{x}_{\mathsf{id}})$ is then appended to the user directory dir.
   (b) Let $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathcal{MMFE}.\mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathbf{x}_{\mathsf{id}}) \in \mathcal{MMFE}.\mathcal{K}$.
   (c) Output $(\mathsf{sk}_{\mathsf{id}}, \mathbf{x}_{\mathsf{id}})$.
3. $\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathsf{dir}, \mathcal{R}, m)$. Upon input the public parameter pp, the master secret key msk, the user directory dir, a set of revoked users $\mathcal{R}$ of size $\leq r$ and a plaintext messages $m \in \mathcal{M} = \{0,1\}^n$, proceed as follows:
   (a) Sample $\mathbf{v}_{\mathcal{R},1}, \ldots, \mathbf{v}_{\mathcal{R},n} \leftarrow \mathbf{X}_{\mathcal{R}}^{\perp}$ where $\mathbf{X}_{\mathcal{R}} = \{\mathbf{x}_{\mathsf{id}} \in \mathbb{Z}_p^{\ell} \ : \ \mathsf{id} \in \mathcal{R}\}$.
   (b) Compute $\mathbf{y}_{\mathcal{R},i} = m_i \cdot \mathbf{v}_{\mathcal{R},i}$ for $i \in [1,n]$.
   (c) Define a matrix $\mathbf{M}_{\mathcal{R}} = (\mathbf{y}_{\mathcal{R},1}, \ldots, \mathbf{y}_{\mathcal{R},n})^\top$.
   (d) Output $C_{\mathcal{R}} = \mathcal{MMFE}.\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathbf{M}_{\mathcal{R}})$.
4. $\mathsf{Dec}(\mathsf{pp}, (\mathbf{x}_{\mathsf{id}}, \mathsf{sk}_{\mathsf{id}}), C_{\mathcal{R}})$. Upon input the public parameters pp, the secret key $\mathsf{sk}_{\mathsf{id}}$ for user id and a ciphertext $C_{\mathcal{R}}$ considering the revoked set $\mathcal{R}$, proceed as follows:
   (a) Compute $\mathbf{t} = \mathcal{MMFE}.\mathsf{Dec}(\mathsf{pp}, (\mathbf{x}_{\mathsf{id}}, \mathsf{sk}_{\mathsf{id}}), C_{\mathcal{R}})$.
   (b) Output $m' = (m'_1, \ldots, m'_n) \in \{0,1\}^n$ where for all $i \in [1,n]$, $m'_i = 0$ if $t_i = \mathit{elem}^*$; else $m'_i = 1$.

Correctness. The correctness basically follows from the correctness of TR_0 above. The main difference is that, functionally, Enc of TR_1 is some-what n many copies of Enc of TR_0. Thus, Dec must concatenate all the bits to get back the message. Therefore, TR_1 is correct if Dec of TR_1 retrieves all the bits m_i correctly. Now, if $\exists i \in [1,n]$, such that Dec of TR_1 didn't compute m_i correctly,

this can be extended to an attack on the correctness of Dec of TR_0. This basically ensures the correctness of TR_1.

Security. We prove that TR_1 enjoys message hiding and revocation set hiding. We defer these proofs to the full version due to page limitation.

Theorem 6. *If $\mathcal{MMFE}$ is an* IND-CPA *secure matrix multiplication functional encryption scheme, then* TR_1 *is* IND-CPA *secure.*

Theorem 7. *If $\mathcal{MMFE}$ is an* IND-CPA *secure matrix-multiplication functional encryption scheme allowing at most* $(t+r-1)$ *key extraction queries, then* TR_1 *is* mIND-ID-CPA *secure.*

Construction TR_0 *and* TR_1. Note that, available IPFE schemes [4,5] suffice to construct of TR_0 and TR_1. In particular, withholding the public keys of available IPFE schemes, one can get symmetric-key IPFE schemes and use them to construct TR_0. Furthermore, TR_1 can be constructed from running n independent instances of any symmetric-key IPFE scheme. We in fact use this technique to construct TR_0 and TR_1 in the lattice-based settings withholding the public key of Agrawal *et al.*'s IPFE [4]. In the group-based settings, however, we can achieve more efficient constructions than naively hiding the public key of the public-key IPFE. In Sect. 5, we propose new constructions of symmetric-key IPFE and symmetric-key MMFE in the prime-order groups.

