Homomorphic Encryption with Access Policies: Characterization and New Constructions

Michael Clear*, Arthur Hughes, and Hitesh Tewari

School of Computer Science and Statistics,
Trinity College Dublin

Abstract. A characterization of predicate encryption (PE) with support for homomorphic operations is presented and we describe the homomorphic properties of some existing PE constructions. Even for the special case of IBE, there are few known group-homomorphic cryptosystems. Our main construction is an XOR-homomorphic IBE scheme based on the quadratic residuosity problem (variant of the Cocks' scheme), which we show to be strongly homomorphic. We were unable to construct an anonymous variant that preserves this homomorphic property, but we achieved anonymity for a weaker notion of homomorphic encryption, which we call *non-universal*. A related security notion for this weaker primitive is formalized. Finally, some potential applications and open problems are considered.

1 Introduction

There has been much interest recently in encryption schemes with homomorphic capabilities. Traditionally, malleability was avoided to satisfy strong security definitions, but many applications have been identified for cryptosystems supporting homomorphic operations. More recently, Gentry [1] presented the first fully-homomorphic encryption (FHE) scheme, and several improvements and variants have since appeared in the literature [2–5]. There are however many applications that only require a scheme to support a single homomorphic operation. Such schemes are referred to as *partial homomorphic*. Notable examples of unbounded homomorphic cryptosystems include Goldwasser-Micali [6] (XOR), Paillier [7] and ElGamal [8].

Predicate Encryption (PE) [9] enables a sender to embed a hidden descriptor within a ciphertext that consists of attributes describing the message content. A Trusted Authority (TA) who manages the system issues secret keys to users corresponding to predicates. A user can decrypt a ciphertext containing a descriptor **a** if and only if he/she has a secret key for a predicate that evaluates to true for **a**. This construct turns out to be quite powerful, and generalizes many encryption primitives. It facilitates expressive fine-grained access control i.e. complex policies can be defined restricting the recipients who can decrypt a message. It also facilitates the evaluation of complex queries on data such as

---

range, subset and search queries. Extending the class of supported predicates for known schemes is a topic of active research at present.

PE can be viewed in two ways. It can be viewed as a means to delegate computation to a third party i.e. allow the third party to perform a precise fixed function on the encrypted data, and thus limit what the third party learns about the data. In the spirit of this viewpoint, a generalization known as Functional Encryption has been proposed [10], which allows general functions to be evaluated.

PE can also be viewed as a means to achieve more fine-grained access control. It enables a stronger separation between sender and recipient since the former must only describe the content of the message or more general conditions on its access while decryption then depends on whether a recipient's access policy matches these conditions.

Why consider homomorphic encryption in the PE setting? It is conceivable that in a multi-user environment such as a large organization, certain computations may be delegated to the cloud whose inputs depend on the work of multiple users distributed within that organization. Depending on the application, the circuit to be computed may be chosen or adapted by the cloud provider, and thus is not fixed by the delegator as in primitives such as non-interactive *verifiable computing* [11]. Furthermore, the computation may depend on data sets provided by multiple independent users. Since the data is potentially sensitive, the organization's security policy may dictate that all data must be encrypted. Accordingly, each user encrypts her data with a PE scheme using relevant attributes to describe it. She then sends the ciphertext(s) to the cloud. It is desirable that the results of the computation returned from the cloud be decryptable only by an entity whose access policy (predicate) satisfies the attributes of *all* data sets used in the computation. Of course a public-key homomorphic scheme together with a PE scheme would be sufficient if the senders were able to interact before contacting the cloud, but we would like to remove this requirement since the senders may not be aware of each other. This brings to mind the recent notion of multikey homomorphic encryption presented by López-Alt, Tromer and Vaikuntanathan [12].

