Blind Identity-Based Encryption and Simulatable Oblivious Transfer*

Matthew Green and Susan Hohenberger

The Johns Hopkins University
Information Security Institute
3400 N. Charles Street; Baltimore, MD 21218, USA
{mgreen,susan}@cs.jhu.edu

Abstract. In an identity-based encryption (IBE) scheme, there is a *key extraction* protocol where a user submits an identity string to a master authority who then returns the corresponding secret key for that identity. In this work, we describe how this protocol can be performed efficiently and in a *blind* fashion for several known IBE schemes; that is, a user can obtain a secret key for an identity without the master authority learning anything about this identity.

We formalize this notion as *blind IBE* and discuss its many practical applications. In particular, we build upon the recent work of Camenisch, Neven, and shelat [12] to construct oblivious transfer (OT) schemes which achieve full simulatability for both sender and receiver. OT constructions with comparable efficiency prior to Camenisch *et al.* were proven secure in the weaker half-simulation model. Our OT schemes are constructed from the blind IBE schemes we propose, which require only static complexity assumptions (*e.g.*, DBDH) whereas prior comparable schemes require dynamic assumptions (*e.g.*, q-PDDH).

1 Introduction

In an oblivious transfer (OT_k^N) protocol, introduced by Rabin [41] and generalized by Even, Goldreich and Lempel [25] and Brassard, Crépeau and Robert [10], a Sender with messages $M_1, \ldots, M_N$ and a Receiver with indices $\sigma_1, \ldots, \sigma_k \in [1, N]$ interact in such a way that at the end the Receiver obtains $M_{\sigma_1}, \ldots, M_{\sigma_k}$ without learning anything about the other messages and the Sender does not learn anything about $\sigma_1, \ldots, \sigma_k$. Naor and Pinkas were the first to consider an *adaptive* setting, $\mathsf{OT}_{k \times 1}^N$, where the sender may obtain $M_{\sigma_{i-1}}$ before deciding on σ_i [36]. Oblivious transfer is a useful, interesting primitive in its own right, but it has even greater significance as OT_1^4 is a key building block for secure multi-party computation [46,28,32]. Realizing efficient protocols under modest complexity assumptions is therefore an important goal.

The definition of security for oblivious transfer has been evolving. Informally, security is defined with respect to an ideal-world experiment in which the Sender

* This work was supported in part by the NSF under grant CT-0716142.

K. Kurosawa (Ed.): ASIACRYPT 2007, LNCS 4833, pp. 265–282, 2007.

and Receiver exchange messages via a trusted party. An OT protocol is secure if, for every real-world cheating Sender (resp., Receiver) we can describe an ideal-world counterpart who gains as much information from the ideal-world interaction as from the real protocol. Bellare and Micali [1] presented the first practical OT_1^2 protocol to satisfy this intuition in the honest-but-curious model. This was followed by practical OT protocols due to Naor and Pinkas [35,36,37] in the "half-simulation" model where the simulation-based model (described above) is used only to show Sender security and Receiver security is defined by a simpler game-based definition. Almost all efficient OT protocols are proven secure with respect to the half-simulation model, *e.g.,* [36,35,37,24,38,31]. Unfortunately, Naor and Pinkas demonstrated that this model permits *selective-failure* attacks, in which a malicious Sender can induce transfer failures that are dependent on the message that the Receiver requests [36].

Recently, Camenisch, Neven, and shelat [12] proposed practical $\mathsf{OT}_{k\times 1}^N$ protocols that are secure in the "full-simulation" model, where the security of both the Sender and Receiver are simulation-based. These simulatable OT protocols are particularly nice because they can be used to construct other cryptographic protocols in a simulatable fashion. More specifically, Camenisch *et al.* [12] provide two distinct results. First, they show how to efficiently construct $\mathsf{OT}_{k\times 1}^N$ generically from any unique blind signature scheme in the random oracle model. The two known efficient unique blind signature schemes due to Chaum [19] and Boldyreva [2] both require *interactive* complexity assumptions: one-more-inversion RSA and chosen-target CDH, respectively. (Interestingly, when instantiated with Chaum signatures, this construction coincides with a prior one of Ogata and Kurosawa [38] that was analyzed in the half-simulation model.) Second, they provide a clever $\mathsf{OT}_{k\times 1}^N$ construction in the standard model based on dynamic complexity assumptions, namely the q-Power Decisional Diffie-Hellman (*i.e.*, in a bilinear setting $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, given $(g, g^x, g^{x^2}, \ldots, g^{x^q}, H)$ where $g \leftarrow \mathbb{G}$ and $H \leftarrow \mathbb{G}_T$, distinguish $(H^x, H^{x^2}, \ldots, H^{x^q})$ from random values) and q-Strong Diffie-Hellman (q-SDH) assumptions. (Unfortunately, Cheon showed that q-SDH requires larger than commonly used security parameters [21]). These dynamic (including interactive) assumptions seem significantly stronger than those, such as DDH and quadratic residuosity, used to construct efficient OT schemes in the half-simulation model. Thus, a well-motivated problem is to find efficient, fully-simulatable OT schemes under weaker complexity assumptions.

Our Contributions. In this work, we provide, to our knowledge, the first efficient and fully-simulatable OT_k^N and $\mathsf{OT}_{k\times 1}^N$ schemes secure under *static* complexity assumptions (*e.g.*, DBDH, where given (g, g^a, g^b, g^c), it is hard to distinguish $e(g, g)^{abc}$ from random). We summarize our results as follows.

First, we introduce a building block, which is of independent interest. In identity-based encryption (IBE) [43], there is an *extraction* protocol where a user submits an identity string to a master authority who then returns the corresponding decryption key for that identity. We formalize the notion of *blindly* executing this protocol, in a strong sense; where the authority does not learn the identity nor can she cause failures dependent on the identity, and the user learns nothing beyond the normal extraction protocol. This concept has similarities to recent work by Goyal [29], in which a user wishes to hide certain characteristics of an extracted IBE key from the authority. In §3.1, we describe efficient *blind extraction* protocols satisfying this definition for the IBE schemes due to Boneh and Boyen [3] and Waters [44] (using a generalization proposed independently by Naccache [34] and Chatterjee and Sarkar [17]). The latter protocol is similar to a blind signature scheme proposed by Okamoto [39]. We call IBE schemes supporting efficient blind extraction protocols: *blind IBE*, for short.

Second, we present an efficient and fully-simulatable OT_k^N protocol constructed from any of the proposed blind IBE schemes (without requiring additional assumptions), and thus our constructions are secure under only DBDH. Intuitively, consider the following OT_k^N construction. The Sender runs the IBE setup algorithm and sends the corresponding public parameters to the Receiver. Next, for $i = 1$ to N, the Sender encrypts M_i under identity "i" and sends this ciphertext to the Receiver. To obtain k messages, the Receiver blindly extracts k decryption keys for identities of his choice and uses these keys to decrypt and recover the corresponding messages. While this simple protocol does not appear to be simulatable, we are able to appropriately modify it. (Indeed, one must also be cautious of possibly malformed ciphertexts, as we discuss later.) Our constructions from blind IBE are inspired by the Camenisch *et al.* [12] generic construction from unique blind signatures. Indeed, recall that the secret keys sk_{id} of any fully-secure IBE can be viewed as signatures by the authority on the message *id* [6]. Camenisch *et al.* [12] require *unique* blind signatures, whereas we do not; however, where they require unforgeability, we require that our "blind key extraction" protocol does not jeopardize the semantic security of the IBE.

