Ad Hoc (Decentralized) Broadcast, Trace, and Revoke

罗辑 (Ji Luo)

Paul G. Allen School of Computer Science & Engineering,
University of Washington, Seattle, USA
luoji@cs.washington.edu

12 March 2023

Abstract

Traitor tracing schemes [Chor–Fiat–Naor, Crypto ’94] help content distributors fight against piracy and are defined with the content distributor as a trusted authority having access to the secret keys of all users. While the traditional model caters well to its original motivation, its centralized nature makes it unsuitable for many scenarios. For usage among mutually untrusted parties, a notion of ad hoc traitor tracing (naturally with the capability of broadcast and revocation) is proposed and studied in this work. Such a scheme allows users in the system to generate their own public/secret key pairs, without trusting any other entity. To encrypt, a list of public keys is used to identify the set of recipients, and decryption is possible with a secret key for any of the public keys in the list. In addition, there is a tracing algorithm that given a list of recipients’ public keys and a pirate decoder capable of decrypting ciphertexts encrypted to them, identifies at least one recipient whose secret key must have been used to construct the said decoder.

Two constructions are presented. The first is based on obfuscation and has constant-size ciphertext, yet its decryption time is linear in the number of recipients. The second is a generic transformation that reduces decryption time at the cost of increased ciphertext size. A lower bound on the trade-off between ciphertext size and decryption time is shown, indicating that the two constructions achieve all possible optimal trade-offs, i.e., they fully demonstrate the Pareto front of efficiency. The lower bound also applies to broadcast encryption and is of independent interest.

Keywords. traitor tracing, broadcast encryption, obfuscation.

This research is “open-thoughts”. See https://github.com/GeeLaw/ahbtr.
1 Introduction

Traitor tracing schemes [CFN94] enable content distributors to fight against piracy. A content distributor such as a media streaming service can generate a public key and many different secret keys for individual subscribers, all of which can decrypt the ciphertexts created using the public key. Given a pirate decoder capable of decrypting, which could have been created from the secret keys of multiple subscribers, the tracing algorithm can find at least one subscriber (a traitor) whose key was used to create the said decoder. A long line of subsequent works [BSW06,BW06,BN08,BZ14,NWZ16,GKW18,GKW18,CGW+18,GWW19,GKW19,Zha20a,Zha21] proposed the different security definitions, extended the functionality, and presented new constructions.

While the traditional model caters well to the needs of content distributors, its centralized nature makes it unsuitable for many scenarios, e.g., when a group of individuals want to communicate among themselves and trace traitors who provide decoders to outsiders. For example [Zha21], in an encrypted group chat among protesters, the users are worried about potential infiltration by government agents. To mitigate this concern, they want to trace traitors and remove them from the group. If they used a traditional traitor tracing scheme, whoever set it up would be able to impersonate anyone since they would know all the secret keys. Moreover, as words are spread and the protest gets wider support, more people need to join the group. The joining process should as simple as possible, preferably without interaction. This motivation naturally calls for a decentralized notion of traitor tracing, termed ad hoc traitor tracing in this work.

The first question is thus naturally the following:

What is the right notion of a secure ad hoc traitor tracing scheme?

Having formalized its syntax and security, we study its constructions:

How can such a scheme be constructed, from what assumptions, and with what efficiency?

Efficiency improvement never ends until we reach the optimum, for which it is necessary to understand where the limit stands:

What bounds are there on the efficiency of such schemes?

Our Contributions. We provide answers to all three questions:

• Conceptually, we pose the question of ad hoc traitor tracing, develop from the ideas thereof, and eventually arrive at the definitions for ad hoc broadcast, trace, and revoke (AH-BTR). We prove the relation among the security notions considered in this work.

• Construction-wise, we present secure AH-BTR schemes based on functional encryption for general circuits [BSW11]. With polynomial factors in the security parameter ignored, they achieve

$$T_{\text{Enc}} = O(N),$$
$$|\text{ct}| = O(N^{1-\gamma}),$$
$$T_{\text{Dec}} = O(N^\gamma),$$

for any constant $0 \leq \gamma \leq 1$. 

1 / 34
• Questing for the ultimate efficiency, we prove that for all secure AH-BTR,
  \[ |\text{ct}| \cdot T_{\text{Dec}} = \Omega(N), \]
so our schemes offer all possible optimal trade-offs between $|\text{ct}|$ and $T_{\text{Dec}}$, fully
demonstrating the Pareto front of AH-BTR efficiency. Better yet, the bound holds
for a restricted kind of weakly secure broadcast encryption [FN94], which is a
specific case of attribute-based encryption [SW05,GPSW06]. Our result is the first
time-space lower bound applicable to any computationally secure BE scheme,\(^1\)
shedding new insights into the efficiency of ABE and BE.

A final addition is that our scheme is compatible with the existing public-key encryption
schemes, i.e., the keys of such a scheme can be those of any secure public-key
encryption, and there is no need to regenerate keys to take advantage of our scheme.

Open Questions. The tracing model in this work is black-box and classical, and recent
works [Zha21,Zha20c] have studied white-box or quantum traitor tracing. Conceptually,
it is interesting to understand the ad hoc versions of those tracing models.

Another question for future investigation is whether (weakened versions of) AH-BTR
can be constructed from more lightweight assumptions such as factoring-related, group-
based, or lattice-based assumptions. Potential relaxations include making the scheme
bounded,\(^2\) settling for static security, considering security against bounded collusion,
and only achieving threshold tracing [NP98].

1.1 Overview

Developing Definitions. We start with the first principles of ad hoc traitor tracing.
Syntactically, there should be a key generation algorithm that is run by each user of
the system.\(^3\) To encrypt, a list of public keys is used to identify the set of recipients.
Decryption should only require one secret key from the list of public keys. In addition,
the decryptor gets random access to all the recipients’ public keys as well as the
ciphertext. The choice to give random access to these inputs is based on performance
concerns, as the decryptor might not have to read all of the public keys or the ciphertext.

It should be clear that such a scheme would automatically have the functionality of
broadcast encryption [FN94].\(^4\) There is no event prior to encryption that “binds” the
system to a specific, fixed set of possible recipients, and the encryptor is free to use
whatever public keys it sees fit. Similarly, the encryptor can remove any public key
when it encrypts a second ciphertext, i.e., the scheme supports revocation. Therefore,
the object is named ad hoc broadcast, trace, and revoke (AH-BTR).

As usual with broadcast encryption, we do not hide the list of recipients. Hiding
the recipients makes ciphertext grow at least linearly with the number of recipients,

\(^1\)Previous works [BC95,LS98,KYDB98,AK08,KY09,GKW15,DLY21] show a few efficiency lower bounds
related to ABE and BE. Yet they only apply to information-theoretically secure primitives and even specific
construction techniques. Moreover, all of them are space (ciphertext or secret key size, or their trade-
off) lower bounds. Indeed, based on obfuscation [BWZ14] or both LWE and pairing [AY20], BE with
$|\text{ct}|,|\text{sk}| = O(1)$ can be constructed.

\(^2\)A maximum of number of recipients per ciphertext is set when generating a key pair, and only
“compatible” public keys can be used to form a recipient set.

\(^3\)We aim for a scheme without any trusted party, so there should be no global set-up.

\(^4\)Decentralized versions of broadcast encryption were studied in [PPS12,DPP07] with interactive
management of recipient sets. Ad hoc (threshold) broadcast encryption was studied in [DHMR08,WQZD10]
with constructions for bounded schemes requiring global set-up.
diminishing the potential of efficiency. As we shall see, it is possible to construct AH-BTR with short ciphertexts.

Due to the decentralized nature of such systems, an adversary might indistinguishably generate malformed keys, which could potentially evade tracers that only take well-formed keys into account. To make it worse, a malformed key could be used to mount a denial-of-service attack against (other) honest users if it appears in the list of recipients’ public keys during encryption — the encryption algorithm might have been carelessly designed and the presence of certain malformed keys could make it impossible to decrypt for anyone, including the recipients with honestly generated public keys.

In order to protect against such attacks by definition, we require correctness be robust against malformed keys — however, for performance reasons, namely to be able to index into any particular public key in constant time, we reject blatantly malformed keys, e.g., those of incorrect lengths, in the definition of correctness. This restriction does not hamper the usefulness of such a scheme.

As for security, when attacking the traceability of the scheme, the adversary is allowed to supply an arbitrary list of recipients’ public keys, generated honestly by the challenger or (adversarially) by the adversary, so that the definition covers the scenario when (blatantly or not) malformed keys are present in the list of recipients’ public keys. The tracing algorithm is given oracle access to a stateless decoder. It must not accuse an honest user, defined as one whose public key is generated by the challenger without its secret key revealed to the adversary. It must find a traitor as long as the decoder has sufficient advantage (i.e., succeeds in decrypting with sufficient probability), where traitors are associated with public keys in the recipient list that are either generated by the challenger with their secret keys revealed to the adversary or crafted by the adversary in any manner (e.g., skewed distribution, or even without a well-defined secret key).

Once the issues above are identified and conceptually resolved (as done here), it is straight-forward to define AH-BTR analogously to traditional broadcast, revoke, and trace schemes [NP01,NNL01,GQWW19].

Simplifying Security Notions. Traditionally [BSW06], traceability has been defined using one comprehensive interactive experiment, which is complicated to work with. Intuitively, the notion requires that i) a traitor should be found from a decoder with sufficient advantage and ii) no honest user should be identified as a traitor, regardless of the decoder advantage.

We thus define two security notions for AH-BTR capturing the requirements separately. The former is called completeness and the latter is called soundness. Their conjunction is equivalent to traceability. Since only one requirement is considered in each notion, both of them can be vastly simplified and the interactions in those notions are minimal. They are also more convenient for reductionist proofs.

Construction. Our first construction of AH-BTR follows the existing blueprint of traitor tracing schemes from private linear broadcast encryption (PLBE) schemes introduced in [BSW06]. We first define an ad hoc version of PLBE.\(^7\)

\(^5\)The general transformation [KY01,BSW06] to deal with stateful decoder applies to our definition of AH-BTR, mutatis mutandis.

\(^6\)While some previous works [BF99,GKW18,Zha20a] separate traceability into multiple notions, those notions still share one single complicated security experiment.

\(^7\)AH-PLBE can be cast as multi-authority attribute-based encryption [Cha07] for 1-local monotone functions without global set-up.
• Everyone generates their own public and secret key pair \((pk, sk)\).

• Encryption uses a list \(\{pk_j\}_{j \in [N]}\) of \(N\) public keys of the recipients as well as a cut-off index \(0 \leq i_\perp \leq N\).

• Decryption is possible with \(sk_j\) if \(j > i_\perp\).

There are two security requirements. Message-hiding requires that the plaintext is hidden if \(i_\perp = N\). Index-hiding requires that an adversary without \(sk_j\) for an \textit{honest} \(pk_j\) cannot distinguish between cut-off index being \((j-1)\) versus \(j\).

Colloquially, the cut-off index \(i_\perp\) disables \(sk_1, \ldots, sk_{i_\perp}\), and the only way to detect whether an index is disabled is to have control over the corresponding key pair (by knowing \(sk\) or generating a malformed \(pk\)). When \(i_\perp = N\), the plaintext should be hidden since all keys are disabled.

Given an AH-PLBE scheme, an AH-BTR scheme can be constructed by adapting the work of [BSW06]. The AH-BTR inherits key generation and decryption algorithms from AH-PLBE. To perform AH-BTR encryption, simply encrypt using AH-PLBE with \(i_\perp = 0\), disabling no key so that every recipient can decrypt. Given a pirate decoder with advantage at least \(\epsilon\), the tracing algorithm computes its advantages with the cut-off index \(i_\perp\) being \(0, 1, 2, \ldots, N\), and identifies the recipient associated with \(pk_{i^*}\) as a traitor if the advantage changes by \(\Omega(\epsilon/N)\) when \(i_\perp\) increases from \((i^* - 1)\) to \(i^*\).

The message-hiding property translates to completeness, and index-hiding to soundness. It now remains to construct an AH-PLBE.

\textit{Constructing AH-PLBE.} It is folklore that any public-key encryption (PKE) scheme can be used to construct a naïve PLBE by encrypting individually to each recipient. The individual ciphertext that corresponds to a disabled key encrypts garbage instead of the actual plaintext. This scheme is also \textit{ad hoc}. The downside of it is that the ciphertext is of size \(\Omega(N)\).

Our scheme uses obfuscation to compress the naïve PLBE ciphertext. The ciphertext will contain an obfuscated program, which, when evaluated at \(j \in [N]\), allows us to recover the PKE ciphertext under \(pk_j\). However, the obfuscated program itself cannot simply compute each PKE ciphertext if we want AH-PLBE ciphertexts of size \(o(N)\), as there is no enough space in the program to encode all the public keys that have been independently generated.

Laconic oblivious transfer (OT) [CDG+17] comes to rescue. It allows compressing an arbitrarily long string \(D\) down to a fixed-length hash \(h\) with which one can efficiently perform oblivious transfer. The sender can encrypt messages \(L_0, L_1\) to a hash \(h\) and an index \(m\) into \(D\). The time to encrypt is independent of the length of \(D\). The receiver will be able to obtain \(L_{D[m]}\) by decrypting the laconic OT ciphertext.