4 Cryptanalysis of the Wang *et al.* IPFE Construction

As we mention above, the schemes from Sect. 3 can be instantiated with the LWE-based $\mathcal{IPFE}$ scheme from [4]. Note that the latter does not enjoy IND-CPA security, but it was showed to enjoy a weaker security property that still suffices for the trace-and-revoke scheme from [4]. That weaker security property restricts the number of key requests to be significantly smaller than the dimension of the vector space, and imposes that the vectors of the key queries are uniformly sampled. This relaxation of IND-CPA security also suffices for our adaptation from Sect. 3.

$\mathcal{IPFE}$ scheme from [26], note that the LWE-based $\mathcal{IPFE}$ scheme from [26] is also claimed to enjoy a security property that is stronger than IND-CPA security (which the authors leverage to obtain a decentralized Attribute-Based Encryption scheme). In fact, as we will show below, this scheme can be broken for the parameters suggested in [26]. Before showing an attack, we first recall some definitions.

Lattices. Given n linear independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, the lattice generated by them is defined as

$$L(\mathbf{B}) := \{\mathbf{Bz} = \sum_{i \in [1,n]} z_i \mathbf{b}_i : \mathbf{z} \in \mathbb{Z}^n\}.$$

The rank of this lattice is n and its dimension is m.

We define the determinant of L as $\det(L) := \sqrt{\det(\mathbf{B}^t\mathbf{B})}$. For a rank-$n$ matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$, there exist orthogonal matrices $\mathbf{U}, \mathbf{V}$ and a diagonal matrix $\mathbf{\Sigma} = \mathrm{Diag}(\sigma_1, \ldots, \sigma_n) \in \mathbb{R}^{m\times n}$ such that $\mathbf{B} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^t$ and $\sigma_1 \geq \cdots \geq \sigma_n > 0$. From this decomposition, we see that $\det(L(\mathbf{B})) = \prod_{i\in[1,n]} \|\sigma_\mathbf{i}\|$.

For $i \in [1, n]$, the i-th successive minimum $\lambda_i(L)$ is defined as

$$\lambda_i(L) := \inf\{r : \dim(\mathrm{Span}(L \cap \mathcal{B}(r))) \geq i\},$$

where $\mathcal{B}(r)$ denotes the closed zero-centered Euclidean ball of radius r.

Definition 2. *Let $m > n \geq 1$ be integers and $q \geq 2$ be prime. Let $\mathbf{X} \in \mathbb{Z}^{m\times n}$.*

*The **orthogonal lattice** $\Lambda^\perp(\mathbf{X})$ is the integral lattice whose vectors are orthogonal to the rows of $\mathbf{X}$, i.e.,*

$$\Lambda^\perp(\mathbf{X}) := \{\mathbf{u} \in \mathbb{Z}^m : \mathbf{X}^t\mathbf{u} = \mathbf{0}\}.$$

We note that if $\mathbf{X}$ has rank n (over the integers), then $\Lambda^\perp(\mathbf{X})$ has rank $(m-n)$.

Definition 3. *The bounded distance decoding problem BDD_γ is as follows: given a basis $\mathbf{B}$ of an n-rank lattice L, $\mathbf{t} \in \mathbb{R}^n$, and real $d \leq \frac{\lambda_1}{2}$ such that $dist(\mathbf{t}, L) \leq d$, find the unique $\mathbf{v} \in L$ closest to $\mathbf{t}$. Note that this is equivalent to finding $\mathbf{e} \in \mathbf{t}+L$ such that $\|\mathbf{e}\| \leq d$.*