Third, we present an efficient and fully-simulatable $\mathsf{OT}_{k\times 1}^N$ protocol constructed from our proposed blind IBE schemes in the random oracle model. We discuss how to remove these oracles at an additional cost. This improves on the complexity assumptions required by the comparable random-oracle scheme in Camenisch *et al.* [12], although we leave the same improvement for their adaptive construction without random oracles as an open problem. Finally, in §5, we discuss the independent usefulness of blind IBE to other applications, such as blind signatures, anonymous email, and encrypted keyword search.

2 Technical Preliminaries

Let $\mathsf{BMsetup}$ be an algorithm that, on input the security parameter 1^κ, outputs the parameters for a bilinear mapping as $\gamma = (q, g, \mathbb{G}, \mathbb{G}_T, e)$, where g generates $\mathbb{G}$, both $\mathbb{G}$ and $\mathbb{G}_T$ have prime order q, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. In our schemes, we will require that the correctness of these parameters be publicly verifiable (Chen *et al.* [20] describe efficient techniques for verifying these parameters in a typical instantiation). We will refer to the following complexity assumption made in these groups.

Decisional Bilinear Diffie-Hellman (DBDH) [6]: Let $\mathsf{BMsetup}(1^\kappa) \to (q, g, \mathbb{G}, \mathbb{G}_T, e)$. For all p.p.t. adversaries Adv, the following probability is strictly less than $1/2 + 1/\mathrm{poly}(\kappa)$: $\Pr[a,b,c,d \leftarrow \mathbb{Z}_q;\ x_0 \leftarrow e(g,g)^{abc};\ x_1 \leftarrow e(g,g)^d;\ z \leftarrow \{0,1\};\ z' \leftarrow \mathsf{Adv}(g,g^a,g^b,g^c,x_z) : z = z']$.

Known Discrete-Logarithm-Based, Zero-Knowledge Proofs. We use known techniques for proving statements about discrete logarithms, such as (1) proof of knowledge of a discrete logarithm modulo a prime [42], (2) proof that a committed value lies in a given integer interval [16,11,8], and also (3) proof of the disjunction or conjunction of any two of the previous [23]. These protocols are secure under the discrete logarithm assumption, although some implementations of (2) require the Strong RSA assumption.

When referring to the proofs above, we will use the notation of Camenisch and Stadler [13]. For instance, $PoK\{(x,r) : y = g^x h^r \wedge (1 \leq x \leq n)\}$ denotes a zero-knowledge proof of knowledge of integers x and r such that $y = g^x h^r$ holds and $1 \leq x \leq n$. All values not in enclosed in ()'s are assumed to be known to the verifier. We can apply the Fiat-Shamir heuristic [26] to make such proofs non-interactive in the random oracle model.

Commitments. Let ($\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Decommit}$) be a commitment scheme where CSetup generates public parameters ρ; on input a message M, $\mathsf{Commit}(\rho, M)$ outputs a pair $(\mathcal{C}, \mathcal{D})$; and $\mathsf{Decommit}(\rho, M, \mathcal{C}, \mathcal{D})$ outputs 1 if $\mathcal{D}$ decommits $\mathcal{C}$ to M, or 0 otherwise. Our subsequent constructions require an efficient protocol for proving knowledge of a decommitment $\mathcal{D}$ with respect to $(\rho, M, \mathcal{C})$. We recommend using the Pedersen commitment scheme [40] based on the discrete logarithm assumption, in which the public parameters are a group of prime order q, and random generators $(g_0, \ldots, g_m)$. In order to commit to the values $(v_1, \ldots, v_m) \in \mathbb{Z}_q^m$, pick a random $r \in \mathbb{Z}_q$ and set $\mathcal{C} = g_0^r \prod_{i=1}^m g_i^{v_i}$ and $\mathcal{D} = r$. Schnorr's technique [42] is used to efficiently prove knowledge of the value $\mathcal{D} = r$.

3 Blind Identity-Based Encryption

An identity-based encryption (IBE) scheme supports two types of players: a single master authority and multiple users; together with the algorithms Setup, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$ and the protocol $\mathsf{Extract}$. Let us provide some input/output specification for these protocols with intuition for what they do.

Notation: Let $\mathcal{I}$ be the identity space and $\mathcal{M}$ be the message space. We write $P(\mathcal{A}(a), \mathcal{B}(b)) \rightarrow (c, d)$ to indicate that protocol P is between parties $\mathcal{A}$ and $\mathcal{B}$, where a is $\mathcal{A}$'s input, c is $\mathcal{A}$'s output, b is $\mathcal{B}$'s input and d is $\mathcal{B}$'s output.

- In the $\mathsf{Setup}(1^\kappa, c(\kappa))$ algorithm, on input a security parameter 1^κ and a description of an the identity space $|\mathcal{I}| \leq 2^{c(\kappa)}$ where $c(\cdot)$ is a computable, polynomially-bounded function, the master authority $\mathcal{P}$ outputs master parameters *params* and a master secret key *msk*.
- In the $\mathsf{Extract}(\mathcal{P}(params, msk), \mathcal{U}(params, id)) \rightarrow (id, sk_{id})$ protocol, an honest user $\mathcal{U}$ with identity $id \in \mathcal{I}$ obtains the corresponding secret key sk_{id} from the master authority $\mathcal{P}$ or outputs an error message. The master authority's output is **the identity** *id* or an error message.

- In the $\mathsf{Encrypt}(params, id, m)$ algorithm, on input identity $id \in \mathcal{I}$ and message $m \in \mathcal{M}$, any party can output ciphertext C.
- In the $\mathsf{Decrypt}(params, id, sk_{id}, C)$ algorithm, on input a ciphertext C, the user with sk_{id} outputs a message $m \in \mathcal{M}$ or the distinguished symbol ϕ.

Definition 1 (Selective-Identity Secure IBE (IND-sID-CPA) [15]). *Let κ be a security parameter, $c(\cdot)$ be a polynomially-bounded function, $|\mathcal{I}| \leq 2^{c(\kappa)}$ and $\mathcal{M}$ be the message space. An IBE is* IND-sID-CPA*-secure if every p.p.t. adversary $\mathcal{A}$ has an advantage negligible in κ for the following game: (1) $\mathcal{A}$ outputs a target identity $id^* \in \mathcal{I}$. (2) Run $\mathsf{Setup}(1^\kappa, c(\kappa))$ to obtain $(params, msk)$, and give params to $\mathcal{A}$. (3) $\mathcal{A}$ may query an oracle $O_{params,msk}(\cdot)$ polynomially many times, where on any input $id \neq id^*$ in $\mathcal{I}$, the oracle returns sk_{id}, and on any other input, the oracle returns an error message. (4) $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$ where $|m_0| = |m_1|$. Select a random bit b and give $\mathcal{A}$ the challenge ciphertext $c^* \leftarrow \mathsf{Encrypt}(params, id^*, m_b)$. (5) $\mathcal{A}$ may continue to query oracle $O_{msk}(\cdot)$ under the same conditions as before. (6) $\mathcal{A}$ outputs $b' \in \{0,1\}$. We define $\mathcal{A}$'s advantage in the above game as $|\Pr[b' = b] - 1/2|$.*

On stronger notions of ciphertext security for IBE. A stronger notion of ciphertext security for IBE schemes is adaptive-identity security (IND-ID-CPA) [6], which strengthens the IND-sID-CPA definition by allowing $\mathcal{A}$ to select the target identity id^* at the start of step (4) in the above game. In §3.1, we show blind IBE schemes satisfying both IND-sID-CPA and IND-ID-CPA security. Fortunately, our oblivious transfer applications in §4 require only IND-sID-CPA-security (because the "identities" will be fixed integers from 1 to poly(κ)), some additional applications in §5 require the stronger IND-ID-CPA-security.