During AH-PLBE encryption, we use laconic OT to compress the list of public keys. The obfuscated program in our AH-PLBE ciphertext, when evaluated at \(j \in [N]\), will output \(i\) a garbled circuit whose input (resp. output) is a PKE public key (resp. ciphertext) and \(ii\) a bunch of laconic OT ciphertexts that decrypts to the labels so that the garbled circuit is evaluated at \(pk_j\). Decryption proceeds in the obvious manner.

The obfuscated program size, thus the ciphertext size, can be made constant,\(^8\)

\[^8\text{We ignore fixed polynomial factors in the security parameter. The point is that the size does not grow with } N \text{ (the number of recipients).}\]
because both the time to garble a PKE encryption circuit and the time of laconic OT encryptions are constant.

**You Can (Not) Optimize.** While our basic construction enjoys constant-size ciphertext, its decryption algorithm runs in time \(\Omega(N)\). Concretely, the laconic OT hash is a Merkle tree, and before performing laconic OT decryption, it is necessary to reconstruct the tree as it is not stored in the ciphertext. In contrast, the decryption time of the scheme implied by the naïve PLBE is constant in the RAM model, as it only looks at the relevant piece of the underlying PKE ciphertext.

We can trade ciphertext size for decryption time by using the naïve PLBE on top of our construction. By grouping the recipients into \(\Theta(N^{1-\gamma})\) sets of size \(\Theta(N^\gamma)\) and using our basic construction over each set, we obtain a scheme with ciphertext size \(\Theta(N^{1-\gamma})\) and decryption time \(\Theta(N^\gamma)\). The core idea of this transformation was formalized as the user expansion compiler [Zha20a] in the context of traditional traitor tracing.

All the constructions we now know have \(|ct| \cdot T_{Dec} = \Omega(N)\), where \(|ct|\) is the ciphertext length and \(T_{Dec}\) is the decryption time. It turns out that this bound necessarily holds for all secure AH-BTR, and the blame is on the functionality of broadcast encryption (not traitor tracing). Indeed, it is possible to make both \(|ct|\) and \(T_{Dec}\) constant in a traditional traitor tracing scheme [BZ14]. In existing broadcast encryption (or revocation) schemes [BGW05,Del07,GW09,BZ14,AY20,AWY20,BV20] for \(N\) users, encrypting to arbitrary subsets of size \(S\) or \((N - S)\) makes \(|ct| \cdot T_{Dec} = \Omega(S)\). It is precisely the capability to encrypt to many \(\Theta(N)\)-subsets among \(N\) users that is the deal breaker, as we shall see in the formal proof. Interestingly, the adversary used in the proof is simply the decryption algorithm, so the bound holds as long as the scheme is not **blatantly** insecure.

We explain the ideas of our proof based on a corollary\(^9\) of a result [Unr07] dealing with random oracles in the presence of non-uniform advice. Let \(S, T \geq 0\) be such that \(ST \ll N\). The corollary says that for any adversary learning any \(S\)-bit function (advice) of a random string \(R \leftarrow \{0,1\}^N\) and additionally (adaptively) querying at most \(T\) bits in \(R\), it is “indistinguishable” to flip a bit in \(R\) at a random location after the advice is computed (using the non-flipped \(R\)) and before queries are answered, even if the index of the potentially flipped bit is revealed to the adversary after the advice is computed.

Back to AH-BTR. Imagine that there are \(2N\) users in the system, associated with key pairs \((pk_{j,s},sk_{j,s})\) for \(j \in [N]\) and \(s \in \{0,1\}\). Consider a ciphertext \(ct\) encrypting a random plaintext \(\{pk_{j,R[j]}\}_{j \in [N]}\) for a random string \(R\) and regard \(ct\) as the advice. Let’s try decrypting \(ct\) using \(sk_{i^*,R[i^*]}\) for a random \(i^* \leftarrow [N]\). Each time the AH-BTR decryption algorithm queries \(pk_{j}\), we probe \(R[j]\) and respond with \(pk_{j,R[j]}\). By way of contradiction, suppose \(|ct| \cdot T_{Dec} \ll N\), which would translate to the setting of the corollary as \(S = |ct|, T \leq T_{Dec},\) and \(ST \ll N\).

By the correctness of AH-BTR, the attempted decryption should successfully recover the plaintext. From the corollary it follows that flipping \(R[i^*]\) should also lead to successful recovery. But if \(R[i^*]\) is flipped after \(ct\) is computed, by the security of AH-BTR, the attempted decryption must fail to recover the plaintext except for negligible probability, yielding a contradiction.

---

\(^9\)This corollary is also a lower bound of a probabilistic variant of Yao’s box problem [Yao90] (generalized and studied in [CHK22]), on which our proof can be alternatively based.
2 Preliminaries

We denote by $\lambda \in \mathbb{N}$ the security parameter, by $\text{poly}()$ a polynomial function, and by $\text{negl}(\cdot)$ a negligible function of $\cdot$. Efficient algorithms are probabilistic random-access machines $M^w(x)$ of running time $\text{poly}(|x|,|w|)$. Efficient adversaries (in interactive experiments) are probabilistic Turing machines of (total) running time $\text{poly}(\lambda)$, with or without $\text{poly}(\lambda)$-long advices. (All of the proofs in this work are uniform.) The advantage of $\mathcal{A}$ in distinguishing $\text{Exp}_0$ and $\text{Exp}_1$ is $\Pr[\text{Exp}_0^A(1^\lambda) = 1] - \Pr[\text{Exp}_1^A(1^\lambda) = 1]$. We write $\approx$, $\equiv$, $\approx$ for computational indistinguishability, statistical indistinguishability, and identity.

Under the standard assumption that a pseudorandom generator (with polynomial security) exists, we can assume, whenever convenient, that a randomized algorithm uses a uniformly random $\lambda$-bit string as its randomness (without losing polynomial security considered in this work or degrading its efficiency).

For $n, n' \in \mathbb{N}$, we write $[n..n']$ for the set $\{n, \ldots, n'\}$, and $[n]$ for $[1..n]$. For a bit-string $D$, we denote by $|D|$ its bit-length, and given an index $m \in [|D|]$, we denote by $D[m]$ the $m^{\text{th}}$ bit of $D$. For two bit-strings $D, D'$, their concatenation is $D \| D'$. Given a circuit $C : \{0,1\}^{n+M_0} \rightarrow \{0,1\}^{n'}$ and $w \in \{0,1\}^n$, we define $C[w]$ to be $C$ with $w$ hardwired as its first portion of input, so $C[w](x) = C(w \| x)$. For an event $X$, its indicator random variable is $1_X$. For events $X, Y$ in the same probability space, “$X$ implies $Y$” means $X \subseteq Y$.

Garbled Circuits. The following version of partially hiding garbling [IW14] suffices for the purpose of this work.

**Definition 1** (garbled circuit [Yao86,LP09,BHR12,IW14]). A circuit garbling scheme consists of 2 efficient algorithms:

- $\text{Garble}(1^\lambda, C, w)$ takes as input a circuit $C : \{0,1\}^{n+M_0} \rightarrow \{0,1\}^{n'}$ and some hardwired input $w \in \{0,1\}^n$. It outputs a garbled circuit $\widehat{C}$ and $M_0$ pairs of labels $L_{m_0,b} \in \{0,1\}^\lambda$ for $m_0 \in [M_0]$, $b \in \{0,1\}$.

- $\text{Eval}(1^\lambda, \widehat{C}, x, \{L_{m_0} \mid m_0 \in [M_0]\})$ takes as input a garbled circuit, a non-hardwired input, and $M_0$ labels. It outputs an $n'$-bit string.

The scheme must be correct, i.e., for all $\lambda \in \mathbb{N}$, $n, M_0, n', M_0' \in \mathbb{N}$, $C : \{0,1\}^{n+M_0} \rightarrow \{0,1\}^{n'}$, $w \in \{0,1\}^n$, $x \in \{0,1\}^{M_0}$,

$$\Pr \left[ \left( \widehat{C}, \{L_{m_0,b} \mid m_0 \in [M_0], b \in \{0,1\}\} \right) \xleftarrow{\$} \text{Garble}(1^\lambda, C, w) : \text{Eval}(1^\lambda, \widehat{C}, x, \{L_{m_0} \mid m_0 \in [M_0]\}) = C[w](x) \right] = 1.$$

**Definition 2** (garbled circuit security [Yao86,LP09,BHR12,IW14]). Let (Garble, Eval) be a circuit garbling scheme (Definition 1). A simulator is an efficient algorithm

$$\text{SimGarble}(1^\lambda, C : \{0,1\}^{n+M_0} \rightarrow \{0,1\}^{n'}, x \in \{0,1\}^{M_0}, y \in \{0,1\}^{n'}) = (\widehat{C}, \{L_{m_0} \mid m_0 \in [M_0]\})$$

taking as input a circuit, a non-hardwired input, and a circuit output, and producing a simulated garbled circuit and $M_0$ simulated labels. The scheme is $w$-hiding (or secure for the purpose of this work) if there exists a simulator $\text{SimGarble}$ such that $\text{Exp}_0^w(1^\lambda) \approx \text{Exp}_1^w(1^\lambda)$ where $\text{Exp}_G(1^\lambda)$ with adversary $\mathcal{A}$ proceeds as follows:
• **Challenge.** Launch $\mathcal{A}(1^\lambda)$ and receive a circuit $C : \{0,1\}^{n+M_0} \rightarrow \{0,1\}^n$, a hardwired input $w \in \{0,1\}^n$, and a non-hardwired input $x \in \{0,1\}^{M_0}$ from it. Run

$$
\begin{align*}
\text{if } b = 0, & \quad (\hat{C}, \{L_{m_0,b} \}_{m_0 \in [M_0], b \in \{0,1\}}) \leftarrow \text{Garble}(1^\lambda, C, w); \\
\text{if } b = 1, & \quad (\hat{C}, \{L_{m_0,x[m_0]} \}_{m_0 \in [M_0]}) \leftarrow \text{SimGarble}(1^\lambda, C, x, C[w](x));
\end{align*}
$$

and send $(\hat{C}, \{L_{m_0,x[m_0]} \}_{m_0 \in [M_0]})$ to $\mathcal{A}$.

• **Guess.** $\mathcal{A}$ outputs a bit $b'$, which is the output of the experiment.

**Puncturable Pseudorandom Function.** We rely on PPRF $[BW13,KPTZ13,BGI14,SW14]$.

**Definition 3 (PPRF $[BW13,KPTZ13,BGI14,SW14]$).** A puncturable pseudorandom function (PPRF) family (with key space, domain, and codomain $\{0,1\}^\lambda$) consists of 2 efficient algorithms:

- Puncture$(1^\lambda, k \in \{0,1\}^\lambda, x)$ takes as input a non-punctured key and a point. It outputs a punctured key $\hat{k}_x$.
- Eval$(1^\lambda, k, x \in \{0,1\}^\lambda)$ takes as input a (punctured or non-punctured) key and a point. It is deterministic and outputs a $\lambda$-bit string.

The scheme must be correct, i.e., for all $\lambda \in \mathbb{N}$, $x, x' \in \{0,1\}^\lambda$ such that $x \neq x'$,

$$
\Pr \left[ \begin{array}{c}
k \leftarrow \{0,1\}^\lambda \\
\hat{k}_x \leftarrow \text{Puncture}(1^\lambda, k, x)
\end{array} \right] : \text{Eval}(1^\lambda, k, x') = \text{Eval}(1^\lambda, \hat{k}_x, x') = 1.
$$

**Definition 4 (PPRF security $[BW13,KPTZ13,BGI14,SW14]$).** A PPRF (Puncture, Eval) per Definition 3 is pseudorandom at the punctured point (or secure for the purpose of this work) if $\text{Exp}_b^\lambda \approx \text{Exp}_b^{\text{PPRF}(1^\lambda)}$, where $\text{Exp}_b^{\text{PPRF}(1^\lambda)}$ with adversary $\mathcal{A}$ proceeds as follows:

- **Challenge.** Launch $\mathcal{A}(1^\lambda)$ and receive from it a point $x \in \{0,1\}^\lambda$. Run

$$
k \leftarrow \{0,1\}^\lambda, \quad \hat{k}_x \leftarrow \text{Puncture}(1^\lambda, k, x), \quad r_0 \leftarrow \text{Eval}(1^\lambda, k, x), \quad r_1 \leftarrow \{0,1\}^\lambda,
$$

and send $(\hat{k}_x, r_b)$ to $\mathcal{A}$.

- **Guess.** $\mathcal{A}$ outputs a bit $b'$, which is the output of the experiment.

**Public-Key Encryption.** Our ad hoc broadcast, trace, and revoke scheme can be based on any public-key encryption scheme.

**Definition 5 (PKE).** A public-key encryption (PKE) scheme (with message space $\{0,1\}^\lambda$ and public key length $M_0(\lambda)$) consists of 3 efficient algorithms:

- Gen$(1^\lambda)$ outputs a pair $(pk, sk)$ of public and secret keys with $|pk| = M_0(\lambda)$.
- Enc$(1^\lambda, pk, \mu \in \{0,1\}^\lambda)$ takes as input the public key and a message. It outputs a ciphertext $ct$.
- Dec$(1^\lambda, sk, ct)$ takes as input the secret key and a ciphertext. It outputs a message.
The scheme must be correct, i.e., for all $\lambda \in \mathbb{N}$, $\mu \in \{0, 1\}^\lambda$,
\[
\Pr \left[ (pk, sk) \xleftarrow{\$} \text{Gen}(1^\lambda) : \text{Dec}(1^\lambda, sk) = \mu \right] = 1.
\]

**Definition 6** (PKE security). A PKE scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ per Definition 5 is semantically secure for random messages (or secure for the purpose of this work) if
\[
\{(1^\lambda, \mu_0, \mu_1, pk, ct_0) \} \approx \{(1^\lambda, \mu_0, \mu_1, pk, ct_1) \},
\]
where $(pk, sk) \xleftarrow{\$} \text{Gen}(1^\lambda)$ and $\mu_b \xleftarrow{\$} \{0, 1\}^\lambda$, $ct_b \xleftarrow{\$} \text{Enc}(1^\lambda, pk, \mu_b)$ for $b \in \{0, 1\}$.