We now describe here a simplified version of the security property that this scheme aims to achieve, and the corresponding simplified version of the scheme (this corresponds to setting $k = 1$ in the definition from [26]; our attack readily extends to $k \geq 1$). In the challenge phase, the adversary sends to the challenger descriptions of two distributions D_0 and D_1 over plaintext vectors. The challenger chooses $\beta \leftarrow \{0, 1\}$ and samples $\mathbf{y} \leftarrow D_\beta$; it encrypts it under the public key pk and the resulting ciphertext $\mathsf{Enc}_{\mathsf{pk}}(\mathbf{y})$ is given to the adversary. The adversary can adaptively make key queries $\mathbf{x}$, before or after the challenge phase. The security property, called adaptive security for chosen message distributions, requires that the adversary cannot guess β correctly, as long as the distributions D_0 and D_1 remain indistinguishable given the replies to the key queries.

We review their construction based on LWE.

- $\mathit{IPFE}.\mathsf{Setup}(1^n, 1^\ell, p)$. Set integers $m, q = p^e$ for some integer e, and reals $\alpha, \alpha' \in (0, 1)$. Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times n}$, $\mathbf{Z} \leftarrow \{0, \ldots, p-1\}^{\ell\times m}$,[4] compute $\mathbf{T} = \mathbf{Z}\mathbf{A} \in \mathbb{Z}_q^{\ell\times n}$, define

$$\mathsf{msk} := \mathbf{Z} \quad \text{and} \quad \mathsf{pk} := (\mathbf{A}, \mathbf{T}).$$

[4] In [26], the notation $\mathbb{Z}_p^{\ell\times m}$ is used instead of $\{0, \ldots, p-1\}^{\ell\times m}$. We stress that it should indeed be interpreted as $\{0, 1, \ldots, p-1\}^{\ell\times m}$. In particular, the operation $\mathbf{x}^t\mathbf{Z}$ in the $\mathit{IPFE}.\mathsf{KeyGen}$ algorithm is over $\mathbb{Z}$ and not modulo p, as otherwise decryption correctness would not hold.

- $\mathit{IPFE}.\mathsf{KeyGen}(\mathsf{msk}, \mathbf{x})$. Given $\mathbf{x} \in \mathbb{Z}_p^\ell$, set $\mathbf{z_x} = \mathbf{x}^t\mathbf{Z} \in \mathbb{Z}^m$ (interpreting each coordinate of $\mathbf{x}$ as an integer in $\{0, \ldots, p-1\}$), and output $\mathsf{sk}_\mathbf{x} = \mathbf{z_x}$.
- $\mathit{IPFE}.\mathsf{Enc}(\mathsf{pk}, \mathbf{y})$. To encrypt a vector $\mathbf{y} \in \mathbb{Z}_p^\ell$, sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e}_0 \leftarrow D_{\mathbb{Z}^m, \alpha q}$, $\mathbf{e}_1 \leftarrow D_{\mathbb{Z}^l, \alpha' q}$ and compute

$$\mathbf{c}_0 = \mathbf{A}\mathbf{s} + \mathbf{e}_0 \in \mathbb{Z}_q^m, \qquad \mathbf{c}_1 = \mathbf{T}\mathbf{s} + \mathbf{e}_1 + p^{e-1} \cdot \mathbf{y} \in \mathbb{Z}_q^\ell.$$

  Then, return the ciphertext $C = (\mathbf{c}_0, \mathbf{c}_1)$.
- $\mathit{IPFE}.\mathsf{Dec}(\mathsf{sk}, C)$. Given $C = (\mathbf{c}_0, \mathbf{c}_1)$ and secret key $\mathsf{sk}_\mathbf{x} = \mathbf{z_x}$, compute $\mu' = \langle \mathbf{x}, \mathbf{c}_1 \rangle - \langle \mathbf{z_x}, \mathbf{c}_0 \rangle \bmod q$, and output the value $\mu \in \mathbb{Z}_p$ that minimize $|\mu' - p^{e-1}\mu|$.

In [26], the dimensions n is proportional to the security parameter λ, the parameters $\ell, m, p, q, 1/\alpha, 1/\alpha'$ are polynomial in n, and e is a constant. In [26, Theorem 3.5], the authors state that under the LWE assumption, the above functional encryption for inner products is adaptively secure for chosen message distributions, assuming that the secret key queries corresponding are linearly independent.