Blind IBE. So far, we have only described traditional IBE schemes. A *blind IBE* scheme consists of the same players, together with the same algorithms Setup, Encrypt, Decrypt and yet we replace the protocol Extract with a new protocol BlindExtract which differs only in the authority's output:

- In the $\mathsf{BlindExtract}(\mathcal{P}(params, msk), \mathcal{U}(params, id)) \rightarrow (\text{nothing}, sk_{id})$ protocol, an honest user $\mathcal{U}$ with identity $id \in \mathcal{I}$ obtains the corresponding secret key sk_{id} from the master authority $\mathcal{P}$ or outputs an error message. The master authority's output is **nothing** or an error message.

We now define security for blind IBE, which informally is any IND-sID-CPA-secure IBE scheme with a BlindExtract protocol that satisfies two properties:

1. **Leak-free Extract:** a potentially malicious user cannot learn anything by executing the BlindExtract protocol with an honest authority which she could not have learned by executing the Extract protocol with an honest authority; moreover, as in Extract, the user must know the identity for which she is extracting a key.
2. **Selective-failure Blindness:** a potentially malicious authority cannot learn anything about the user's choice of identity during the BlindExtract protocol; moreover, the authority cannot cause the BlindExtract protocol to fail in a manner dependent on the user's choice.

Of course, a protocol realizing the functionality $\mathsf{BlindExtract}$ (in a fashion that satisfies the properties above) is a special case of secure two-party computation [46,28,32]. However, using generic tools may be inefficient, so as in the case of blind signature protocols, we seek to optimize this specific computation. Let us now formally state these properties.

Definition 2 (Leak-Free Extract). *A protocol* $\mathsf{BlindExtract} = (\mathcal{P},\mathcal{U})$ *associated with an IBE scheme* $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *is* leak free *if for all efficient adversaries* $\mathcal{A}$*, there exists an efficient simulator* $\mathcal{S}$ *such that for every value* κ *and polynomial* $c(\cdot)$*, no efficient distinguisher* D *can distinguish whether* $\mathcal{A}$ *is playing Game Real or Game Ideal with non-negligible advantage:*

Game Real: *Run* $(params, msk) \leftarrow \mathsf{Setup}(1^\kappa, c(\kappa))$*. As many times as* D *wants,* $\mathcal{A}$ *chooses an identity* id *and executes the* $\mathsf{BlindExtract}$ *protocol with* $\mathcal{P}$*:* $\mathsf{BlindExtract}(\mathcal{P}(params, msk), \mathcal{A}(params, id))$.

Game Ideal: *Run* $(params, msk) \leftarrow \mathsf{Setup}(1^\kappa, c(\kappa))$*. As many times as* D *wants,* $\mathcal{S}$ *chooses an identity* id *and queries a trusted party to obtain the output of* $\mathsf{Extract}(params, msk, id)$*, if* $id \in \mathcal{I}$ *and* $\perp$ *otherwise.*

Here D *and* $\mathcal{A}$ *(or* $\mathcal{S}$*) may communicate at any time. Also,* $params$ *defines* $\mathcal{I}$*.*

This definition implies that the identity id (for the key being extracted) is *extractable* from the $\mathsf{BlindExtract}$ protocol, since $\mathcal{S}$ must be able to interact with $\mathcal{A}$ to learn which identities to submit to the trusted party. We will make use of this observation later. Another nice property of this definition is that any key extraction protocol with leak-freeness (regardless of whether blindness holds or not) composes into the existing security definitions for IBE. (This would not necessarily be true of a blind signature protocol for the same type of signatures.) We state this formally below.

Lemma 1. *If* $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *is an* $\mathsf{IND\text{-}sID\text{-}CPA}$*-secure (resp.,* $\mathsf{IND\text{-}ID\text{-}CPA}$*) IBE scheme and* $\mathsf{BlindExtract}$ *associated with* Π *is leak-free, then* $\Pi' = (\mathsf{Setup}, \mathsf{BlindExtract}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *is an* $\mathsf{IND\text{-}sID\text{-}CPA}$*-secure (resp.,* $\mathsf{IND\text{-}ID\text{-}CPA}$*) IBE scheme.*

Next, we define the second property of *blindness*. We use a strong notion of blindness called *selective-failure blindness* proposed recently by Camenisch et al. [12], ensuring that even a malicious authority is unable to induce $\mathsf{BlindExtract}$ protocol failures that are dependent on the identity being extracted.

Definition 3 (Selective-Failure Blindness (SFB) [12]). *A protocol* $P(\mathcal{A}(\cdot), \mathcal{U}(\cdot,\cdot))$ *is said to be selective-failure blind if every p.p.t. adversary* $\mathcal{A}$ *has a negligible advantage in the following game: First,* $\mathcal{A}$ *outputs params and a pair of identities* $id_0, id_1 \in \mathcal{I}$*. A random* $b \in \{0,1\}$ *is chosen.* $\mathcal{A}$ *is given black-box access to two oracles* $\mathcal{U}(params, id_b)$ *and* $\mathcal{U}(params, id_{b-1})$*. The* $\mathcal{U}$ *algorithms produce local output* sk_b *and* sk_{b-1} *respectively. If* $sk_b \neq \perp$ *and* $sk_{b-1} \neq \perp$ *then* $\mathcal{A}$ *receives* (sk_0, sk_1)*. If* $sk_b = \perp$ *and* $sk_{b-1} \neq \perp$ *then* $\mathcal{A}$ *receives* $(\perp, \varepsilon)$*. If* $sk_b \neq \perp$ *and* $sk_{b-1} = \perp$ *then* $\mathcal{A}$ *receives* $(\varepsilon, \perp)$*. If* $sk_b = \perp$ *and* $sk_{b-1} = \perp$ *then* $\mathcal{A}$ *receives* $(\perp, \perp)$*. Finally,* $\mathcal{A}$ *outputs its guess* b'*. We define* $\mathcal{A}$*'s advantage in the above game as* $|\Pr[b' = b] - 1/2|$*.*

We thus arrive at the following definition.

Definition 4 (Secure Blind IBE). *A blind IBE Π =* (Setup*,* BlindExtract*,* Encrypt*,* Decrypt*) is called* IND-sID-CPA-secure *(resp.* IND-ID-CPA*) if and only if: (1) Π is* IND-sID-CPA*-secure (resp.* IND-ID-CPA*), and (2)* BlindExtract *is leak free and selective-failure blind.*

3.1 IBE Schemes with Efficient BlindExtract Protocols

In this section, we describe efficient BlindExtract protocols for: (1) the IND-sID-CPA-secure IBE due to Boneh and Boyen [3] and (2) the IND-ID-CPA-secure IBE proposed independently by Naccache [34] and Chatterjee-Sarkar [17] which is a generalized version of Waters IBE [44]. Note that in §3.3 we will be adding some additional features to these IBE schemes; these will help us to construct oblivious transfer protocols in §4. Since all of these schemes share a similar structure, we'll begin by describing their common elements.