**Laconic Oblivious Transfer.** We rely on laconic oblivious transfer [CDG+17].

**Definition 7** (laconic OT [CDG+17]). A laconic oblivious transfer (OT) scheme (with message space $\{0, 1\}^\lambda$) consists of 4 efficient algorithms:

- $\text{Gen}(1^\lambda, M \in \mathbb{N})$ takes the database length as input and outputs a hash key $hk$.
- $\text{Hash}(1^\lambda, hk, D \in \{0, 1\}^M)$ takes as input a hash key and a database. It is deterministic, runs in time $O(M) \text{poly}(\lambda, \log M)$, and outputs a hash $h$ of length $\text{poly}(\lambda, \log M)$ and a processed database $\tilde{D}$.
- $\text{Send}(1^\lambda, hk, h, m \in [M], L_0 \in \{0, 1\}^\lambda, L_1 \in \{0, 1\}^\lambda)$ takes as input a hash key, a hash, an index, and two labels (messages). It outputs a ciphertext $ct$.
- $\text{Recv}^\tilde{D}(1^\lambda, hk, h, m \in [M], ct)$ is given random access to a processed database, and takes as input a hash key, a hash, an index, and a ciphertext. It runs in time $\text{poly}(\lambda, \log M)$ and outputs a label (message).

The scheme must be correct, i.e., for all $\lambda, M \in \mathbb{N}$, $D \in \{0, 1\}^M$, $m \in [M]$, $L_0, L_1 \in \{0, 1\}^\lambda$,
\[
\Pr \left[ \begin{array}{c}
hk \xleftarrow{\$} \text{Gen}(1^\lambda, M) \\
(h, \tilde{D}) \leftarrow \text{Hash}(1^\lambda, hk, D) \\
ct \xleftarrow{\$} \text{Send}(1^\lambda, hk, h, m, L_0, L_1)
\end{array} : \text{Recv}^\tilde{D}(1^\lambda, hk, h, m, ct) = L_{D[m]} \right] = 1.
\]

We only need database-selective security [AL18]. The following indistinguishability-based definition is equivalent to the usual simulation-based formulation.

**Definition 8** (laconic OT security [CDG+17,AL18,KNTY19]). A laconic OT scheme $(\text{Gen}, \text{Hash}, \text{Send}, \text{Recv})$ per Definition 7 is database-selectively sender-private (or secure for the purpose of this work) if $\text{Exp}^0_{\text{LOT}} = \text{Exp}^1_{\text{LOT}}$, where $\text{Exp}^b_{\text{LOT}}(1^\lambda)$ with adversary $\mathcal{A}$ proceeds as follows:

- **Setup.** Launch $\mathcal{A}(1^\lambda)$ and receive from it some $M \in \mathbb{N}$ and a database $D \in \{0, 1\}^M$. Run
\[
\text{hk} \xleftarrow{\$} \text{Gen}(1^\lambda, M), \quad (h, \tilde{D}) \leftarrow \text{Hash}(1^\lambda, hk, D),
\]
and send $hk$ to $\mathcal{A}$. 

8 / 34
\[ \text{ct} \leftarrow \begin{cases} \text{Send}(1^A, h, h, m, L_0, L_1), & \text{if } b = 0; \\ \text{Send}(1^A, h, h, m, L_{D[m]}, L_{D[m]}), & \text{if } b = 1; \end{cases} \]

and send \( \text{ct} \) to \( A \).

- **Guess.** \( A \) outputs a bit \( b' \), which is the output of the experiment.

**Obfuscation.** We rely on indistinguishability obfuscator for polynomial-sized domain.

**Definition 9 ((circuit) obfuscator [BGI′01]).** A (circuit) obfuscator is an efficient algorithm \( \text{Obf}(1^A, C) \) taking a circuit \( C : \{0,1\}^n \rightarrow \{0,1\}^{n'} \) as input and producing a circuit \( \tilde{C} : \{0,1\}^n \rightarrow \{0,1\}^{n'} \) as output. The scheme must be correct, i.e., for all \( \lambda \in \mathbb{N}, n, n' \in \mathbb{N}, C : \{0,1\}^n \rightarrow \{0,1\}^{n'}, x \in \{0,1\}^n \),

\[
\Pr[\text{Obf}(1^A, C)(x) = C(x)] = 1.
\]

**Definition 10 (iO [BGI′01] for poly(\( \lambda \))-sized domain).** An obfuscator \( \text{Obf} \) (Definition 9) is a \textit{indistinguishability obfuscator for polynomial-sized domain} (iO for poly(\( \lambda \))-sized domain) if \( \text{Exp}_{iO}^0 \approx \text{Exp}_{iO}^1 \), where \( \text{Exp}_{iO}^b(1^A) \) with adversary \( A \) proceeds as follows:

- **Challenge.** Launch \( A(1^A) \) and receive from it the domain size \( 1^2^\lambda \) and two circuits \( C_0, C_1 : \{0,1\}^n \rightarrow \{0,1\}^{n'} \). Send \( \text{Obf}(1^A, C_b) \) to \( A \).

- **Guess.** \( A \) outputs a bit \( b' \). The output of the experiment is \( b' \) if \( C_0, C_1 \) have the same (description) size and \( C_0(x) = C_1(x) \) for all \( x \in \{0,1\}^n \). Otherwise, the output is set to 0.

**Assumption.** All of the primitives defined in this section are implied by the existence of weakly selectively secure, single key, and sublinearly succinct public-key functional encryption for general circuits (so-called obfuscation-minimum PKFE), of which we refer the reader to [KNTY19] for the precise definition.

**Lemma 1.** Suppose there exists an obfuscation-minimum PKFE with polynomial security, then there exist

- [Yao86,LP09,BHR12] a secure circuit garbling scheme (Definitions 1 and 2),
- [GGM84,BW13,KPTZ13,BGI14] a secure PPRF (Definitions 3 and 4),
- [folklore] a secure PKE scheme (Definitions 5 and 6),
- [CDG+17,LZ17,AL18,KNTY19] a secure laconic OT scheme (Definitions 7 and 8), and
- [LT17,LZ17] an iO for poly(\( \lambda \))-sized domain (Definitions 9 and 10),

with polynomial security.
Alternatively, those primitives can be based on the existence of \( iO \) and one-way function. However, \( iO \) security (for circuits whose domains are not necessarily \( \text{poly}(\lambda) \)-sized) is not known to be falsifiable [GW11] and it is hard to conceive [GGSW13] a reduction of \( iO \) security to complexity assumptions [GK16]. Since all of the security notions defined in this section are falsifiable, it is unsatisfactory to base them on \( iO \) from a theoretical point of view.

In contrast, obfuscation-minimum PKFE security is falsifiable and there are constructions [JLS21, JLS22] from well-studied complexity assumptions. The point of Lemma 1 is to base our constructions solely on one falsifiable assumption, or even complexity assumptions.

### 3 Ad Hoc Broadcast, Trace, and Revoke

This section concerns the definitions for ad hoc broadcast, trace, and revoke. After formally defining the syntax and correctness of AH-BTR, we present an intuitive definition of its security. While the security definition is comprehensive, it is not the easiest to work with, so we turn to define two simpler security notions, whose conjunction is equivalent to the comprehensive definition. The proof of their equivalence follows the definitions. Later in this paper, we will only work with the simpler notions.

**Definition 11 (AH-BTR).** An ad hoc broadcast, trace, and revoke (AH-BTR) scheme (with message space \( \{0,1\}^4 \) and public key length \( M_0(\lambda) \)) consists of 4 efficient algorithms:

- \( \text{Gen}(1^\lambda) \) outputs a pair \((\text{pk}, \text{sk})\) of public and secret keys with \( |\text{pk}| = M_0(\lambda) \).
- \( \text{Enc}(1^\lambda, \{\text{pk}_j\}_{j \in [N]}, \mu \in \{0,1\}^4) \) takes as input a list of public keys and a message. It outputs a ciphertext \( \text{ct} \).
- \( \text{Dec}(\{\text{pk}_j\}_{j \in [N]}, \text{ct}) \) is given random access to a list of public keys and a ciphertext, and takes as input the length of the list, an index, and a secret key. It outputs a message.
- \( \text{Trace}^D(1^\lambda, \{\text{pk}_j\}_{j \in [N]}, 1^{1/\epsilon'}) \) is given oracle access to a (stateless randomized) distinguisher \( D \) and takes as input a list of public keys and an error bound. It outputs an index \( i^* \in \{\bot\} \cup [N] \).

The scheme must be robustly correct, i.e., for all \( \lambda \in \mathbb{N}, N \in \mathbb{N}, i \in [N], \{\text{pk}_j\}_{j \in [N]} \setminus \{i\}\) such that \( |\text{pk}_j| = M_0(\lambda) \) for all \( j \in [N] \setminus \{i\} \), and \( \mu \in \{0,1\}^4 \),

\[
\Pr \left[ (\text{pk}_i, \text{sk}_i) \leftarrow \text{Gen}(1^\lambda), \text{ct} \leftarrow \text{Enc}(1^\lambda, \{\text{pk}_j\}_{j \in [N]}, \mu) : \text{Dec}(\{\text{pk}_j\}_{j \in [N]}, \text{ct}) \in [N], i, \text{sk}_i = \mu \right] = 1.
\]

**Definition 12** (traceability). An AH-BTR scheme (\( \text{Gen}, \text{Enc}, \text{Dec}, \text{Trace} \)) per Definition 11 is traceable if all efficient adversary wins \( \text{Exp}^\text{trace} \) only with negligible probability, where \( \text{Exp}^\text{trace}(1^\lambda) \) with adversary \( B \) proceeds as follows:

- **Setup.** Launch \( B(1^\lambda) \). Initialize the set \( S \) to \( \emptyset \) and let \( Q \leftarrow 0 \).

\[\text{\textsuperscript{10}}\text{These public keys could be out of the support of \text{Gen}, i.e., malformed.}\]
• **Query.** Repeat the following for arbitrarily many rounds determined by \( B \). In each round, \( B \) has two options:
  - \( B \) can request that a new user be initialized and obtain the newly generated public key. Upon this request, let \( Q \leftarrow Q + 1 \), run
    \[
    (pk_Q, sk_Q) \leftarrow \text{Gen}(1^\lambda),
    \]
    insert \( Q \) into \( S \), and send \( pk_Q \) to \( B \).
  - \( B \) can query for \( sk_t \) by submitting \( t \in [Q] \). Upon this query, remove \( t \) from \( S \) and send \( sk_t \) to \( B \).

• **Challenge.** \( B \) outputs a (probabilistic) circuit \( D \), a list \( \{pk_j^*\}_{j \in [N]} \) of public keys, and an error bound \( 1/\varepsilon^* \). Run
  \[
  i^* \leftarrow \text{Trace}^D(1^\lambda, \{pk_j^*\}_{j \in [N]}, 1^{1/\varepsilon^*}).
  \]
  Let
  - FalsePos be the event that \( i^* \in [N] \) and \( pk_{i^*}^* = pk_s \) for some \( s \in S \),
  - GoodDist the event that
    \[
    \Pr \left[ \begin{array}{c}
    \mu_0 \xleftarrow{} \{0, 1\}^\lambda, \\
    \mu_1 \xleftarrow{} \{0, 1\}^\lambda \\
    ct \xleftarrow{} \text{Enc}(1^\lambda, \{pk_j^*\}_{j \in [N]}, \mu_\beta)
    \end{array} : D(\mu_0, \mu_1, ct) = \beta \right] - \frac{1}{2} \geq \varepsilon^*,
    \]
  - and NotFound the event that \( i^* \notin [N] \) (i.e., \( i^* = \perp \)).

\( B \) wins if and only if \( \text{FalsePos} \lor (\text{GoodDist} \land \text{NotFound}) \).

AH-BTR as defined above is KEM, following [Zha20a]. Using hybrid encryption, such a scheme can be easily adapted for arbitrarily long messages with traceability under adversarially chosen messages. As noted in Remark 3 of [Zha20b], traceability implies KEM security (or IND-CPA when combined with hybrid encryption).

### 3.1 Simplified Security Notions

The traceability of AH-BTR guarantees that a traitor must be found (if the decoder is good enough) and innocent users must not be accused (whether or not the decoder is good enough). Decomposing the two requirements (plus some apparent weakening) makes each of them simpler (in particular, non-interactive). The first requirement is called **completeness**, and the second **soundness**.