Below, we describe a cryptanalysis of the scheme above with the specified parameters. We then explain why this attack does not apply to the schemes from [5] and [4].

We show that even for with challenge vectors rather than distributions, key queries allow to recover the master secret key msk. Concretely, we can recover $\mathbf{Z}$ from $\mathbf{X}^t$ and $\mathbf{X}^t\mathbf{Z}$, where $\mathbf{Z} \leftarrow \{0, \ldots, p-1\}^{\ell \times m}$ and $\mathbf{X} \in \{0, \ldots, p-1\}^{\ell \times (\ell-1)}$ is chosen by the adversary. We let our adversary sample $\mathbf{X} \leftarrow \{0, \ldots, p-1\}^{\ell \times (\ell-1)}$ (recall that the multiplication $\mathbf{X}^t\mathbf{Z}$ is over $\mathbb{Z}$). The fact that $\mathbf{X}$ has only $\ell - 1$ columns means that we can find distinct challenge plaintexts (which are elements of $\mathbb{Z}_p^\ell$) so that the columns of $\mathbf{X}$ are valid key queries.

It suffices to show how the adversary can recover the first column $\mathbf{z}$ of $\mathbf{Z}$ from $\mathbf{X}^t\mathbf{z}$, as it can proceed similarly for all columns of $\mathbf{Z}$. Given $\mathbf{t} = \mathbf{X}^t\mathbf{z}$ and $\mathbf{X}$, we know that $\mathbf{z}$ belongs to a coset of the lattice $\Lambda^\perp(\mathbf{X})$ defined by $\mathbf{t}$.

Let us now study the lattice $\Lambda^\perp(\mathbf{X})$. As $\mathbf{X} \leftarrow \{0, \ldots, p-1\}^{\ell \times (\ell-1)}$, its columns are expected to be linearly independent with overwhelming probability and $\det(\mathbf{X}\mathbb{Z}^{\ell-1})$ is expected to grow as $p^{\Omega(\ell)}$. These properties would be easier to prove if the entries of $\mathbf{X}$ were Gaussian with standard deviation p, but it can be experimentally checked that this behaviour also holds for this distribution. We also expect the lattice $\mathbf{X}\mathbb{Z}^{\ell-1}$ to be primitive, i.e., that $\mathbf{X}^t\mathbb{Z}^\ell = \mathbb{Z}^{\ell-1}$. By [23, p. 30], we hence have that $\det(\Lambda^\perp(\mathbf{X})) = \det(\mathbf{X}\mathbb{Z}^{\ell-1})$. As $\mathbf{X}$ is full column-rank, we known that $\dim(\Lambda^\perp(\mathbf{X})) = 1$, and hence we expect that $\lambda_1(\Lambda^\perp(\mathbf{X})) = p^{\Omega(\ell)}$. Finally, note that the orthogonal lattice can be efficiently computed, by using a Hermite Normal Form algorithm.

Now, recall that we want to recover $\mathbf{z}$ from a known coset of $\Lambda^\perp(\mathbf{X})$. As $\|\mathbf{z}\| \leq \sqrt{\ell}p$, by the above analysis of $\Lambda^\perp(\mathbf{X})$, we expect to have

$$\|\mathbf{z}\| < \lambda_1(\Lambda^\perp(\mathbf{X}))/2.$$

This implies that $\mathbf{z}$ is uniquely determined from the coset. Moreover, this is a Bounded Distance Decoding problem instance in a lattice of dimension 1, which

can be solved efficiently. Concretely, if $\Lambda^{\perp}(\mathbf{X}) = \mathbf{b}\mathbb{Z}$ and we are given $\mathbf{b}$ and $k\mathbf{b} + \mathbf{z}$, we can recover $k = \lfloor \langle k\mathbf{b} + \mathbf{z}, \mathbf{b} \rangle / \|\mathbf{b}\|^2 \rceil$ and hence $\mathbf{z}$.