Setup$(1^\kappa, c(k))$**:** Let $\gamma = (q, g, \mathbb{G}, \mathbb{G}_T, e)$ be the output of BMsetup(1^κ). Choose random elements $h, g_2 \in \mathbb{G}$ and a random value $\alpha \in \mathbb{Z}_q$. Set $g_1 = g^\alpha$. Finally, select a function $F : \mathcal{I} \to \mathbb{G}$ that maps identities to group elements. (The descriptions of F and $\mathcal{I}$ will be defined specific to the schemes below.) Output $params = (\gamma, g, g_1, g_2, h, F)$ and $msk = g_2^\alpha$.

Extract**:** Identity secret keys are of the form: $sk_{id} = (d_0, d_1) = (g_2^\alpha \cdot F(id)^r, g^r)$, where $r \in \mathbb{Z}_q$ is randomly chosen by the master authority. Note that the correctness of these keys can be publicly verified using a test described below.

Encrypt$(params, id, M)$**:** Given an identity $id \in \mathcal{I}$, and a message $M \in \mathbb{G}_T$, select a random $s \in \mathbb{Z}_q$ and output the ciphertext $C = (e(g_1, g_2)^s \cdot M, g^s, F(id)^s)$.

Decrypt$(params, id, sk_{id}, c_{id})$**:** On input a decryption key $sk_{id} = (d_0, d_1) \in \mathbb{G}^2$ and a ciphertext $C = (X, Y, Z) \in \mathbb{G}_T \times \mathbb{G}^2$, output $M = X \cdot e(Z, d_1)/e(Y, d_0)$.

Next, we'll describe the precise format of the secret keys sk_{id} and corresponding BlindExtract protocols for particular IBEs.

A BlindExtract Protocol for an IND-sID-CPA-Secure IBE. In the Boneh-Boyen IBE [3], $\mathcal{I} \subseteq \mathbb{Z}_q$ and the function $F : \mathcal{I} \to \mathbb{G}$ is defined as $F(id) = h \cdot g_1^{id}$. A secret key for identity id, where $r \in \mathbb{Z}_q$ is random, is:

$$sk_{id} = (d_0, d_1) = (g_2^\alpha \cdot F(id)^r, g^r) = (g_2^\alpha \cdot (h \cdot g_1^{id})^r, g^r).$$

The protocol BlindExtract$(\mathcal{P}(params, msk), \mathcal{U}(params, id))$ is described in Figure 1. Recall that $\mathcal{U}$ wants to obtain sk_{id} without revealing id, and $\mathcal{P}$ wants to reveal no more than sk_{id}. Let Π_1 be the blind IBE that combines algorithms Setup, Encrypt, Decrypt with the protocol BlindExtract in Figure 1.

Theorem 1. *Under the DBDH assumption, blind IBE Π_1 is secure (according to Definition 4); i.e.,* BlindExtract *is both leak-free and selective-failure blind.*

A proof of Theorem 1 is presented in the full version of this work [30].

$\underline{\mathcal{P}(params, msk)}$	$\underline{\mathcal{U}(params, id)}$
	1. Choose $y \xleftarrow{\$} \mathbb{Z}_q$.
	2. Compute $h' \leftarrow g^y g_1^{id}$ and send h' to $\mathcal{P}$.
	3. Execute $PoK\{(y, id) : h' = g^y g_1^{id}\}$.
4. If the proof fails to verify, abort.	
5. Choose $r \xleftarrow{\$} \mathbb{Z}_q$.	
6. Compute $d_0' \leftarrow g_2^{\alpha} \cdot (h'h)^r$.	
7. Compute $d_1' \leftarrow g^r$.	
8. Send (d_0', d_1') to $\mathcal{U}$.	
	9. Check that $e(g_1, g_2) \cdot e(d_1', h'h) = e(d_0', g)$.
	10. If the check passes, choose $z \xleftarrow{\$} \mathbb{Z}_q$; otherwise, output $\perp$ and abort.
	11. Compute $d_0 \leftarrow (d_0'/(d_1')^y) \cdot F(id)^z$ and $d_1 \leftarrow d_1' \cdot g^z$.
	12. Output $sk_{id} = (d_0, d_1)$.

Fig. 1. A BlindExtract protocol for the Boneh-Boyen IBE

A BlindExtract Protocol for an IND-ID-CPA-Secure IBE. In the generalized version of Waters IBE [44], proposed independently by Naccache [34] and Chatterjee and Sarkar [17], the identity space $\mathcal{I}$ is the set of bit strings of length N, where N is polynomial in κ, represented by n blocks of ℓ bits each. The function $F : \{0,1\}^N \rightarrow \mathbb{G}$ is defined as $F(id) = h \cdot \prod_{j=1}^{n} u_j^{a_j}$, where each $u_j \in \mathbb{G}$ is randomly selected by the master authority and each a_j is an ℓ-bit segment of id. Naccache discusses practical IBE deployment with $N = 160$ and $\ell = 32$ [34]. A secret key for identity id, where $r \in \mathbb{Z}_q$ is random, is:

$$sk_{id} = (d_0, d_1) = (g_2^{\alpha} \cdot F(id)^r, g^r) = (g_2^{\alpha} \cdot (h \cdot \prod_{j=1}^{n} u_j^{a_j})^r, g^r).$$

The protocol BlindExtract($\mathcal{P}(params, msk), \mathcal{U}(params, id)$) is described in Figure 1, with the following alterations. Parse the identity as $id = (a_1, \ldots, a_n)$, where each a_i is ℓ bits. In line 2, compute h' as $g^y \cdot \prod_{j=1}^{n} u_j^{a_j}$. In line 3, execute the proof $PoK\{(y, a_1, \ldots, a_n) : h' = g^y \cdot \prod_{j=1}^{n} u_j^{a_j} \wedge 0 \leq a_i < 2^{\ell}$, for $i = 1$ to $n\}$. The range part of this proof (*e.g.*, $0 \leq a_i < 2^{\ell}$) can be performed exactly or, by shortening each a_i by a few bits, can be done at almost no additional cost [16,11,8]. Follow the rest of the protocol as is. Let Π_2 be the blind IBE that combines Setup, Encrypt, Decrypt with the BlindExtract protocol described above.

Theorem 2. *Under the DBDH assumption, blind IBE Π_2 is secure (according to Definition 4); i.e.,* BlindExtract *is both leak-free and selective-failure blind.*

A proof of Theorem 2 is presented in the full version of this paper [30].

3.2 On Other IBEs and HIBEs

Let us briefly summarize what we know about efficient $\mathsf{BlindExtract}$ protocols for other IBE schemes and hierarchical IBE (HIBE) schemes. First, random oracle based IBEs [6,22] appear to be less suited to developing efficient $\mathsf{BlindExtract}$ protocols than their standard model successors. This is in part due to the fact that the identity string is hashed into an element in $\mathbb{G}$ in these schemes, instead of represented as an integer exponent, which makes our proof of knowledge techniques unwieldy. We were not able to find $\mathsf{BlindExtract}$ protocols for the Boneh and Franklin [6], Cocks [22], or the recent Boneh-Gentry-Hamburg [7] IBEs with running time better than $O(|\mathcal{I}|)$, where $\mathcal{I}$ is the identity space. Additionally, we did not consider the efficient IBE of Gentry [27], as our focus was on schemes with *static* complexity assumptions.