**Definition 13** (completeness). An AH-BTR scheme \((\text{Gen}, \text{Enc}, \text{Dec}, \text{Trace})\) per Definition 11 is **complete** if all efficient adversary wins \( \text{Exp}_{\text{complete}} \) only with negligible probability, where \( \text{Exp}_{\text{complete}}(1^\lambda) \) with adversary \( C \) proceeds as follows:

• **Challenge.** Launch \( C(1^\lambda) \), which outputs a (probabilistic) circuit \( D \), a list \( \{pk_j^*\}_{j \in [N]} \) of public keys, and an error bound \( 1^{1/\varepsilon^*} \). Run
  \[
  i^* \leftarrow \text{Trace}^D(1^\lambda, \{pk_j^*\}_{j \in [N]}, 1^{1/\varepsilon^*}).
  \]
  Let
- GoodDist be the event that
  \[ \Pr \left[ \begin{array}{l}
  \mu_0 \leftarrow \{0, 1\}^\lambda, \\
  \beta \leftarrow \{0, 1\} \\
  \text{ct} \leftarrow \text{Enc}(1^\lambda, \{\beta_j\}_{j \in [N]}, \mu_\beta)
\end{array} \right] : D(\mu_0, \mu_1, \text{ct}) = \beta - \frac{1}{2} \geq \epsilon^*,
\]
  and NotFound the event that \( i^* \notin [N] \) (i.e., \( i^* = \perp \)).

\( C \) wins if and only if GoodDist \& NotFound.

**Definition 14** (soundness). An AH-BTR scheme \((\text{Gen}, \text{Enc}, \text{Dec}, \text{Trace})\) per Definition 11 is sound if all efficient adversary wins \(\text{Exp}_{\text{sound}}\) only with negligible probability, where \(\text{Exp}_{\text{sound}}(1^\lambda)\) with adversary \( C \) proceeds as follows:

- **Challenge.** Run \((pk, sk) \leftarrow \text{Gen}(1^\lambda)\), then run \( C(1^\lambda, pk)\), which outputs a (probabilistic) circuit \( D \), some \( N \in N \), a challenge index \( i^*_\perp \in [N] \), a list \( \{pk_j^*\}_{j \in [N] \setminus \{i^*_\perp\}} \) of public keys, and an error bound \( 1^{1/\epsilon^*} \). Let \( pk_{i^*_\perp}^* \leftarrow pk \) and run
  \[ i^* \leftarrow \text{Trace}^D(1^\lambda, \{pk_j^*\}_{j \in [N]}, 1^{1/\epsilon^*}) \]
  \( C \) wins if and only if \( i^* = i^*_\perp \) (the event FalsePos).

**Theorem 2** (\(*\)). An AH-BTR scheme is traceable if and only if it is both complete and sound.

**Proof** (Theorem 2). The reductionist proof of necessity is straight-forward — the query phase is unused by the reduction algorithm for completeness, and used only for creating the public key given to the adversary as input for soundness.

To show sufficiency, suppose the AH-BTR scheme \((\text{Gen}, \text{Enc}, \text{Dec}, \text{Trace})\) is both complete and sound and let \( B \) be an efficient adversary against its traceability. We consider two efficient adversaries. \( C_1 \) is against the completeness of the scheme. It works by internally simulating the traceability game for \( B \) and outputting whatever \( B \) outputs. Consider the coupling between \(\text{Exp}_{\text{complete}}\) for \( C_1 \) and the simulated \(\text{Exp}_{\text{trace}}\) for \( B \) inside, writing the events for adversary \( \lambda' \) in its security experiment with subscript \( \lambda' \),

\[ \text{GoodDist}_{C_1} \iff \text{GoodDist}_{B} \quad \text{and} \quad \text{NotFound}_{C_1} \iff \text{NotFound}_{B}. \]

Therefore,

\[ \Pr[\text{GoodDist}_{B} \& \text{NotFound}_{B}] = \Pr[\text{GoodDist}_{C_1} \& \text{NotFound}_{C_1}]. \]

\( C_2 \) is against the soundness of the scheme. Let \( B = \text{poly}(\lambda) > 1 \) be an upper bound of the running time of \( B \). The adversary \( C_2 \) does the following:

- \( C_2(pk) \) launches \( B \), initializes \( S \) to \( \emptyset \), lets \( Q \leftarrow 0 \), and samples and sets
  \[ s^* \leftarrow [B], \quad pk_{s^*} \leftarrow pk, \quad (pk_t, sk_t) \leftarrow \text{Gen}() \quad \text{for} \ t \in [B] \setminus \{s^*\}. \]

- \( C_2 \) answers queries from \( B \) and updates \( Q, S \) as stipulated by the query phase of the traceability experiment, except that it aborts if \( B \) queries for \( sk_{s^*} \).
• After the query phase, $B$ outputs $\mathcal{D}, \{pk_j\}_{j \in [N]}, 1^{1/\epsilon}$, and $C_2$ samples or sets

$$i^*_1 \left\{ \begin{array}{ll}
i^*_1 \leftarrow \{ i \in [N] : pk_i = pk \} \neq \emptyset; \\
\perp \quad \text{otherwise.} \end{array} \right.$$ 

It aborts if $i^*_1 = \perp$. Otherwise, $C_2$ outputs $\mathcal{D}, N, i^*_1, \{pk_j\}_{j \in [N] \setminus \{i^*_1\}}, 1^{1/\epsilon}$.

Consider the coupling between $\text{Exp}_{\text{sound}}$ for $C_2$ and the simulated $\text{Exp}_{\text{trace}}$ for $B$ inside. Routine calculation yields

$$\Pr[\text{FalsePos}_{C_2}] \geq \frac{1}{B^2} \Pr[\text{FalsePos}_{B}].$$

By the union bound,

$$\Pr[\text{FalsePos}_{B} \lor (\text{GoodDist}_{B} \land \text{NotFound}_{B})] \leq \Pr[\text{FalsePos}_{B}] + \Pr[\text{GoodDist}_{B} \land \text{NotFound}_{B}] \leq B^2 \Pr[\text{FalsePos}_{C_2}] + \Pr[\text{GoodDist}_{C_1} \land \text{NotFound}_{C_1}] = (\text{poly}(\lambda))^2 \text{negl}(\lambda) + \text{negl}(\lambda) = \text{negl}(\lambda). \quad \Box$$

## 4 Ad Hoc Private Linear Broadcast Encryption

Our construction of AH-BTR follows that of traitor tracing schemes in [BSW06]. We define ad hoc broadcast linear encryption (AH-PLBE) by adapting the notion of PLBE [BSW06] to the ad hoc setting.

**Definition 15** (AH-PLBE). An ad hoc private linear broadcast encryption (AH-PLBE) scheme (with message space $\{0,1\}^\lambda$ and public key length $M_0(\lambda)$) consists of 3 efficient algorithms:

- $\text{Gen}(1^\lambda)$ outputs a pair $(pk, sk)$ of public and secret keys with $|pk| = M_0(\lambda)$.
- $\text{Enc}(1^\lambda, \{pk_j\}_{j \in [N]}, i_{\perp} \in [0..N], \mu \in \{0,1\}^\lambda)$ takes as input a list of public keys, a cut-off index, and a message. It outputs a ciphertext $ct$.
- $\text{Dec}^{\{pk_j\}_{j \in [N]}, \text{ct}}(1^\lambda, N, i \in [N], sk_i)$ is given random access to a list of public keys and a ciphertext, and takes as input the length of the list, an index, and a secret key. It outputs a message.

The scheme must be robustly correct, i.e., for all $\lambda \in \mathbb{N}$, $N \in \mathbb{N}$, $i \in [N]$, $\{pk_j\}_{j \in [N] \setminus \{i\}}^{11}$ such that $|pk_i| = M_0(\lambda)$ for all $j \in [N] \setminus \{i\}$, and $\mu \in \{0,1\}^\lambda$, 

$$\Pr \left[ \begin{array}{l}
(pk_i, sk_i) \xleftarrow{\$} \text{Gen}(1^\lambda) \\
ct \xleftarrow{\$} \text{Enc}(1^\lambda, \{pk_j\}_{j \in [N]}, 0, \mu) \end{array} \right] \xrightarrow{i^*} \text{Dec}^{\{pk_j\}_{j \in [N]}, \text{ct}}(1^\lambda, N, i, sk_i) = \mu = 1.$$

$^{11}$These public keys could be out of the support of $\text{Gen}$, i.e., malformed.
Security. We define security notions of AH-PLBE analogously to those in [BSW06], except “mode indistinguishability” (Game 1 in [BSW06]), which is not needed here. The two security definitions have a one-to-one correspondence to the simplified security notions of AH-BTR in Section 3.1. Namely, message-hiding translates to completeness, and index-hiding translates to soundness.

Definition 16 (message-hiding). An AH-PLBE scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) per Definition 15 is message-hiding if \(\text{Exp}^0_{\text{MH}} \approx \text{Exp}^1_{\text{MH}}\), where \(\text{Exp}^b_{\text{MH}}(1^\lambda)\) with adversary \(\mathcal{A}\) proceeds as follows:

- **Challenge.** Launch \(\mathcal{A}(1^3)\) and receive from it a list \(\{pk_j^s\}_{j \in [N]}\) of public keys. Run
  \[
  \mu_0 \leftarrow \{0, 1\}^\lambda, \quad \mu_1 \leftarrow \{0, 1\}^\lambda, \quad ct \leftarrow \text{Enc}(1^\lambda, \{pk_j^s\}_{j \in [N]}, N, \mu_b),
  \]
  and send \((\mu_0, \mu_1, ct)\) to \(\mathcal{A}\).

- **Guess.** \(\mathcal{A}\) outputs a bit \(b'\), which is the output of the experiment.

Definition 17 (index-hiding). An AH-PLBE scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) per Definition 15 is index-hiding if \(\text{Exp}^0_{\text{IH}} \approx \text{Exp}^1_{\text{IH}}\), where \(\text{Exp}^b_{\text{IH}}(1^\lambda)\) with adversary \(\mathcal{A}\) proceeds as follows:

- **Challenge.** Run \((pk, sk) \leftarrow \text{Gen}(1^3)\), launch \(\mathcal{A}(1^3, pk)\), and receive from it some \(N \in \mathbb{N}\), a cut-off index \(i^*_\perp \in [N]\), and a list \(\{pk_j^s\}_{j \in [N]\setminus\{i^*_\perp\}}\) of public keys. Let \(pk_{i^*_\perp}^s \leftarrow pk\), run
  \[
  \mu \leftarrow \{0, 1\}^\lambda, \quad ct \leftarrow \text{Enc}(1^\lambda, \{pk_j^s\}_{j \in [N], i^*_\perp - 1 + b}, \mu),
  \]
  and send \((\mu, ct)\) to \(\mathcal{A}\).

- **Guess.** \(\mathcal{A}\) outputs a bit \(b'\), which is the output of the experiment.

4.1 Construction

Ingredients of Construction 1. Let

- GC = (GC.Garble, GC.Eval, GC.SimGarble) be a circuit garbling scheme such that GC.Garble uses \(\lambda\)-bit randomness,
- PPRF = (PPRF.Puncture, PPRF.Eval) a PPRF,
- PKE = (PKE.Gen, PKE.Enc, PKE.Dec) a PKE scheme such that PKE.Enc uses \(\lambda\)-bit randomness and whose public keys are (exactly) of polynomial length \(M_0\),
- LOT = (LOT.Gen, LOT.Hash, LOT.Send, LOT.Recv) a laconic OT scheme,
- Obf an obfuscator.

Construction 1 (AH-PLBE). Our AH-PLBE works as follows:

- Gen is the same as PKE.Gen.
\[ C_{\text{GC}}[N, hk, i, \mu, \mu', k_{\text{GC}}, k_{\text{PKE}}, \{k_{m_0}^{\text{LOT}}\}_{m_0 \in [M_0]}](i) \]

**Hardwired.**
- \( N \), number of users;
- \( hk \), laconic OT hash key;
- \( h_i \), laconic OT hash of \( D = \text{pk}_1 \parallel \cdots \parallel \text{pk}_N \);
- \( i \), cut-off index;
- \( \mu \), cut-off message;
- \( k_{\text{GC}} \), PPRF key for circuit garbling;
- \( k_{\text{PKE}} \), PPRF key for public-key encryption;
- \( k_{m_0}^{\text{LOT}} \), PPRF key for sending the \( m_0 \)th label using laconic OT.