Remarks. Our proof shows that the scheme from [26] is not secure with the specified parameters. We explain here why the above attack does not work for the [5] and [4] schemes. First, in the mod-p scheme from [5, Section 4.1], the authors take $\mathbf{z}$ from a discrete Gaussian distribution with a large standard deviation. With the parameters specified in [5], we then have that $\|\mathbf{z}\|$ is significantly larger than $\lambda_1(\Lambda^{\perp}(\mathbf{X}))$. This implies that there is a large amount of entropy left in $\mathbf{z}$ given $\mathbf{t} = \mathbf{X}^t\mathbf{z}$. Also, this attack does not work for the [5] scheme over $\mathbb{Z}$, because in that case, the matrix $\mathbf{X}$ and hence the lattice $\Lambda^{\perp}(\mathbf{X})$ are not random at all. Indeed, the kernel lattice is forced to be $(\mathbf{y}_0 - \mathbf{y}_1)\mathbb{Z}^{\ell}$, where $\mathbf{y}_0$ and $\mathbf{y}_1$ are the challenge vectors. By assumption on the scheme, these challenge vectors are small. Put differently, in that setting, if we first do $(\ell - 1)$ random queries, there does not exist $\mathbf{y}_0 - \mathbf{y}_1 \neq \mathbf{0}$ short anymore that allows us to create a non-trivial challenge phase. Finally, the attack does not work for the [4] scheme variant, because in that case, the matrix $\mathbf{X}$ has much fewer columns than rows. This increases the dimension of $\Lambda^{\perp}(\mathbf{X})$ enough to make $\lambda_1(\Lambda^{\perp}(\mathbf{X}))$ much smaller, and in particular smaller than $\|\mathbf{z}\|$.

5 Linear Functional Encryptions in Prime-Order Groups

As outlined in Sect. 3, our trace-and-revoke schemes are instantiated using different linear functional encryption schemes. In this section, we give a construction of $\mathcal{MMFE}$ in the symmetric-key setting. For $n = 1$, the $\mathcal{MMFE}$ construction reduces to IPFE. Due to space restraint, we omit the description of IPFE and present the $\mathcal{MMFE}$ below. The point of interest being, the Dec in our $\mathcal{MMFE}$ (and in our IPFE) does not compute the discrete log.

5.1 $\mathcal{MMFE}$ from $\mathcal{D}_k$-matDH

We propose a construction of matrix multiplication functional encryption ($\mathcal{MMFE}$) from $\mathcal{D}_k$-matDH. Since, the complete matrix $\mathbf{M} = (\mathbf{y}_1, \ldots, \mathbf{y}_n)^{\top}$ is available to Enc at once, our construction can reuse the randomness for all $\mathbf{y}_i \in \mathbb{Z}_p^{\ell}$. This also allows the proof to be tightly reduced to $\mathcal{D}_k$-matDH. For this, we require n matrices $\mathbf{W}_1, \ldots, \mathbf{W}_n$ unlike IPFE from $\mathcal{D}_k$-matDH that required only one. We emphasize that, similar to IPFE above, $\mathcal{MMFE}$ also does not need to evaluate discrete logarithm algorithm.

- $\mathsf{Setup}(1^{\lambda}, 1^{\ell}, 1^{n}, p)$. Run $(g, \mathbb{G}) \leftarrow \mathcal{G}_{gen}(1^{\lambda}, p)$. Sample $\mathbf{A} \leftarrow \mathcal{D}_k$ and $\mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{\ell \times k\ell n}$. Define $\mathsf{msk} = (\mathbf{W}_1, \ldots, \mathbf{W}_n)$ and $\mathsf{pp} = ([1])$.
- $\mathsf{KeyGen}(\mathsf{pp}, \mathsf{msk}, \mathbf{x} \in \mathbb{Z}_p^{\ell})$. Set $\mathsf{sk}_{\mathbf{x}} \leftarrow (\mathbf{x}^{\top}\mathbf{W}_1, \ldots, \mathbf{x}^{\top}\mathbf{W}_n, \mathbf{x})$.
- $\mathsf{Enc}(\mathsf{pp}, \mathsf{msk}, \mathbf{M} = (\mathbf{y}_1, \ldots, \mathbf{y}_n)^{\top} \in \mathbb{Z}_p^{n \times \ell})$ proceeds as follows to encrypt the given vectors $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \mathbb{Z}_p^{\ell}$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{k\ell n}$. Set $\mathsf{ct}_{\mathbf{M}} \leftarrow ([\mathbf{s}], [\mathbf{y}_1 + \mathbf{W}_1\mathbf{s}], \ldots, [\mathbf{y}_n + \mathbf{W}_n\mathbf{s}])$.