We additionally considered hierarchical IBE schemes, such as those due to Boneh and Boyen [3], Waters [44] and Chatterjee and Sarkar [18]. For all of these HIBEs, the number of elements comprising an identity secret key grow with the depth of the hierarchy, but each piece is similar in format to the original keys and our same techniques would apply.

3.3 Additional Properties for a Blind IBE

In §4, we use blind IBE as a tool for constructing oblivious transfer protocols. We can use either of the efficient blind IBEs Π_1 and Π_2 defined above together with the following observations about efficient protocols relating to them.

First, in our OT constructions, we require an efficient zero-knowledge proof of knowledge protocol for the statement $PoK\{(msk) : (params, msk) \in \mathsf{Setup}(1^\kappa, c(\kappa))\}$. If efficiency were not critical, we could accomplish this proof using general techniques [46,28,32]. However, for the parameters used in Π_1, Π_2, this proof can be conducted efficiently in a number of ways; one technique is to set $msk = \alpha$ and conduct the equivalent $PoK\{(\alpha) : g_1 = g^\alpha\}$ using a standard Schnorr proof [42].

The second property that we require is more subtle. Note that in the schemes Π_1 and Π_2, there are many valid decryption keys for each identity. This may lead to a condition where some incorrectly-formed ciphertexts decrypt differently depending on which secret key is used. This can cause problems with the proofs of full-simulation security for our OT protocols (specifically, we may not be able to show Receiver security.) To address this condition in our OT protocols, we require that Π_1 and Π_2 possess a property similar to *committing encryption* [14]. Intuitively, this property ensures that for a ciphertext and identity (C, id): (1) running the honest decryption algorithm on C with respect to any valid secret key for identity id will result in the same unique value, or (2) if this is not so, then this fact can be publicly identified.

Let us define a public *ciphertext validity check* algorithm, which we denote by $\mathsf{IsValid}(params, id, C)$. In the case of blind IBE schemes Π_1 and Π_2, we implement this algorithm by first checking the group parameters γ are valid (see [20]), and verifying that for any *params* and $C = (X, Y, Z)$, all the values are in the correct groups and $e(Y, F(id)) = e(Z, g)$. The *correctness* property for the $\mathsf{IsValid}$ algorithm is that it outputs 1 for all honestly-generated parameters and ciphertexts. From the description of Π_1 and Π_2, it is easy to see that $\mathsf{IsValid}$ is correct. The algorithm's behavior in the case of maliciously-generated input is constrained insofar as it affects the following definition:

Definition 5 (Committing IBE). *An IBE scheme (resp., blind IBE) Π is* committing *if and only if: (1) it is* $\mathsf{IND\text{-}sID\text{-}CPA}$*-secure (resp., secure in the sense of definition 4) and (2) every p.p.t. adversary $\mathcal{A}$ has an advantage negligible in κ for the following game: First, $\mathcal{A}$ outputs $params, id \in \mathcal{I}$ and a ciphertext C. If* $\mathsf{IsValid}(params, id, C) \neq 1$ *then abort. Otherwise, the challenger, on input $(params, id)$, runs the* $\mathsf{Extract}$ *(resp.,* $\mathsf{BlindExtract}$*) protocol with $\mathcal{A}$ twice to obtain purported keys sk_{id}, sk'_{id}. $\mathcal{A}$'s advantage is defined as:*

$$\left|\Pr\left[\mathsf{Decrypt}(params, id, sk_{id}, C) \neq \mathsf{Decrypt}(params, id, sk'_{id}, C)\right]\right|$$

In the full version of this work [30], we prove that both Π_1 and Π_2 are committing blind IBE schemes in the sense of definition 5.

4 Simulatable Oblivious Transfer

We now turn our attention to constructing efficient and fully-simulatable oblivious transfer protocols. We'll use any of the efficient blind IBEs presented in the previous section as a building block. In particular, we focus on building (non-adaptive) OT_k^N and (adaptive) $\mathsf{OT}_{k\times 1}^N$ protocols, in which a Sender and Receiver transfer up to k messages out of an N-message set. In the non-adaptive model [10,35], the Receiver requests all k messages simultaneously. In the adaptive model [36], the Receiver may request the messages one at a time, using the result of previous transfers to inform successive requests. Intuitively, the Receiver should learn only the messages it requests (and nothing about the remaining messages), while the Sender should gain no information about *which* messages the Receiver selected.

Full-simulation vs. half-simulation security. Security for oblivious transfer is defined via simulation. Informally, a protocol is secure if, for every real-world cheating Sender (resp., Receiver) we can describe an ideal-world counterpart who gains as much information from the ideal-world interaction as from the real protocol. Much of the oblivious transfer literature uses the simulation-based definition only to show *Sender* security, choosing to define Receiver security by a simpler game-based definition. Naor and Pinkas demonstrated that this weaker "half-simulation" approach permits *selective-failure* attacks, in which a malicious Sender induces transfer failures that are dependent on the message that the Receiver requests [36]. Recently, Camenisch *et al.* [12] proposed several practical $\mathsf{OT}_{k\times 1}^N$ protocols that are secure under a "full-simulation" definition, using adaptive (*e.g.*, q-PDDH) or interactive (*e.g.*, one-more-inversion RSA) assumptions. We now enhance their results by demonstrating efficient full-simulation OT_k^N and $\mathsf{OT}_{k\times 1}^N$ protocols secure under static complexity assumptions (*e.g.*, DBDH).

4.1 Definitions

Recall the definitions for both the non-adaptive and adaptive protocols. For consistency with earlier work, we use the notation from Camenisch *et al.* [12].

Definition 6 (k-out-of-N Oblivious Transfer (OT_k^N, $\mathsf{OT}_{k\times 1}^N$)). *An oblivious transfer scheme is a tuple of algorithms* $(\mathsf{S_I}, \mathsf{R_I}, \mathsf{S_T}, \mathsf{R_T})$*. During the initialization phase, the Sender and the Receiver run an interactive protocol, where the Sender runs* $\mathsf{S_I}(M_1, \ldots, M_N)$ *to obtain state value* S_0*, and the Receiver runs* $\mathsf{R_I}()$ *to obtain state value* R_0*. Next, during the transfer phase, the Sender and Receiver interactively execute* $\mathsf{S_T}, \mathsf{R_T}$*, respectively,* k *times as described below.*

Adaptive OT. *In the adaptive* $\mathsf{OT}_{k\times 1}^N$ *case, for* $1 \leq i \leq k$*, the* i^{th} *transfer proceeds as follows: the Sender runs* $\mathsf{S_T}(S_{i-1})$ *to obtain state value* S_i*, and the Receiver runs* $\mathsf{R_T}(R_{i-1}, \sigma_i)$ *where* $1 \leq \sigma_i \leq N$ *is the index of the message to be received. This produces state information* R_i *and the message* M'_{σ_i} *or* $\perp$ *indicating failure.*