**Input.**
- \( i \in [N] \), index of recipient.

**Output.**
Computed as follows.

\[
\begin{align*}
    r_i^{\text{GC}} &\leftarrow \text{PPRF.Eval}(k_{\text{GC}}, i) \\
    r_i^{\text{PKE}} &\leftarrow \text{PPRF.Eval}(k_{\text{PKE}}, i) \\
    r_{i,m_0}^{\text{LOT}} &\leftarrow \text{PPRF.Eval}(k_{m_0}^{\text{LOT}}, i) \quad \text{for } m_0 \in [M_0] \\
    (\widehat{C}_{\text{ct}, i}, \{L_{i,m_0,b}\}_{m_0\in[M_0], b\in\{0,1\}}) &\leftarrow \begin{cases} 
        \text{GC.Garble}(\widehat{C}_{\text{ct}}, (\mu, r_i^{\text{PKE}}); r_i^{\text{GC}}), & \text{if } i \leq i_\perp; \\
        \text{GC.Garble}(\widehat{C}_{\text{ct}}, (\mu', r_i^{\text{PKE}}); r_i^{\text{GC}}), & \text{if } i > i_\perp;
    \end{cases} \\
    \text{LOT.ct}_{i,m_0} &\leftarrow \text{LOT.Send}(hk, h_i, (i-1)M_0 + m_0, \\
    &\quad L_{i,m_0,0}, L_{i,m_0,1}; r_{i,m_0}^{\text{LOT}}) \quad \text{for } m_0 \in [M_0] \\
    \text{output} &\leftarrow (\widehat{C}_{\text{ct}, i}, \{\text{LOT.ct}_{i,m_0}\}_{m_0\in[M_0]})
\end{align*}
\]

**Hardwired.**
- \( \mu' \), message or cut-off message;
- \( r_i^{\text{PKE}} \), public-key encryption randomness.

**Input.**
- \( \text{pk}_i \), public key of recipient.

**Output.**
- \( \text{PKE.ct}_i \leftarrow \text{PKE.Enc}(\text{pk}_i, \mu'; r_i^{\text{PKE}}) \).

**Figure 1.** The circuits \( C_{\text{GC}} \) and \( C_{\text{ct}} \) in Construction 1.
\textbullet \text{Enc} (\{p_{j}\}_{j \in [N]}, i, \mu, \mu) \text{ first checks whether } \lvert p_{j} \rvert = M_{0} \text{ for all } j \in [N]. \text{ If not, it outputs } ct = \bot \text{ and terminates. Otherwise, the algorithm hashes down the public keys by running}

\begin{align*}
M & \leftarrow NM_{0}, \\
D & \leftarrow \text{pk}_{1} \cdots \text{pk}_{N}, \\
hk & \leftarrow \text{LOT.Gen}(M), \\
(h, \tilde{D}) & \leftarrow \text{LOT.Hash}(hk, D).
\end{align*}

It samples the cut-off message \( \mu_{\bot} \leftarrow \{0, 1\}^{\lambda} \) and PPRF keys

\begin{align*}
k_{\text{GC}} & \leftarrow \{0, 1\}^{\lambda}, \\
k_{\text{PKE}} & \leftarrow \{0, 1\}^{\lambda}, \\
k_{\text{LOT}} & \leftarrow \{0, 1\}^{\lambda} \text{ for } m_{0} \in [M_{0}],
\end{align*}

and obfuscates \( C_{\text{GC}} \) (Figure 1) by running

\( \tilde{C}_{\text{GC}} \leftarrow \text{Obf}(C_{\text{GC}}[N, hk, h, i, \mu, \mu, k_{\text{GC}}, k_{\text{PKE}}, \{k_{\text{LOT}}\}_{m_{0} \in [M_{0}]}]) \).

The algorithm outputs \( ct = (hk, \tilde{C}_{\text{GC}}) \) as the ciphertext.

\textbullet \text{Dec}(\text{pk}_{i})_{i \in [N], ct} \text{ first parses } ct = (hk, \tilde{C}_{\text{GC}}) \text{ and recomputes}

\begin{align*}
M & \leftarrow NM_{0}, \\
D & \leftarrow \text{pk}_{1} \cdots \text{pk}_{N}, \\
(h, \tilde{D}) & \leftarrow \text{LOT.Hash}(hk, D).
\end{align*}

The algorithm next runs the obfuscated circuit,

\( (\tilde{C}_{ct,i}, \{\text{LOT.ct}_{i,m_{0}}\}_{m_{0} \in [M_{0}]}) \leftarrow \tilde{C}_{\text{GC}}(i), \)

to obtain the garbled \( C_{ct} \) (Figure 1) for the decryptor and the laconic OT ciphertexts sending its labels. It then receives the labels,

\( L_{i,m_{0},pk_{i}[m_{0}] \leftarrow \text{LOT.Recv}(hk, h, (i-1)M_{0} + m_{0}, \text{LOT.ct}_{i,m_{0}}) \text{ for } m_{0} \in [M_{0}], \)

and evaluates the garbled circuit,

\( \text{PKE.ct}_{i} \leftarrow \text{GC.Eval}(\tilde{C}_{ct,i}, \text{pk}_{i}, \{L_{i,m_{0},pk_{i}[m_{0}]_{m_{0} \in [M_{0}]}}\}, \)

to obtain the PKE ciphertext under the decryptor’s public key. Lastly, the algorithm runs and outputs (as the decrypted message)

\( \mu \leftarrow \text{PKE.Dec}(sk_{i}, \text{PKE.ct}_{i}). \)

**Robustness Correctness.** This can be verified by inspection.

**Efficiency.** By the efficiency of laconic OT, LOT.Gen takes time \( \text{poly}(\lambda, \log N) \), LOT.Hash takes time \( O(N) \text{ poly}(\lambda, \log N) \), and \( \lvert hk \rvert, \lvert h \rvert = \text{poly}(\lambda, \log N) \). As we shall see later, it suffices to pad \( C_{\text{GC}} \) to size \( \text{poly}(\lambda, \log N) \) for the security proofs to go through. Putting these together,

\( T_{\text{Enc}} = O(N) \text{ poly}(\lambda, \log N), \quad \lvert ct \rvert = \text{poly}(\lambda, \log N), \quad T_{\text{Dec}} = O(N) \text{ poly}(\lambda, \log N). \)

In practice and for security reasons, we always assume \( N \leq 2^{\lambda} \) and \( \log N \) is absorbed by \( \lambda \). Therefore, with \( \text{poly}(\lambda) \) factors ignored, both encryption and decryption take linear time, and the ciphertext is constant-size.
Compatibility. Since the key generation algorithm of Construction 1 is just the key generation algorithm of the underlying PKE scheme (which only has to be semantically secure for random messages), it is compatible with the existing public-key encryption schemes, i.e., existing users possessing PKE key pairs can utilize our AH-PLBE without regenerating their keys.

4.2 Message-Hiding Property

Theorem 3 (∗). Suppose in Construction 1, the obfuscator Obf is an iO for poly(λ)-sized domain, then the resultant AH-PLBE is message-hiding.

Proof (Theorem 3). For Construction 1, the only difference between Exp^0_{MH} and Exp^1_{MH} is whether C_{GC} used to create ct = (hk, C_{GC}) has \mu_0 or \mu_1 hardwired as \mu. In C_{GC} (Figure 1), \mu is used only in the branch i > i_{\perp}, which is never taken in Exp^0_{MH} or Exp^1_{MH} because i_{\perp} is hardwired to be N and the domain of i is [N]. Therefore, the two C_{GC}'s in Exp^0_{MH} and Exp^1_{MH} being obfuscated are functionally equivalent and have the same size. Moreover, their domain size is N (polynomially large). Therefore, Exp^0_{MH} \approx Exp^1_{MH} reduces to the iO security for poly(λ)-sized domain of Obf.

4.3 Index-Hiding Property

Theorem 4 (∗). Suppose in Construction 1, all of the ingredients are secure, then the resultant AH-PLBE is index-hiding.

Proof (Theorem 4). The only difference between Exp^0_{IH} and Exp^1_{IH} is whether the C_{GC} being obfuscated hardwires \mu (in Exp^0_{IH}) or \mu_{\perp} (in Exp^1_{IH}) into C_{ct;i_{\perp}} which only affects the output of C_{GC} at i = i_{\perp}. We consider the following hybrids, each (except the first) described by the changes from the previous one:

- H^b_0 (for b ∈ \{0, 1\}) is Exp^b_{IH}, where
  \begin{align*}
  &hk \leftarrow \text{LOT.Gen}(NM_0), \quad (h, \tilde{D}) \leftarrow \text{LOT.Hash}(hk, pk_1^* || \cdots || pk_N^*), \\
  &k_{\text{GC}}^0 \leftarrow \{0, 1\}^\lambda, \quad k_{\text{PKE}}^0 \leftarrow \{0, 1\}^\lambda, \quad k_{\text{LOT}}^0 \leftarrow \{0, 1\}^\lambda \quad \text{for } m_0 \in [M_0], \\
  &C_{\text{GC}}^0 \leftarrow \text{Obf}(C_{\text{GC}}[N,hk,h,i_{\perp}^* - 1 + b,\mu_{\perp},\mu,k_{\text{GC}}^0,k_{\text{PKE}}^0,k_{\text{LOT}}^0,m_0\in[M_0]]), \\
  &ct = (hk, C_{\text{GC}}^0).
  \end{align*}

- H^b_1 alters the obfuscation into
  \begin{align*}
  &C_{\text{GC}}' \leftarrow \text{Obf}(C_{\text{GC}}[N,hk,h,\mu_{\perp},\mu, \\
  &i_{\perp}^*,k_{i_{\perp}}^0,k_{i_{\perp}}^\text{PKE},k_{i_{\perp}}^\text{LOT},m_0\in[M_0],C_{\text{ct};i_{\perp}^*},\{\text{LOT}\cdot\text{ct};i_{\perp}^*,m_0\in[M_0]\}]),
  \end{align*}
  where
  - C_{\text{GC}}' is defined in Figure 2,
  - the PPRF keys are punctured at i_{\perp}^* by running
    \begin{align*}
    &k_{i_{\perp}}^\text{GC} \leftarrow \text{PPRF.Puncture}(k_{i_{\perp}}^\text{GC},i_{\perp}^*), \\
    &k_{i_{\perp}}^\text{PKE} \leftarrow \text{PPRF.Puncture}(k_{i_{\perp}}^\text{PKE},i_{\perp}^*), \\
    &k_{i_{\perp}}^\text{LOT} \leftarrow \text{PPRF.Puncture}(k_{i_{\perp}}^\text{LOT},i_{\perp}^*),
    \end{align*}
    for m_0 \in [M_0].
and the output $(\widetilde{C}_{ct,i*}, \{\text{LOT.}ct_{i*,m_0}\}_{m_0 \in [M_0]})$ of $C'_{GC}$ at $i = i^*_1$ is computed as

\[
\begin{align*}
    r^G_{GC} &\leftarrow \text{PPRF.Eval}(k^G_{GC}, i^*_1), \\
    r^P_{PKE} &\leftarrow \text{PPRF.Eval}(k^P_{PKE}, i^*_1), \\
    r^L_{i^*_1, m_0} &\leftarrow \text{PPRF.Eval}(k^L_{m_0}, i^*_1) \\
    (\widetilde{C}_{ct,i*}, \{L_{i*,m_0,b}\}_{m_0 \in [M_0], b \in \{0, 1\}}) &\leftarrow \begin{cases} \\
    \text{GC.Garble}(C_{ct}, (\mu, r^G_{i^*_1}); r^G_{i^*_1}), & \text{if } b = 0; \\
    \text{GC.Garble}(C_{ct}, (\mu, r^P_{i^*_1}); r^G_{i^*_1}), & \text{if } b = 1; \\
    \end{cases}
\end{align*}
\]

\[
\text{LOT.ct}_{i^*_1, m_0} \leftarrow \text{LOT.Send}(hk, h, (i^*_1 - 1)M_0 + m_0, \\
L_{i^*_1, m_0,0}, L_{i^*_1, m_0,1}; r^L_{i^*_1, m_0}) \\
\text{for } m_0 \in [M_0].
\]

\[
\begin{itemize}
    \item $H^b$ changes $r^G_{i^*_1}, r^P_{i^*_1}$, and $r^L_{i^*_1, m_0}$'s into true randomness, i.e.,
    \[
    r^G_{i^*_1} \leftarrow \{0, 1\}^\lambda, \quad r^P_{i^*_1} \leftarrow \{0, 1\}^\lambda, \quad r^L_{i^*_1, m_0} \leftarrow \{0, 1\}^\lambda \quad \text{for } m_0 \in [M_0].
    \]
\end{itemize}

\[
\begin{align*}
    C'_{GC} &\leftarrow [N, hk, h, \mu, \mu, i^*_1, k^G_{GC}, k^P_{PKE}, k^L_{m_0, i^*_1}, \{\text{LOT.ct}_{i^*_1, m_0}\}_{m_0 \in [M_0]}, (\widetilde{C}_{ct,i*}, \{\text{LOT.}ct_{i*,m_0}\}_{m_0 \in [M_0]})(i) \\
\text{Hardwired.} &\quad N, hk, h, \mu, \mu, \mu, \quad \text{see Figure 1;} \\
&\quad i^*_1, \quad \text{challenge cut-off index;}
&\quad k^G_{GC}, k^P_{PKE}, \quad \text{PPRF keys punctured at } i^*_1; \\
&\quad (\widetilde{C}_{ct,i*}, \text{LOT.ct}_{i*,\ldots}), \quad \text{hardwired output of } C'_{GC} \text{ at } i = i^*_1. \\
\text{Input.} &\quad i \in [N], \quad \text{index of recipient.}
\end{align*}
\]

\textbf{Output.} Computed as follows.

\begin{itemize}
    \item \textbf{if } $[i = i^*_1]$:
    \begin{itemize}
        \item \textbf{output} $(\widetilde{C}_{ct,i*}, \{\text{LOT.}ct_{i*,m_0}\}_{m_0 \in [M_0]})$ as hardwired
    \end{itemize}
    \item \textbf{else}:
    \begin{itemize}
        \item $r^G_{i^*_1} \leftarrow \text{PPRF.Eval}(k^G_{i^*_1}, i)$
        \item $r^P_{i^*_1} \leftarrow \text{PPRF.Eval}(k^P_{i^*_1}, i)$
        \item $r^L_{i^*_1, m_0} \leftarrow \text{PPRF.Eval}(k^L_{m_0, i^*_1}, i) \quad \text{for } m_0 \in [M_0]$
        \item $(\widetilde{C}_{ct,i}, \{L_{i,m_0,b}\}_{m_0 \in [M_0], b \in \{0, 1\}}) \leftarrow \begin{cases} \\
            \text{GC.Garble}(\widetilde{C}_{ct}, (\mu, r^G_{i^*_1}); r^G_{i^*_1}), & \text{if } i < i^*_1; \\
            \text{GC.Garble}(\widetilde{C}_{ct}, (\mu, r^P_{i^*_1}); r^G_{i^*_1}), & \text{if } i > i^*_1; \\
        \end{cases}
        \end{cases}
        \end{itemize}
    \end{itemize}