- $\mathsf{Dec}(\mathsf{pp}, \mathsf{sk}_{\mathbf{x}}, \mathsf{ct}_{\mathbf{M}})$. Parse $\mathsf{ct}_{\mathbf{M}} = ([\mathbf{c}_0], [\mathbf{c}_1], \ldots, [\mathbf{c}_n])$. Return $\mathbf{t} = (t_1, \ldots, t_n)$ where $t_i = \left[\mathbf{x}^\top \mathbf{c}_i\right] \cdot \left[\mathsf{sk}_{\mathbf{x}} \cdot \mathbf{c}_0\right]^{-1}$.

The correctness is easy to verify.

We show a rough comparison of our scheme with [25] if their scheme was used for symmetric key settings directly. Section 1 shows that the symmetric key variant resulted from hiding the public key of [25] has bigger public parameters and bigger ciphertext i.e. contain more group elements than our scheme. On the other hand, our secret key contains more elements from $\mathbb{Z}_p$. Both the schemes are proven secure under same assumption $\mathcal{D}_k$-matDH with constant degradation. We further compare the result for the SXDH based instances which shows that their scheme outputs ciphertext that is 1.5 times bigger than us.

Table 1. Comparison of naive application of [25] with our construction in symmetric-key settings. The sizes of pp and ct are in number of group elements, whereas those of the sk column are in number of elements of $\mathbb{Z}_p$.

	$\lvert\mathsf{pp}\rvert$	$\lvert\mathsf{sk}\rvert$	$\lvert\mathsf{ct}\rvert$	Degradation	Assumption
[25]	$k^3(k+1)\ell^2 + k^2\ell^2$	$(k+1)k\ell$	$n((k+1)k\ell + \ell)$	4	$\mathcal{D}_k$-matDH
	$2\ell^2 + \ell^2$	2ℓ	$3n\ell$	4	SXDH
This work	1	$k\ell n^2$	$k\ell n + \ell n$	$k+1$	$\mathcal{D}_k$-matDH
	1	$n^2\ell$	$2n\ell$	2	SXDH

Security. Next, we argue the security of $\mathcal{MMFE}$ in the IND-CPA security model. Our construction is basically a modification of [25] for symmetric-key settings. This improves upon the performance in terms of ciphertext size and removes the usage of public parameters completely. Note that, this modification required us to argue the security proof in a different manner. Although the overall proof strategy stayed more-or-less the same, our proof presents a completely new proof for an essential lemma. We state the security theorem next and defer the proof to the full version due to space restraint.

Theorem 8. *For any adversary $\mathcal{A}$ of the construction $\mathcal{MMFE}$ in the* IND-CPA *security model that makes at most q_{sk} secret key queries (for $q_{\mathsf{sk}} < \ell$) and q_{ct} challenge ciphertext queries in an interleaved manner, there exists adversary $\mathcal{C}$ such that,*

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{MMFE},\mathcal{A}}(\lambda) \leq (k+1) \cdot \mathrm{Adv}^{\mathcal{D}_k\text{-}\mathsf{matDH}}_{\mathcal{C}}(\lambda).$$

Acknowledgments. The authors thank Benoît Libert for interesting discussions. This work was supported in part by European Union Horizon 2020 Research and Innovation Program Grant 780701 and by BPI-France in the context of the national project RISQ (P141580).