Non-adaptive OT. *In the non-adaptive* OT_k^N *case the parties execute the protocol as above; however, for round* $i < k$ *the algorithm* $\mathsf{R_T}(R_{i-1}, \sigma_i)$ **does not** *output a message. At the end of the the* k^{th} *transfer* $\mathsf{R_T}(R_{k-1}, \sigma_k)$ *outputs the messages* $(M'_{\sigma_1}, \ldots, M'_{\sigma_k})$ *where for* $j = 1, \ldots, N$ *each* M'_{σ_j} *is a valid message or the symbol* $\perp$ *indicating protocol failure. (In a non-adaptive scheme, the* k *transfers do not necessarily require a corresponding number of communication rounds).*

Definition 7 (Full Simulation Security). *Security for oblivious transfer is defined according to a simulation-based definition.*

Real experiment. *In experiment* $\mathbf{Real}_{\hat{\mathsf{S}},\hat{\mathsf{R}}}(N, k, M_1, \ldots, M_N, \Sigma)$ *the possibly cheating sender* $\hat{\mathsf{S}}$ *is given messages* $(M_1, \ldots, M_N)$ *as input and interacts with possibly cheating receiver* $\hat{\mathsf{R}}(\Sigma)$*, where* Σ *is a selection algorithm that on input messages* $(M_{\sigma_1}, \ldots, M_{\sigma_{i-1}})$ *outputs the index* σ_i *of the next message to be queried. At the beginning of the experiment, both* $\hat{\mathsf{S}}$ *and* $\hat{\mathsf{R}}$ *output initial states* (S_0, R_0)*. In the adaptive case, for* $1 \leq i \leq k$ *the sender computes* $S_i \leftarrow \hat{\mathsf{S}}(S_{i-1})$*, and the receiver computes* $(R_i, M'_i) \leftarrow \hat{\mathsf{R}}(R_{i-1})$*, where* M'_i *may or may not be equal to* M_i*. In the non-adaptive case, the Receiver obtains no messages until the* k^{th} *round, and therefore the selection strategy* Σ *must be non-adaptive. At the end of the* k^{th} *transfer the output of the experiment is* (S_k, R_k)*.*

Ideal experiment. *In experiment* $\mathbf{Ideal}_{\hat{\mathsf{S}}',\hat{\mathsf{R}}'}(N, k, M_1, \ldots, M_N, \Sigma)$ *the possibly cheating sender algorithm* $\hat{\mathsf{S}}'$ *generates messages* $(M_1^*, \ldots, M_N^*)$ *and transmits them to a trusted party* T*. In the* i^{th} *round* $\hat{\mathsf{S}}'$ *sends a bit* b_i *to* T*; the possibly cheating receiver* $\hat{\mathsf{R}}'(\Sigma)$ *transmits* σ_i^* *to* T*. In the adaptive case, if* $b_i = 1$ *and* $\sigma_i^* \in (1, \ldots, N)$ *then* T *hands* $M_{\sigma_i{}^*}$ *to* $\hat{\mathsf{R}}'$*. If* $b_i = 0$ *then* T *hands* $\perp$ *to* $\hat{\mathsf{R}}'$*. Note that in the non-adaptive case,* T *does not give* $\hat{\mathsf{R}}'$ *any response until the* k^{th} *round. At the end of the* k^{th} *transfer the output of the experiment is* (S_k, R_k)*.*

Sender Security. $\mathsf{OT}^N_{k\times 1}$ *provides Sender security if for every real-world p.p.t. receiver* $\hat{\mathsf{R}}$ *there exists a p.p.t. ideal-world receiver* $\hat{\mathsf{R}}'$ *such that* $\forall N = \ell(\kappa)$, $k \in [1, N]$, $(M_1, \ldots, M_N)$, Σ, *and every p.p.t. distinguisher:*
$\mathbf{Real}_{\mathsf{S},\hat{\mathsf{R}}}(N, k, M_1, \ldots, M_N, \Sigma) \overset{c}{\approx} \mathbf{Ideal}_{\mathsf{S}',\hat{\mathsf{R}}'}(N, k, M_1, \ldots, M_N, \Sigma)$.

Receiver Security. $\mathsf{OT}^N_{k\times 1}$ *provides Receiver security if for every real-world p.p.t. sender* $\hat{\mathsf{S}}$ *there exists a p.p.t. ideal-world sender* $\hat{\mathsf{S}}'$ *such that* $\forall N = \ell(\kappa)$, $k \in [1, N]$, $(M_1, \ldots, M_N)$, Σ, *and every p.p.t. distinguisher:*
$\mathbf{Real}_{\hat{\mathsf{S}},\mathsf{R}}(N, k, M_1, \ldots, M_N, \Sigma) \overset{c}{\approx} \mathbf{Ideal}_{\hat{\mathsf{S}}',\mathsf{R}'}(N, k, M_1, \ldots, M_N, \Sigma)$.

4.2 Constructions

Non-adaptive OT^N_k without Random Oracles. Given a committing blind IBE scheme Π, it is tempting to consider the following "intuitive" protocol: First, the Sender runs the IBE Setup algorithm and sends *params* to the Receiver. Next, for $i = 1, \ldots, N$ the Sender transmits an encryption of message M_i under identity "i". To obtain k messages, the Receiver extracts decryption keys for identities $(\sigma_1, \ldots, \sigma_k)$ via k distinct executions of $\mathsf{BlindExtract}$, and uses these keys to decrypt the corresponding ciphertexts. If Π is a blind IBE secure in the sense of definition 4, then a cheating Receiver gains no information about the messages corresponding to secret keys he did not extract. Similarly, with additional precautions, a cheating Sender does not learn the identities extracted. However, it seems difficult to show this protocol is fully-simulatable, because the ideal Sender would have to form the N ciphertexts *before* learning the messages that k of them must decrypt to!

Fortunately, we are able to convert this simple idea into the fully-simulatable OT^N_k protocol shown in Figure 2. We require only the following modifications: first, we have the Sender prove knowledge of the value *msk* using appropriate zero-knowledge techniques.[1] Then, rather than transmitting the ciphertext vector during the first phase of the protocol, the Sender transmits only a *commitment* to a collision-resistant hash of the ciphertext vector, and sends the actual ciphertexts at the end of the k^{th} round together with a proof that she can open the commitment to the hash of the ciphertexts. (She does *not* open the commitment; she only proves that she knows how to do so.)

Theorem 3 (Full-simulation Security of the OT^N_k Scheme). *If blind IBE* $\Pi \in \{\Pi_1, \Pi_2\}$ *with the* $\mathsf{IsValid}$ *as defined in §3.3 and* ($\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Decommit}$) *is a secure commitment scheme, then the* OT^N_k *protocol of figure 2 is sender-secure and receiver-secure in the full-simulation model under DBDH.*

We include a proof of Theorem 3 in the full version [30].

Adaptive $\mathsf{OT}^N_{k\times 1}$ in the Random Oracle Model. While our first protocol is efficient and full-simulation secure, it permits only *non-adaptive* queries. For

[1] In §3.3, we describe how to conduct these proofs efficiently for the practical blind IBE constructions we consider.