\text{LOT.ct}_{i^*_1, m_0} \leftarrow \text{LOT.Send}(hk, h, (i - 1)M_0 + m_0, \\
L_{i^*_1, m_0,0}, L_{i^*_1, m_0,1}; r^L_{i^*_1, m_0}) \quad \text{for } m_0 \in [M_0]
\]

\textbf{output} $(\widetilde{C}_{ct,i}, \{\text{LOT.}ct_{i,m_0}\}_{m_0 \in [M_0]})$

\begin{figure}
\caption{The circuit $C'_{GC}$ in the proof of Theorem 4.}
\end{figure}
• $H^b_3$ removes the unused labels from $\text{LOT}.ct_{i^*_1,m_0}$'s by setting
  \[ \text{LOT}.ct_{i^*_1,m_0} \leftarrow \text{LOT}.\text{Send}(hk, h, (i^*_1 - 1)M_0 + m_0, \]
  \[ L_{i^*_1,m_0, pk_{i^*_1}^* [m_0]}, L_{i^*_1,m_0, pk_{i^*_1}^* [m_0]} ; \gamma_{i^*_1,m_0}^{\text{LOT}} \]
  \text{for } m_0 \in [M_0]. \]

• $H^b_4$ changes $\widehat{C}_{ct,i^*_1}$ into simulation, i.e.,
  \[ \text{PKE}.ct_{i^*_1} \leftarrow \begin{cases} \text{PKE}.\text{Enc}(pk_{i^*_1}^*, \mu ; r_{\text{PKE}}), & \text{if } b = 0; \\ \text{PKE}.\text{Enc}(pk_{i^*_1}^*, \mu_{\perp} ; r_{\text{PKE}}), & \text{if } b = 1; \end{cases} \]
  \[ (\widehat{C}_{ct,i^*_1}, \{L_{i^*_1,m_0, pk_{i^*_1}^* [m_0]}\}_{m_0 \in [M_0]} \) \leftarrow \text{GC}.\text{SimGarble}(C_{ct}, pk_{i^*_1}^*, \text{PKE}.ct_{i^*_1}), \]
  where $pk_{i^*_1}^* = pk$ is sampled by the experiment (not adversarially controlled).

The following claims hold, all of which are immediate by inspection:

Claim 5. $H^b_0 = H^b_1$ for $b \in \{0, 1\}$ if $\text{Obf}$ is an $iO$ for poly($\lambda$)-sized domain.

Claim 6. $H^b_0 = H^b_2$ for $b \in \{0, 1\}$ if $\text{PPRF}$ is pseudorandom at the punctured point.

Claim 7. $H^b_0 \approx H^b_3$ for $b \in \{0, 1\}$ if $\text{LOT}$ is database-selectively sender-private.

Claim 8. $H^b_0 = H^b_4$ for $b \in \{0, 1\}$ if $\text{GC}$ is $w$-hiding.

Claim 9. $H^b_0 = H^1_1$ if $\text{PKE}$ is semantically secure for random messages.

$\text{Exp}^b_{IH} = \text{Exp}^1_{IH}$ follows from a hybrid argument. \hfill \square

5 \ AH-BTR from AH-PLBE

**Ingredient of Construction 2.** Let $\text{ahPLBE} = (\text{ahPLBE}.\text{Gen}, \text{ahPLBE}.\text{Enc}, \text{ahPLBE}.\text{Dec})$ be an AH-PLBE scheme.

**Construction 2** (adapted from Section 2.2 in [BSW06]). Our AH-BTR works as follows:

- Gen is the same as $\text{ahPLBE}.\text{Gen}$.
- $\text{Enc}(\{pk_j\}_{j \in [N]}, \mu)$ runs and outputs $ct \leftarrow \text{ahPLBE}.\text{Enc}(\{pk_j\}_{j \in [N]}, 0, \mu)$.
- Dec is the same as $\text{ahPLBE}.\text{Dec}$.
- $\text{Trace}^D(\{pk_j\}_{j \in [N]}, 1^{1/\epsilon^*})$ defines for $i \in [0..N],
  \epsilon_i = \text{Pr}[\begin{array}{c} \mu_0 \leftarrow \{0, 1\}^\lambda, \mu_1 \leftarrow \{0, 1\}^\lambda, \beta \leftarrow \{0, 1\} \\ ct \leftarrow \text{ahPLBE}.\text{Enc}(1^{\lambda}, \{pk_j\}_{j \in [N]}, i, \mu_\beta) \end{array} : \text{D}(\mu_0, \mu_1, ct) = \beta] - \frac{1}{2}$.

Experiment $\mathcal{E}_i$ (sampling and testing) and event $E_i$ (correct guessing)

Setting $\beta \leftarrow \frac{\epsilon^*}{10N}$ and $\eta \leftarrow \left[\frac{10 \log(2M + 2)}{2m^2}\right]$, for each $i \in [0..N]$, the algorithm runs $\mathcal{E}_i$ for $\eta$ times independently, counts the absolute frequency $\xi_i \in [0..\eta]$ of $E_i$, and computes $\widehat{\xi}_i = \frac{\xi_i}{\eta} - \frac{1}{2}$. It outputs

$$i^* = \begin{cases} \min T, & \text{if } T \leftarrow \{i \in [N] : |\widehat{\xi}_i - \widehat{\xi}_{i-1}| \geq 3\delta \} \neq \emptyset; \\ \bot, & \text{if } T = \emptyset. \end{cases}$$
Robustness, Correctness, Efficiency, Compatibility. These are inherited from the underlying AH-PLBE. When based on Construction 1, the resultant AH-BTR has

\[ T_{\text{Enc}} = O(N) \text{ poly}(\lambda), \quad |\text{ct}| = \text{poly}(\lambda), \quad T_{\text{Dec}} = O(N) \text{ poly}(\lambda), \]

and is compatible with the existing public-key encryption schemes.

**Theorem 10 (¶).** Suppose in Construction 2, the AH-PLBE scheme \( \text{ahPLBE} \) is message-hiding, then the resultant AH-BTR is complete.

**Theorem 11 (¶).** Suppose in Construction 2, the AH-PLBE scheme \( \text{ahPLBE} \) is index-hiding, then the resultant AH-BTR is sound.

**Proof (Theorem 10).** Consider any efficient adversary \( C \) against the completeness of Construction 2. Let \( \text{GoodEst} \) be the event that \( |\hat{e}_i - e_i| \leq \delta \) for all \( i \in [0..N] \). By the Chernoff bound, the union bound, and the law of total probability,

\[
\text{Pr}[\neg \text{GoodEst}] = \mathbb{E}[\text{Pr}[\neg \text{GoodEst} \mid e^*, N]] \leq \mathbb{E}[2(N + 1) \exp(-2\delta^2 \eta)] \leq 2^{-\lambda}.
\]

Let \( \text{BadEnd} \) be the event that \( |e_N| > \frac{e^*}{2} \), then \( \text{GoodDist} \land \neg \text{BadEnd} \) implies

\[
\max_{i \in [N]} |\hat{e}_{i-1} - \hat{e}_i| \geq \frac{1}{N} \sum_{i=1}^{N} |\hat{e}_{i-1} - \hat{e}_i| \geq \frac{1}{N} \left| \sum_{i=1}^{N} (\hat{e}_{i-1} - \hat{e}_i) \right| = \frac{1}{N} |e_0 - e_N| \\
\geq \frac{1}{N} (|e_0| - |e_N|) \geq \frac{1}{N} \left( e^* - \frac{e^*}{2} \right) = \frac{e^*}{2N} = 5\delta.
\]

Therefore, \( \text{GoodDist} \land \neg \text{BadEnd} \land \text{GoodEst} \) implies

\[
\max_{i \in [N]} |\hat{e}_{i-1} - \hat{e}_i| \geq \max_{i \in [N]} (|\hat{e}_{i-1} - \hat{e}_i| - 2\delta) \geq 5\delta - 2\delta = 3\delta,
\]

which in turn implies \( T \neq \emptyset \) hence \( i^* \in [N] \), i.e., \( \neg \text{NotFound} \). By contraposition,

\[
\text{GoodDist} \land \text{NotFound} \land \text{GoodEst} \implies \text{BadEnd}.
\]

By the union bound,

\[
\text{Pr}[C \text{ wins}] \leq \text{Pr}[\neg \text{GoodEst}] + \text{Pr}[(C \text{ wins}) \land \text{GoodEst}]
\]

\[
= \text{Pr}[\neg \text{GoodEst}] + \text{Pr}[\text{GoodDist} \land \text{NotFound} \land \text{GoodEst}]
\]

\[
\leq 2^{-\lambda} + \text{Pr}[\text{BadEnd}],
\]

so it remains to show \( \text{Pr}[\text{BadEnd}] = \text{negl}(\lambda) \).

Consider the following efficient adversary \( A \) against the message-hiding property of \( \text{ahPLBE} \):

- \( A \) runs \( C \) to obtain

\[ \mathcal{D}, \ \{pk^*_j\}_{j \in [N]}, \ 1^{1/e^*}. \]

- \( A \) runs \( E_N \) once and notes down \( \alpha \in \{0, 1\} \) indicating whether \( E_N \) happened, i.e., \( \alpha = 1 \) if and only if \( \mathcal{D} \) guessed correctly in the trial.
• \( A \) submits \( \{ \text{pk}_j \}_{j \in [N]} \) to the message-hiding experiment, receives \((\mu_0, \mu_1, \text{ct})\) back, and runs and outputs \( b' \leftarrow \mathcal{D}(\mu_0, \mu_1, \text{ct}) \oplus a \).

Routine calculation shows that the advantage of \( A \) is \( \mathbb{E}[4\varepsilon_N^2] \), which must be negligible by the message-hiding property of ahPLBE. Let \( B = \text{poly}(\lambda) \) be an upper bound of \( 1/\varepsilon^* \) (\( B \) exists since \( C \) outputs \( 1/\varepsilon^* \) in polynomial time). By Markov's inequality,

\[
\Pr[\text{BadEnd}] = \Pr[4\varepsilon_N^2 > (\varepsilon^*)^2] \leq \Pr[4\varepsilon_N^2 > B^2] \\
\leq B^2 \mathbb{E}[4\varepsilon_N^2] = (\text{poly}(\lambda))^2 \text{negl}(\lambda) = \text{negl}(\lambda).
\]

**Proof (Theorem 11).** Consider any efficient adversary \( C \) against the soundness of Construction 2. Similarly to the proof of Theorem 10, define \( \text{GoodEst} \) and recall that \( \Pr[\neg \text{GoodEst}] \leq 2^{-\lambda} \). We have

\[
\Pr[C \text{ wins}] \leq \Pr[\neg \text{GoodEst}] + \Pr[(C \text{ wins}) \land \text{GoodEst}] \\
= \Pr[\neg \text{GoodEst}] + \Pr[\text{FalsePos} \land \text{GoodEst}] \\
\leq 2^{-\lambda} + \Pr[\text{FalsePos} \land \text{GoodEst}],
\]

and it suffices to prove \( \Pr[\text{FalsePos} \land \text{GoodEst}] = \text{negl}(\lambda) \).

Let \( \alpha \) be a random element in an execution of Trace with

\[
\alpha = \begin{cases} 0, & \text{if } i^* \in [N] \text{ and } \tilde{e}_{i^* - 1} - \tilde{e}_{i^*} \geq 3\delta; \\ 1, & \text{if } i^* \in [N] \text{ and } \tilde{e}_{i^* - 1} - \tilde{e}_{i^*} \leq -3\delta; \\ \bot, & \text{if } i^* = \bot. \end{cases}
\]

Consider the following efficient adversary \( A \) against the index-hiding property of ahPLBE:

• \( A \) runs \( C(\text{pk}) \) to obtain

\[
\mathcal{D}, N, i^*_\bot, \{ \text{pk}_j \}_{j \in [N] \setminus \{i^*_\bot\}}, 1^{1/\varepsilon^*},
\]

and sets \( \text{pk}^*_{i^*_\bot} \leftarrow \text{pk} \).

• \( A \) runs

\[
i^* \leftarrow \text{Trace}^\mathcal{D}(\{ \text{pk}_j \}_{j \in [N]}, 1^{1/\varepsilon^*}),
\]

and aborts if \( i^* \neq i^*_\bot \).

• \( A \) notes down \( \alpha \in \{0, 1\} \) from the above execution of Trace, submits

\[
N, i^*_\bot, \{ \text{pk}_j \}_{j \in [N] \setminus \{i^*_\bot\}}
\]

to the index-hiding experiment, gets \((\mu, \text{ct})\) back, samples and sets

\[
\beta \leftarrow \{0, 1\}, \quad \mu_\beta \leftarrow \mu, \quad \mu_{\neg \beta} \leftarrow \{0, 1\}^4,
\]

and runs and outputs \( b' \leftarrow \mathcal{D}(\mu_0, \mu_1, \text{ct}) \oplus \neg \beta \oplus \alpha \).
Routine calculation shows that the advantage of $A$ is
\[
\mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot (-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}})],
\]
which must be negligible by the index-hiding property of ahPLBE.