References

1. Abdalla, M., Bourse, F., De Caro, A., Pointcheval, D.: Simple functional encryption schemes for inner products. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 733–751. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_33
2. Abdalla, M., Catalano, D., Fiore, D., Gay, R., Ursu, B.: Multi-input functional encryption for inner products: function-hiding realizations and constructions without pairings. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 597–627. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_20
3. Abdalla, M., Gay, R., Raykova, M., Wee, H.: Multi-input inner-product functional encryption from pairings. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 601–626. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_21
4. Agrawal, S., Bhattacherjee, S., Phan, D.H., Stehlé, D., Yamada, S.: Efficient public trace and revoke from standard assumptions: extended abstract. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017, pp. 2277–2293. ACM Press, October/November 2017. https://doi.org/10.1145/3133956.3134041
5. Agrawal, S., Libert, B., Stehlé, D.: Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9816, pp. 333–362. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53015-3_12
6. Agrawal, S., Yamada, S.: Optimal broadcast encryption from pairings and LWE. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12105, pp. 13–43. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45721-1_2
7. Barth, A., Boneh, D., Waters, B.: Privacy in encrypted content distribution using private broadcast encryption. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 52–64. Springer, Heidelberg (2006). https://doi.org/10.1007/11889663_4
8. Boneh, D., Franklin, M.: An efficient public key traitor tracing scheme. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 338–353. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_22
9. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005). https://doi.org/10.1007/11535218_16
10. Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_16
11. Boneh, D., Waters, B.: A fully collusion resistant broadcast, trace, and revoke system. In: Juels, A., Wright, R.N., De Capitani di Vimercati, S. (eds.) ACM CCS 2006, pp. 211–220. ACM Press, October/November 2006. https://doi.org/10.1145/1180405.1180432
12. Castagnos, G., Laguillaumie, F., Tucker, I.: Practical fully secure unrestricted inner product functional encryption modulo p. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11273, pp. 733–764. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03329-3_25
13. Do, X.T., Phan, D.H., Yung, M.: A concise bounded anonymous broadcast yielding combinatorial trace-and-revoke schemes. In: Conti, M., Zhou, J., Casalicchio, E., Spognardi, A. (eds.) ACNS 2020. LNCS, vol. 12147, pp. 145–164. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-57878-7_8

14. Dodis, Y., Fazio, N.: Public key trace and revoke scheme secure against adaptive chosen ciphertext attack. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 100–115. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36288-6_8
15. Fazio, N., Perera, I.M.: Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 225–242. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_14
16. Goyal, R., Koppula, V., Waters, B.: Collusion resistant traitor tracing from learning with errors. In: Diakonikolas, I., Kempe, D., Henzinger, M. (eds.) 50th ACM STOC, pp. 660–670. ACM Press, June 2018. https://doi.org/10.1145/3188745.3188844
17. Kiayias, A., Samari, K.: Lower bounds for private broadcast encryption. In: Kirchner, M., Ghosal, D. (eds.) IH 2012. LNCS, vol. 7692, pp. 176–190. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36373-3_12
18. Kim, C.H., Hwang, Y.H., Lee, P.J.: An efficient public key trace and revoke scheme secure against adaptive chosen ciphertext attack. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 359–373. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40061-5_23
19. Li, J., Gong, J.: Improved anonymous broadcast encryptions. In: Preneel, B., Vercauteren, F. (eds.) ACNS 2018. LNCS, vol. 10892, pp. 497–515. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93387-0_26
20. Libert, B., Paterson, K.G., Quaglia, E.A.: Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 206–224. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_13
21. Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_3
22. Naor, M., Pinkas, B.: Efficient trace and revoke schemes. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 1–20. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45472-1_1
23. Nguyen, P.: La géométrie des nombres en cryptologie. Ph.D. thesis, Université Paris 7 (1999)
24. Nishimaki, R., Wichs, D., Zhandry, M.: Anonymous traitor tracing: how to embed arbitrary information in a key. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 388–419. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_14
25. Tomida, J.: Tightly secure inner product functional encryption: multi-input and function-hiding constructions. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11923, pp. 459–488. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34618-8_16
26. Wang, Z., Fan, X., Liu, F.-H.: FE for inner products and its application to decentralized ABE. In: Lin, D., Sako, K. (eds.) PKC 2019. LNCS, vol. 11443, pp. 97–127. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17259-6_4