$\underline{\mathsf{S_I}(M_1,\ldots,M_N),\mathsf{S_T}()}$	$\underline{\mathsf{R_I}(),\mathsf{R_T}(\sigma_1,\ldots,\sigma_k)}$
Sender and Receiver agree on parameters for a commitment scheme and a collision-resistant hash function H.[a]	
1. Generate $(params, msk) \leftarrow \mathsf{Setup}(1^\kappa, c(\kappa))$.	
2. For $j = 1,\ldots,N$, set $C_j \leftarrow \mathsf{Encrypt}(params, j, M_j)$.	
3. Compute $(\mathcal{C},\mathcal{D}) \leftarrow \mathsf{Commit}\,(H(C_1,\ldots,C_N))$.	
4. Send $(params,\mathcal{C})$ to Receiver.	
5. Conduct $PoK\{(msk) : (params, msk) \in \mathsf{Setup}(1^\kappa, c(\kappa))\}$.	
	6. If the proof does not verify, abort.
For $i = 1, ..., k$, run $\mathsf{BlindExtract}$ on identity σ_i for Receiver to obtain sk_{σ_i}.	
Following the k^{th} extraction:	
1. Send the ciphertexts $(C_1,\ldots,C_N)$ to the Receiver.	
2. Conduct $PoK\{(\mathcal{D}) : \mathsf{Decommit}\,(H(C_1,\ldots,C_N),\mathcal{C},\mathcal{D}) = 1\}$.	
	3. If the proof does not verify, or for any i $\mathsf{IsValid}(params, i, C_i) \neq 1$, abort and set $M'_{\sigma_1},\ldots,M'_{\sigma_k} \leftarrow \perp$.
	4. For $i = 1$ to k: If $\mathsf{BlindExtract}$ on σ_i failed, set $M'_{\sigma_i} \leftarrow \perp$; else, set M'_{σ_i} to the value $\mathsf{Decrypt}(params, \sigma_i, sk_{\sigma_i}, C_{\sigma_i})$.
Output S_k	Output $R_k, (M'_{\sigma_1},\ldots,M'_{\sigma_k})$.

[a] In the case of Pedersen's commitment scheme, the parameters may be generated by the Receiver. H may also be selected by the Receiver.

Fig. 2. OT^N_k from any of the committing blind IBEs in §3, with input messages $M_1,\ldots,M_N \in \mathcal{M}$. We present the $\mathsf{S_I},\mathsf{R_I},\mathsf{S_T},\mathsf{R_T}$ algorithms in a single protocol flow.

many practical applications (*e.g.*, oblivious retrieval from a large database), we desire a protocol that supports an adaptive query pattern. We approach this goal by first proposing an efficient $\mathsf{OT}^N_{k\times 1}$ protocol secure in the random oracle model. The protocol, which we present in Figure 3, requires an IBE scheme with a super-polynomial message space (as in the constructions of §3.1), and has approximately the same efficiency as the construction with random oracles of Camenisch *et al.* [12]. However, their construction requires unique blind signatures and the two known options due to Chaum [19] and Boldyreva [2] both require interactive complexity assumptions. By using the blind IBE schemes in §3.1, our protocols can be based on the DBDH assumption.

Theorem 4 (Full-simulation Security of the $\mathsf{OT}^N_{k\times 1}$ Scheme). *If blind IBE $\Pi \in \{\Pi_1,\Pi_2\}$ with the* $\mathsf{IsValid}$ *as defined in §3.3 and H is modeled as a random*

$\underline{\mathsf{S_I}(M_1, \ldots, M_N)}$	$\underline{\mathsf{R_I}()}$
1. Select $(\mathit{params}, \mathit{msk}) \leftarrow \mathsf{Setup}(1^\kappa, c(\kappa))$. 2. Select random $W_1, \ldots, W_N \in \mathcal{M}$, and for $j = 1, \ldots, N$ set: — $A_j \leftarrow \mathsf{Encrypt}(\mathit{params}, j, W_j)$ — $B_j \leftarrow H(W_j) \oplus M_j$ — $C_j = (A_j, B_j)$ 3. Conduct $PoK\{(\mathit{msk}) : (\mathit{params}, \mathit{msk}) \in \mathsf{Setup}(1^\kappa, c(\kappa))\}$. 4. Send $(\mathit{params}, C_1, \ldots, C_N)$ to Receiver.	
	5. If the proof fails to verify or for any i $\mathsf{IsValid}(\mathit{params}, i, C_i) \neq 1$, abort and set $M'_{\sigma_1}, \ldots, M'_{\sigma_k} \leftarrow \perp$.
Output $S_0 = (\mathit{params}, \mathit{msk})$	Output $R_0 = (\mathit{params}, C_1, \ldots, C_N)$
$\underline{\mathsf{S_T}(S_{i-1})}$	$\underline{\mathsf{R_T}(R_{i-1}, \sigma_i)}$
In the i^{th} transfer, run $\mathsf{BlindExtract}$ on identity σ_i for Receiver to obtain sk_{σ_i}.	
	1. If $\mathsf{BlindExtract}$ fails, then set M'_{σ_i} to $\perp$. 2. Else set $t \leftarrow \mathsf{Decrypt}(\mathit{params}, \sigma_i, sk_{\sigma_i}, A_{\sigma_i})$ and set $M'_{\sigma_i} \leftarrow B_{\sigma_i} \oplus H(t)$.
Output $S_i = S_{i-1}$	Output $R_i = (R_{i-1}, M'_{\sigma_i})$.

Fig. 3. Adaptive $\mathsf{OT}^N_{k\times 1}$ from any of the committing blind IBEs in §3, with $M_1, \ldots, M_N \in \{0,1\}^n$. Let hash $H : \mathcal{M} \rightarrow \{0,1\}^n$ be modeled as a random oracle.

oracle, then the $\mathsf{OT}^N_{k\times 1}$ *protocol of figure 3 is sender-secure and receiver-secure in the full-simulation model under DBDH.*

We include a proof of Theorem 4 in the full version [30].

Adaptive $\mathsf{OT}^N_{k\times 1}$ without Random Oracles. The random-oracle $\mathsf{OT}^N_{k\times 1}$ presented above is reasonably efficient both in terms of communication cost and round-efficiency. Ideally, we would like to construct a protocol of comparable efficiency in the standard model. We could construct an $\mathsf{OT}^N_{k\times 1}$ protocol by compiling k instances of the non-adaptive OT^N_k from §4.2. Each protocol round would consist of a 1-out-of-N instance of the protocol, with new IBE parameters and new a vector of ciphertexts $(C_1, \ldots, C_N)$. To ensure that each round is consistent with the previous rounds, the Sender would need to prove that the underlying plaintexts remain the same from round to round. This can be achieved using standard proof techniques, but is impractical for large values of k or N.

Alternatively, we could combine our scheme with the standard model $\mathsf{OT}^N_{k\times 1}$ of Camenisch *et al.* [12]. Their efficient $\mathsf{OT}^N_{k\times 1}$, for example, incurs only a constant cost per transfer phase. However, the protocol relies on the dynamic q-Strong

DH and q-Power Decisional DH assumptions, where large values of q require larger than normal security parameters [21]. Fortunately, one might be able to keep q small (on the order of k rather than N) by combining the Camenisch *et al.* scheme with ours as follows: in their initialization, the Sender releases N values corresponding to the messages that require $q = N$. Instead, we could use a blind IBE scheme to encrypt these N values during initialization, and then during the adaptive transfer phase, a Receiver could request the decryption key of his choice along with the information required in the Camenisch *et al.* scheme. Thus, reducing the values available to an adversary to $q = k$.