Let $B = \text{poly}(\lambda)$ be an upper bound of $10N/\varepsilon^*$ ($B$ exists since $C$ outputs $1^N$ and $1^{1/\varepsilon^*}$ in polynomial time). The event $\text{FalsePos} \land \text{GoodEst}$ implies
\[
| (\epsilon_{i^{*}-1} - \epsilon_{i^{*}}) - (\hat{\epsilon}_{i^{*}-1} - \hat{\epsilon}_{i^{*}}) | \leq 2\delta < 3\delta \leq |\hat{\epsilon}_{i^{*}-1} - \hat{\epsilon}_{i^{*}} |
\]
\[
\implies (-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}}) = |\epsilon_{i^{*}-1} - \epsilon_{i^{*}}| \geq 3\delta - 2\delta = \frac{\varepsilon^*}{10N} \geq B^{-1}.
\]

Moreover, $(-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}}) \geq -1$ always holds. These together show that
\[
\Pr[\text{FalsePos} \land \text{GoodEst}]
\]
\[
= B \mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot \mathbb{I}_{\text{GoodEst}} \cdot B^{-1}]
\]
\[
\leq B \mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot \mathbb{I}_{\text{GoodEst}} \cdot (-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}})]
\]
\[
\leq B \left( \mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot \mathbb{I}_{\text{GoodEst}} \cdot (-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}})] + \mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot \mathbb{I}_{\neg \text{GoodEst}}] \right)
\]
\[
= B \left( \mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot (-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}})] + \Pr[\text{FalsePos} \land \neg \text{GoodEst}] \right)
\]
\[
\leq B \left( \mathbb{E}[\mathbb{I}_{\text{FalsePos}} \cdot (-1)^a (\epsilon_{i^{*}-1} - \epsilon_{i^{*}})] + 2^{-\lambda} \right)
\]
\[
= \text{poly}(\lambda)(\text{negl}(\lambda) + 2^{-\lambda}) = \text{negl}(\lambda). \quad \square
\]

6 Trading Ciphertext Size for Decryption Time in AH-BTR

While Construction 2 achieves constant ciphertext size, it takes time $\Omega(N)$ to decrypt. In contrast, the naïve scheme that encrypts to each user separately has $\Omega(N)$-size ciphertext, yet decryption only takes constant time. By grouping the recipients and encrypting to each group separately, we can trade ciphertext size for decryption time.\(^\text{12}\)

Previous work [Zha20a] already systemizes the idea of grouping in the context of traditional traitor tracing.

**Ingredients of Construction 3.** Let $\text{old} = (\text{old.Gen}, \text{old.Enc}, \text{old.Dec}, \text{old.Trace})$ be an AH-BTR scheme and $\gamma$ some\(^\text{13}\) constant ($0 < \gamma < 1$).

**Construction 3** (adapted from Theorem 1 in [Zha20a]). Our new AH-BTR works as follows:

- $\text{Gen}$ is the same as $\text{old.Gen}$.

\(^{12}\)Alternatively, one can reformulate Construction 2 as a compiler that trades decryption time for ciphertext size, by grouping the recipients and compressing the groups. We refrained from such a formulation because the “transformation” uses a quite strong additional assumption, namely functional encryption for general circuits.

\(^{13}\)We require that $N \mapsto \lceil N^\gamma \rceil$ can be computed in (deterministic) time $\text{poly}(\log N)$.
• \(\text{Enc}(\{pk_j\}_{j \in [N]}, \mu)\) sets \(N_1 = [N^\gamma]\) and \(N_2 = [N/N_1]\). It runs
  \[
  \text{old.ct}_{j_1} \overset{\$}{\leftarrow} \text{old.Enc}(\{pk_j\}_{(j_1-1)N_2 < j \leq j_1N_2}, \mu) \quad \text{for} \ j_1 \in [N_1].
  \]
  The algorithm outputs \(ct = \{\text{old.ct}_{j_1}\}_{j_1 \in [N_1]}\).

• \(\text{Dec}^{pk}(\{pk_j\}_{j \in [N]}, ct(N, i, sk_i))\) sets \(N_1 = [N^\gamma]\), \(N_2 = [N/N_1]\). It parses \(ct\) as \(\{\text{old.ct}_{j_1}\}_{j_1 \in [N_1]}\), finds \(i_1 \in [N_1]\) such that \((i_1 - 1)N_2 < i \leq i_1N_2\), and sets \(N'_2 = \min\{N_2, N - (i_1 - 1)N_2\}\). The algorithm runs and outputs
  \[
  \text{old.Dec}^{pk}(pk_{i_1-1}N_2 < i \leq i_1N_2, \text{old.ct}_{i_1}(N'_2, i - (i_1 - 1)N_2, sk_i)).
  \]

• \(\text{Trace}^D(\{pk_j^*\}_{j \in [N]}, 1^{1/\epsilon'})\) sets \(N_1 = [N^\gamma]\) and \(N_2 = [N/N_1]\). It runs
  \[
  i^*_{j_1} \overset{\$}{\leftarrow} \text{old.Trace}^D_i(\{pk_j^*\}_{(j_1-1)N_2 < j \leq j_1N_2}, 1^{N_1/N}, 1^{N_i/\epsilon'}), \quad \text{for} \ j_1 \in [N_1],
  \]
  where \(D_i(\mu_0, \mu_1, \text{old.ct}^*)\) runs and outputs \(D(\mu_0, \mu_1, \{\text{old.ct}_{j_1}^*\}_{j_1 \in [N_1]})\) with
  \[
  \text{old.ct}_{j_1}^* \leftarrow \text{old.ct}^*,
  \]
  \[
  \left\{
  \begin{aligned}
  &\text{old.Enc}(\{pk_j^*\}_{(j_1-1)N_2 < j \leq j_1N_2}, \mu_0), & &\text{if} \ j'_1 < j_1; \\
  &\text{old.Enc}(\{pk_j^*\}_{(j_1-1)N_2 < j \leq j_1N_2}, \mu_1), & &\text{if} \ j'_1 > j_1.
  \end{aligned}
  \right.
  \]
  The algorithm outputs
  \[
  (j_1 - 1)N_2 + i^*_{j_1}, \quad \text{if} \ i^*_{j_1} = \bot \text{ for all } j'_1 < j_1 \text{ and } i^*_{j_1} \neq \bot; \]
  \[
  \bot, \quad \text{if} \ i^*_{j_1} = \bot \text{ for all } j'_1 \in [N_1].
  \]

**Robustness Correctness and Compatibility.** These are inherited from the underlying AH-BTR. When based on Construction 2, the resultant AH-BTR is compatible with the existing public-key encryption schemes.

**Efficiency.** Let \(\gamma_1, \gamma_2, \gamma_3\) be constants such that the AH-BTR efficiency is

\[
T_{\text{Enc}} = O(N^{\gamma_1}) \text{ poly}(\lambda), \quad |ct| = O(N^{\gamma_2}) \text{ poly}(\lambda), \quad T_{\text{Dec}} = O(N^{\gamma_3}) \text{ poly}(\lambda),
\]

then the underlying efficiency is mapped to the resultant efficiency\(^{14}\) by

\[
(\gamma_1, \gamma_2, \gamma_3) \mapsto (1 - \gamma + \gamma \gamma_1, 1 - \gamma + \gamma \gamma_2, \gamma \gamma_3).
\]

When based on Construction 2, the resultant AH-BTR enjoys

\[
T_{\text{Enc}} = O(N) \text{ poly}(\lambda), \quad |ct| = O(N^{1-\gamma}) \text{ poly}(\lambda), \quad T_{\text{Dec}} = O(N^{\gamma}) \text{ poly}(\lambda).
\]

**Theorem 12 (\textbullet).** Suppose in Construction 3, the underlying AH-BTR scheme old is complete, then so is the resultant AH-BTR.

**Theorem 13 (\textbullet).** Suppose in Construction 3, the underlying AH-BTR scheme old is sound, then so is the resultant AH-BTR.

\(^{14}\)We assume that old.ct’s are of deterministic length so Dec knows the location of each particular old.ct. Alternatively, Enc can store a look-up table of their locations in ct.
Proof (Theorem 12). Let \( C \) be an efficient adversary against the completeness of the resultant scheme. Consider the following efficient adversary \( C_{\text{old}} \) against the completeness of old:

- \( C_{\text{old}} \) launches \( C \) to obtain
  \[ \mathcal{D}, \ \{\text{pk}_{j}^{*}\}_{j \in [N]}, \ 1^{1/\epsilon^*}. \]

  It computes \( N_{1}, N_{2} \) as specified by the resultant scheme.

- \( C_{\text{old}} \) samples \( j_{1}^{*} \sim [N_{1}] \), prepares \( \mathcal{D}_{j_{1}^{*}} \) (using \( \mathcal{D} \), as specified by the resultant scheme), and outputs
  \[ \mathcal{D}_{j_{1}^{*}}, \ \{\text{pk}_{j}^{*}\}_{(j_{1}^{*}-1)N_{2}<j\leq j_{1}N_{2}}, \ 1^{N_{1}/\epsilon^*}. \]

Let \( B = \text{poly}(\lambda) \) be an upper bound of \( N_{1} \). Routine calculation shows
\[
\Pr[C_{\text{old}} \text{ wins}] \geq \frac{1}{B} \Pr[C \text{ wins}],
\]

hence by the completeness of old,
\[
\Pr[C \text{ wins}] \leq B \Pr[C_{\text{old}} \text{ wins}] = \text{poly}(\lambda) \text{ negl}(\lambda) = \text{negl}(\lambda). \quad \square
\]

Proof (Theorem 13). Let \( C \) be an efficient adversary against the soundness of the resultant scheme. Consider the following efficient adversary \( C_{\text{old}} \) against the soundness of old:

- \( C_{\text{old}}(\text{pk}) \) launches \( C(\text{pk}) \) to obtain
  \[ \mathcal{D}, \ N, \ i_{1}^{*}, \ \{\text{pk}_{j}^{*}\}_{j \in [N]\setminus \{i_{1}^{*}\}}, \ 1^{1/\epsilon^*}. \]

  It computes \( N_{1}, N_{2} \) as specified by the resultant scheme.

- \( C_{\text{old}} \) computes \( j_{1}^{*} = \lceil i_{1}^{*}/N_{2} \rceil \) and outputs
  \[ \mathcal{D}_{j_{1}^{*}}, \ \min\{N_{2}, N - (j_{1}^{*} - 1)N_{2}\}, \ i_{1}^{*} - (j_{1}^{*} - 1)N_{2}, \ \{\text{pk}_{j}^{*}\}_{(j_{1}^{*}-1)N_{2}<j\leq j_{1}N_{2}, j\neq i_{1}^{*}}, \ 1^{N_{1}/\epsilon^*}. \]

Routine calculation and the soundness of old yield
\[
\Pr[C \text{ wins}] \leq \Pr[C_{\text{old}} \text{ wins}] = \text{negl}(\lambda). \quad \square
\]

7 Lower Bound on Ciphertext Size and Decryption Time

In this section, we prove that for all secure AH-BTR,
\[
|ct| \cdot T_{\text{dec}} = \Omega(N),
\]
and therefore, we have constructed all the optimal (ignoring \( \text{poly}(\lambda) \) factors) AH-BTR schemes in this work, completely pinning down the Pareto front of its efficiency. In fact, we will show a related bound against a restricted kind of broadcast encryption,\(^{15}\) which can be implemented using AH-BTR in a straight-forward manner.

The scheme is restricted in the sense that the users are paired and encryption only broadcasts to those sets for which there is precisely one recipient from each pair. The required security notion is also weaker — it does not consider collusion among multiple non-recipients nor adaptive attacks.

\(^{15}\)The lower bound thus also applies to all mildly expressive attribute-based encryption schemes.
Definition 18 (restricted broadcast encryption and its security). A restricted broadcast encryption (BE) scheme (for the purpose of this work) consists of 3 efficient algorithms:

- Gen($1^\lambda, 1^N$) takes a length parameter as input. It outputs a master public key mpk and a list $\{sk_{j,s}\}_{j \in [N], s \in \{0,1\}}$ of secret keys.
- Enc($1^\lambda$, mpk, $R, \mu$) takes as input the master public key mpk, an $N$-bit string $R \in \{0,1\}^N$, and a message $\mu \in \{0,1\}^\lambda$. It outputs a ciphertext ct$_R$.
- Dec$^{mpk,i,r,sk_{i,r},ct_R}(1^\lambda)$ is given random access to the master public key mpk, a secret key with its description $(i, r, sk_{i,r})$, a ciphertext with its attribute $(R, ct_R)$. It is supposed to recover $\mu$ if and only if $R[i] = r$.