5 Other Applications of Blind IBE

Privacy-preserving delegated keyword search. Several works use IBE as a building-block for *public-key searchable encryption* [5,45]. These schemes permit a keyholder to delegate search capability to other parties. For example, Waters *et al.* [45] describe a searchable encrypted audit log in which a third party auditor is granted the ability to independently search the encrypted log for specific keywords. To enable this function, a central authority generates "trapdoors" for the keywords that the auditor wishes to search on. In this scenario, the trapdoor generation authority necessarily learns each of the search terms. This may be problematic in circumstances where the pattern of trapdoor requests reveals sensitive information (*e.g.*, the name of a user under suspicion). By using blind and partially-blind IBE, we permit the authority to generate trapdoors, yet learn no information (or only partial information) about the search terms.[2]

Blind and partially-blind signature schemes. Moni Naor observed that each adaptive-identity secure IBE implies an existentially unforgeable signature scheme [6]. By the same token, an adaptive-identity secure blind IBE scheme implies an unforgeable, selective-failure blind signature scheme. This result applies to the adaptive-identity secure Π_2 protocol of §3.1, and to the selective-identity secure protocol Π_1 when that scheme is instantiated with appropriately-sized parameters and a hash function (see §7 of [3]). The efficient $\mathsf{BlindExtract}$ protocol for the adaptive-identity secure Π_2 scheme can also be used to construct a *partially-blind* signature, by allowing the signer (the master authority) to supply a portion of the input string. Partially-blind signatures have many applications, such as document timestamping and electronic cash [33].

Temporary anonymous identities. In a typical IBE, the master authority can link users to identities. For some applications, users may wish to remain anonymous or pseudonymous. By employing (partially-)blind IBE, an authority can grant temporary credentials without linking identities to users or even learning which identities are in use.

[2] Boneh *et al.* [5] note that keyword search schemes can be constructed from any *key anonymous* IBE scheme. While the schemes of §3 are not key anonymous, Boyen and Waters remark that key anonymity in similar schemes might be acheived by implementing them in *asymmetric* bilinear groups [9].

Acknowledgments. Thanks to abhi shelat for helpful discussions, and to an anonymous reviewer for pointing out an issue regarding malformed ciphertexts.

References

1. Bellare, M., Micali, S.: Non-interactive oblivious transfer and applications. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 547–557. Springer, Heidelberg (1990)
2. Boldyreva, A.: Threshold, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 31–46. Springer, Heidelberg (2003)
3. Boneh, D., Boyen, X.: Efficient selective-ID secure Identity-Based Encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
4. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 382–400. Springer, Heidelberg (2004)
5. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004)
6. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
7. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: FOCS (to appear, 2007)
8. Boudot, F.: Efficient proofs that a committed number lies in an interval. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 431–444. Springer, Heidelberg (2000)
9. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006)
10. Brassard, G., Crépeau, C., Robert, J.-M.: All-or-nothing disclosure of secrets. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 234–238. Springer, Heidelberg (1987)
11. Camenisch, J., Michels, M.: Proving in zero-knowledge that a number n is the product of two safe primes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 107–122. Springer, Heidelberg (1999)
12. Camenisch, J., Neven, G., shelat, A.: Simulatable adaptive oblivious transfer. In: EUROCRYPT 2007. LNCS, vol. 4515, pp. 573–590. Springer, Heidelberg (2007)
13. Camenisch, J., Stadler, M.: Efficient group signature schemes for large groups. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997)
14. Canetti, R., Feige, U., Goldreich, O., Naor, M.: Adaptively secure multi-party computation. In: Twenty-Eighth Annual ACM Symposium on the Theory of Computing, pp. 639–648 (1996)
15. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from Identity Based Encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004)

16. Chan, A., Frankel, Y., Tsiounis, Y.: Easy come – easy go divisible cash. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 561–575. Springer, Heidelberg (1998)
17. Chatterjee, S., Sarkar, P.: Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 424–440. Springer, Heidelberg (2006)
18. Chatterjee, S., Sarkar, P.: HIBE with Short Public Parameters without Random Oracle. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 145–160. Springer, Heidelberg (2006)
19. Chaum, D.: Blind signatures for untraceable payments. In: CRYPTO 1982, pp. 199–203. Plenum Press (1982)
20. Chen, L., Cheng, Z., Smart, N.: Identity-based key agreement protocols from pairings. International Journal of Information Security 6, 213–241 (2007)
21. Cheon, J.H.: Security analysis of the strong Diffie-Hellman problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1–11. Springer, Heidelberg (2006)
22. Cocks, C.: An identity based encryption scheme based on Quadratic Residues. In: Honary, B. (ed.) Cryptography and Coding. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)
23. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 174–187. Springer, Heidelberg (1994)
24. Ding, Y.Z., Harnik, D., Rosen, A., Shaltiel, R.: Constant-round oblivious transfer in the bounded storage model. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 446–472. Springer, Heidelberg (2004)
25. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. In: CRYPTO 1982, pp. 205–210 (1982)
26. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
27. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
28. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: STOC (1987)
29. Goyal, V.: Reducing trust in the PKG in identity based cryptosystems. In: CRYPTO 2007. LNCS, vol. 4622, pp. 430–447. Springer, Heidelberg (2007)
30. Green, M., Hohenberger, S.: Blind identity-based encryption and simulatable oblivious transfer. Cryptology ePrint Archive, Report 2007/235 (2007)
31. Kalai, Y.T.: Smooth projective hashing and two-message oblivious transfer. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 78–95. Springer, Heidelberg (2005)
32. Kilian, J.: Founding cryptography on oblivious transfer. In: STOC, pp. 20–31 (1988)
33. Miyazaki, S., Sakurai, K.: A more efficient untraceable e-cash system with partially blind signatures based on the discrete logarithm problem. In: Hirschfeld, R. (ed.) FC 1998. LNCS, vol. 1465, pp. 296–308. Springer, Heidelberg (1998)
34. Naccache, D.: Secure and *practical* identity-based encryption. Cryptology ePrint Archive, Report 2005/369 (2005), `http://eprint.iacr.org/`
35. Naor, M., Pinkas, B.: Oblivious transfer and polynomial evaluation. In: STOC 1999, pp. 245–254 (1999)

36. Naor, M., Pinkas, B.: Oblivious transfer with adaptive queries. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 573–590. Springer, Heidelberg (1999)
37. Naor, M., Pinkas, B.: Efficient oblivious transfer protocols. In: SODA 2001, pp. 448–457 (2001)
38. Ogata, W., Kurosawa, K.: Oblivious keyword search. Special issue on coding and cryptography Journal of Complexity 20(2-3), 356–371 (2004)
39. Okamoto, T.: Efficient blind and partially blind signatures without random oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 80–99. Springer, Heidelberg (2006)
40. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
41. Rabin, M.: How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University (1981)
42. Schnorr, C.-P.: Efficient signature generation for smart cards. Journal of Cryptology 4(3), 239–252 (1991)
43. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
44. Waters, B.: Efficient Identity-Based Encryption without random oracles. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
45. Waters, B.R., Balfanz, D., Durfee, G., Smetters, D.K.: Building an encrypted and searchable audit log. In: NDSS 2004 (2004)
46. Yao, A.: How to generate and exchange secrets. In: FOCS, pp. 162–167 (1986)