The scheme must be correct, i.e., for all $\lambda, N \in \mathbb{N}, R \in \{0,1\}^N, i \in [N], \mu \in \{0,1\}^\lambda$,
\[
\Pr \left[ (\text{mpk}, \{sk_{j,s}\}_{j \in [N], s \in \{0,1\}}) \overset{s}{\leftarrow} \text{Gen}(1^\lambda, 1^N) \quad \text{ct}_R \overset{s}{\leftarrow} \text{Enc}(1^\lambda, \text{mpk}, R, \mu) \quad : \quad \text{Dec}^{\text{mpk},i,R[i],sk_{i,R[i]},R,\text{ct}_R}(1^\lambda) = \mu \right] = 1.
\]

The scheme is 1-key secure for random challenge against uniform adversaries (or secure for the purpose of this work) if
\[
\{(1^\lambda, \text{mpk}, R, i^*, \mu_0, \text{sk}_{i^*,-R[i^*]},\text{ct}_0)\} \approx \{(1^\lambda, \text{mpk}, R, i^*, \mu_0, \text{sk}_{i^*,-R[i^*]},\text{ct}_1)\},
\]
where
\[
R \overset{s}{\leftarrow} \{0,1\}^N, \quad i^* \overset{r}{\leftarrow} [N],
\]
\[
(\text{mpk}, \{sk_{j,s}\}_{j \in [N], s \in \{0,1\}}) \overset{s}{\leftarrow} \text{Gen}(1^\lambda, 1^N),
\]
\[
\mu_b \overset{r}{\leftarrow} \{0,1\}^\lambda, \quad \text{ct}_b \overset{r}{\leftarrow} \text{Enc}(1^\lambda, \text{mpk}, R, \mu_b) \quad \text{for } b \in \{0,1\},
\]
for all polynomially bounded $N = N(\lambda)$, where the computational indistinguishability only has to hold against uniform adversaries.\footnote{$N$ need not be a computable function of $\lambda$. This does not make the security definition “non-uniformy”, as a standard guessing argument (with advantage sign correction) applies to an interactive formulation in which the uniform and efficient $A$ chooses $N$.}

Theorem 14 (\textcopyright{}). For all secure restricted BE,
\[
\max |\text{ct}| \cdot \max T_{\text{dec}} \geq \frac{N}{1000}
\]
for all polynomially bounded $N = N(\lambda)$ and sufficiently large $\lambda$, where ct runs through all possible ciphertexts and $T_{\text{dec}}$ the time to probe $R$ and produce output by Dec, both for $R$ of length $N$.

We remark that while the statement and the proof here apply to perfectly correct schemes with polynomial security, it is straightforward to adapt them for schemes with sufficient (say, constant) gap between correctness and security.

To prove Theorem 14, we need the following lemma:

Lemma 15 (adapted from Theorem 2 in [Unr07]). For all $N, P \in \mathbb{N}$ subject to $1 \leq P \leq N$, distribution $D$ supported over $\mathbb{Z}$, function $F : \mathbb{Z} \times \{0,1\}^N \rightarrow \{0,1\}^S$, there exists a function $G : \mathbb{Z} \times \{0,1\}^N \rightarrow \{0,1, \bot\}^N$ such that
\[
|\{j \in [N] : G(z,R)[j] \neq \bot\}| \leq P \quad \text{for all } z \in \mathbb{Z} \text{ and } R \in \{0,1\}^N
\]
and for all\textsuperscript{17} oracle (randomized) algorithm $B^Y$ making at most $T$ queries to $Y$,

$$\left| \Pr \left[ B^R(z, F(z, R)) \to 1 \right] - \Pr \left[ B^H(z, F(z, R)) \to 1 \right] \right| \leq \sqrt{\frac{ST}{2P}},$$

where

$$R \xleftarrow{} \{0,1\}^N, \quad z \xleftarrow{} D, \quad H[j] = \begin{cases} G(z, R)[j], & \text{if } G(z, R)[j] \neq \bot; \\ \{0,1\}, & \text{if } G(z, R)[j] = \bot. \end{cases}$$

\textbf{Proof (Theorem 14).} Define

$$S = 1 + \max \{ \text{ct} \}, \quad T = 1 + \max \{ \text{number of bits in } R \text{ probed by } \text{Dec} \}.$$ 

For $\lambda, N \geq 1$, it is necessary that $|\text{ct}| \geq 1$ because $\text{ct}$ can encode any string $\mu$ of length $\lambda$, and that $\max T_{\text{Dec}} \geq T$ because $\text{Dec}$ performs all the probes and, in addition, produces at least 1 bit of output. Therefore,

$$\max |\text{ct}| \cdot \max T_{\text{Dec}} \geq \frac{\max |\text{ct}| + 1}{2} \cdot \max T_{\text{Dec}} \geq \frac{ST}{2}.$$ 

It remains to prove $ST \geq \frac{2N}{1000}$ for sufficiently large $\lambda$. It suffices to consider the case when $N \geq 2$ and $ST \leq 2N$.

We prepare for Lemma 15. Let $P$ be determined later, and

$$z = \left( \mu, z_{\text{Enc}}, \text{mpk}, \{sk_{j, s}\}_{j \in \{N\}, s \in \{0,1\}} \right) \sim D = \begin{cases} \mu \xleftarrow{} \{0,1\}^N, & \text{z}_{\text{Enc}}: \text{randomness for Enc} \\ (\text{mpk}, \{sk_{j, s}\}_{j \in \{N\}, s \in \{0,1\}}) \xleftarrow{} \text{Gen}(1^N) \end{cases},$$

$$F(z, R) = 0^{S-|\text{ct}|-1} \parallel 1 \parallel \text{ct}, \quad \text{where } \text{ct} \leftarrow \text{Enc}(\text{mpk}, R, \mu; z_{\text{Enc}}).$$

Let $G$ be the function guaranteed by Lemma 15 and make $B^Y(z, f)$ do the following:

- Sample $i^* \xleftarrow{} [N]$ and query $r^* \leftarrow Y[i^*]$.
- Read $\mu, \text{mpk}, sk_{i^*, r^*}$ from $z$. Read $\text{ct}$ from $f$.
- Run $\mu' \xleftarrow{} \text{Dec}^{\text{mpk}, i^*, r^*, sk_{i^*, r^*}, Y, \text{ct}()}$.
- Output 1 if and only if $\mu = \mu'$.

Note that $B$ indeed makes at most $T$ queries to $Y$, the first to obtain $r^*$ and the rest to run Dec.

For $w \in \{1, 2, 3, 4, 5\}$, write $p_w$ for $\Pr[B^Y_w(z, f; i^*) \to 1]$, where

$$\begin{align*}
&Y_1 = R, \\
&Y_2[j] = \begin{cases} G(z, F(z, R))[j], & \text{if } G(z, F(z, R))[j] \neq \bot; \\ \{0,1\}, & \text{if } G(z, F(z, R))[j] = \bot; \end{cases} \\
&Y_3[j] = \begin{cases} G(z, F(z, R))[j], & \text{if } j \neq i^* \text{ and } G(z, F(z, R))[j] \neq \bot; \\ \{0,1\}, & \text{if } j = i^*; \end{cases} \\
&Y_4[j] = \begin{cases} R[j], & \text{if } j \neq i^*; \\ \{0,1\}, & \text{if } j = i^*; \end{cases} \\
&Y_5[j] = \begin{cases} R[j], & \text{if } j \neq i^*; \\ -R[i^*], & \text{if } j = i^*. \end{cases}
\end{align*}$$

\textsuperscript{17}Here, $B^Y$ need not be efficient for the lemma to hold. The particular $B^Y$ used in this work is efficient.
By the correctness of the restricted BE scheme, \( p_1 = 1 \).

From Lemma 15,

\[
|p_1 - p_2| \leq \sqrt{\frac{ST}{2P}}, \quad |p_4 - p_3| \leq \sqrt{\frac{ST}{2P}}.
\]

Here, the second inequality is obtained by applying the lemma to

\[
C^Y(z,f) = B^Y(z,f;i^*), \quad \text{where } i^* \overset{s}{\leftarrow} [N], \quad Y'[j] = \begin{cases} Y[j], & \text{if } j \neq i^*; \\ \{0,1\}, & \text{if } j = i^*.
\end{cases}
\]

Clearly, \( |p_2 - p_3| \leq \frac{P}{N} \). Setting \( P = \left\lceil \frac{3STN^2}{2} \right\rceil \), we have

\[
|p_1 - p_4| \leq |p_1 - p_2| + |p_2 - p_3| + |p_3 - p_4| \leq \sqrt{\frac{ST}{2P}} + \frac{P}{N} + \sqrt{\frac{ST}{2P}} \leq 3\sqrt{\frac{ST}{2N}} + \frac{1}{N} < 4\sqrt{\frac{ST}{2N}},
\]

where the last inequality follows from \( N \geq 2 \). By how \( Y[i^*] \) is set,

\[
p_4 = \frac{p_1 + p_5}{2} \implies p_5 = p_1 - 2(p_1 - p_4) \geq p_1 - 2|p_1 - p_4| > 1 - 8\sqrt{\frac{ST}{2N}}.
\]

Consider the following adversary \( A(\text{mpk}, R, i^*, \mu_0, \text{sk}_{i^*}, \neg R[i^*], ct) \) against the security of the restricted BE scheme:

- Construct \( Y_5 \) from \( R \) and let \( r^* \leftarrow Y_5[i^*] = \neg R[i^*] \).
- Run \( \mu' \overset{s}{\leftarrow} \text{Dec}^\text{mpk}_{i^*,r^*,\text{sk}_{i^*},Y_5,ct}() \), i.e., pretend \( R[i^*] \) were \( \neg R[i^*] \) and try decrypting using the key given to \( A \).
- Output 1 if and only if \( \mu' = \mu_0 \).

If \( ct = ct_1 \) is an encryption of \( \mu_1 \), then \( \mu_0 \) is uniformly random and independent of everything else, hence

\[
\Pr[A(\cdots) \rightarrow 1 \text{ with } ct = ct_1] \leq 2^{-\lambda}.
\]

Note that \( A \) is a uniform adversary. By the security of the restricted BE scheme,

\[
p_5 = \Pr[B^{Y_5}(z,f;i^*) \rightarrow 1] = \Pr[A(\cdots) \rightarrow 1 \text{ with } ct = ct_0] \leq 2^{-\lambda} + \text{negl}(\lambda) < \frac{1}{5}
\]

for sufficiently large \( \lambda \), which gives

\[
1 - 8\sqrt{\frac{ST}{2N}} < p_5 < \frac{1}{5} \implies ST > \frac{2N}{1000}.
\]

Corollary 16 (\( \star \)). For all secure AH-BTR,

\[
\max |ct| \cdot \max T_{\text{dec}} \geq \frac{N}{1000}
\]

for all polynomially bounded \( N = N(\lambda) \) and sufficiently large \( \lambda \), where \( T_{\text{dec}} \) only counts the time to probe \( \text{pk}_j \)’s and produce output. Ignoring \( \text{poly}(\lambda) \) factors, Construction 3 achieves all possible optimal trade-offs in terms of the exponents over \( N \) in the dependency of ciphertext size and (actual) decryption time, fully demonstrating the Pareto front of AH-BTR efficiency.
Proof (Corollary 16). Let \( \text{ahBTR} = (\text{ahBTR.Gen}, \text{ahBTR.Enc}, \text{ahBTR.Dec}, \text{ahBTR.Trace}) \) be a secure AH-BTR and construct the following restricted BE scheme:

- \( \text{Gen}(1^N) \) runs

  \[
  (pk_{j,s}, sk_{j,s}) \xleftarrow{s} \text{ahBTR.Gen()} \quad \text{for } j \in [N], s \in \{0, 1\}
  \]

  and outputs \( \text{mpk} = \{pk_{j,s}\}_{j \in [N], s \in \{0, 1\}} \) with \( \{sk_{j,s}\}_{j \in [N], s \in \{0, 1\}} \).

- \( \text{Enc}(\text{mpk}, R, \mu) \) runs and outputs

  \[
  ct \xleftarrow{s} \text{ahBTR.Enc}(\{pk_{j,R[j]}\}_{j \in [N]}, \mu).
  \]

- \( \text{Dec}^{\text{mpk},i,r,sk_{i,r},R,ct}() \) runs \( \text{ahBTR.Dec}^K,ct(N,i,sk_{i,r}) \), where \( K \) is an oracle implemented by \( \text{Dec} \) for \( \text{ahBTR.Dec} \) to probe \( pk_j \)'s. Whenever \( \text{ahBTR.Dec} \) probes \( pk_j[m_0] \), we make \( \text{Dec} \) probe \( R[j] \) and answer \( pk_{j,R[j]}[m_0] \).

It is straightforward to verify that the constructed scheme is correct and secure. Since a restricted BE ciphertext is precisely an AH-BTR ciphertext, each probe to \( pk_j \)'s by \( \text{ahBTR.Dec} \) translates to exactly one probe to \( R[j] \) by \( \text{Dec} \) with no more additional probes by \( \text{Dec} \) on its own, and \( \text{Dec} \) outputs whatever \( \text{ahBTR.Dec} \) outputs, the corollary follows from Theorem 14. \( \square \)

Acknowledgement. The author was supported by NSF grants CNS-1936825 (CAREER), CNS-2026774, a J.P. Morgan AI Research Award, and a Simons Collaboration on the Theory of Algorithmic Fairness. The views expressed in this work are those of the author and do not reflect the official policy or position of any of the supporters. The author thanks Huijia Lin for her encouragement and support for him to pursue an independent research project (culminating this paper), Hoeteck Wee for helpful suggestions on writing from another context, and Daniel Wichs for helpful discussions. He started researching this topic after rereading a post [sil21] on V2EX.

References


[DPP07] Cécile Delerablée, Pascal Paillier, and David Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or


Qianhong Wu, Bo Qin, Lei Zhang, and Josep Domingo-Ferrer. Ad hoc broadcast encryption (poster presentation). In Ehab Al-Shaer, Angelos D.