Using a multikey homomorphic scheme, the senders need not interact with each other before evaluation takes place on the cloud. Instead, they must run an MPC decryption protocol to jointly decrypt the result produced by the cloud. The evaluated ciphertexts in the scheme described in [12] do not depend on the circuit size, and depend only polynomially on the security parameter and the number of parties who contribute inputs to the circuit. Therefore, the problem outlined above may be solved with a multikey fully homomorphic scheme used in conjunction with a PE scheme if we accept the evaluated ciphertext size to be polynomial in the number of parties. In this work, we are concerned with a ciphertext size that is independent of the number of parties. Naturally, this limits the composition of access policies, but if this is acceptable in an application, there may be efficiency gains over the combination of multikey FHE and PE.

In summary, homomorphic encryption in the PE setting is desirable if there is the possibility of multiple parties in a large organization (say) sending encrypted

data to a semi-trusted[1] evaluator and access policies are required to appropriately limit access to the results, where the "composition" of access policies is "lossy". We assume the semi-honest model in this paper; in particular we do not consider verifiability of the computation.

The state of affairs for homomorphic encryption even for the simplest special case of PE, namely identity-based encryption (IBE), leaves open many challenges. At his talk at Crypto 2010, Naccache [13] mentioned "identity-based fully homomorphic encryption" as one of a list of theory questions. Towards this goal, it has been pointed out in [14] that some LWE-based FHE constructions can be modified to obtain a weak form of an identity-based FHE scheme using the trapdoor functions from [15]; that is, additional information is needed (beyond what can be non-interactively derived from a user's identity) in order to evaluate certain circuits and to perform bootstrapping. Therefore, the valued non-interactivity property of IBE is lost whereby no communication between encryptors and the TA is needed. To the best of our knowledge, fully-homomorphic or even "somewhat-homomorphic" IBE remains open, and a variant of the BGN-type scheme of Gentry, Halevi and Vaikuntanathan [16] is the only IBE scheme that can compactly evaluate quadratic formulae (supports 2-DNF).

As far as the authors are aware, there are no $(\mathbb{Z}_N, +)$ (like Paillier) or $(\mathbb{Z}_p^*, *)$ (like ElGamal) homomorphic IBE schemes. Many pairings-based IBE constructions admit multiplicative homomorphisms which give us a limited additive homomorphism for small ranges; that is, a discrete logarithm problem must be solved to recover the plaintext, and the complexity thereof is $O(\sqrt{M})$, where M is the size of the message space. Of a similar variety are public-key schemes such as BGN [17] and Benaloh [18]. It remains open to construct an unbounded additively homomorphic IBE scheme for a "large" range such as Paillier [7]. Possibly a fruitful step in this direction would be to look at Galbraith's variant of Paillier's cryptosystem based on elliptic curves over rings [19].

One of the contributions of this paper is to construct an additively homomorphic IBE scheme for $\mathbb{Z}_2$, which is usually referred to as XOR-homomorphic. XOR-homomorphic schemes such as Goldwasser-Micali [6] have been used in many practical applications including sealed-bid auctions, biometric authentication and as the building blocks of protocols such as private information retrieval, and it seems that an IBE XOR-homomorphic scheme may be useful in some of these scenarios.

We faced barriers however trying to make our XOR-homomorphic scheme anonymous. The main obstacle is that the homomorphism depends on the public key. We pose as an open problem the task of constructing a variant that achieves anonymity and retains the homomorphic property. Inheriting the terminology of Golle et al. [20] (who refer to re-encryption without the public key as *universal* re-encryption), we designate homomorphic evaluation in a scheme that does not require knowledge of the public key as *universal*. We introduce a weaker primitive that explicitly requires additional information to be passed to the homomorphic evaluation algorithm. Our construction can be made anonymous and retain its

---

[1] We assume all parties are semi-honest.

homomorphic property in this context; that is, if the attribute (identity in the case of IBE) is known to an evaluator. While this certainly is not ideal, it may be plausible in some scenarios that an evaluator is allowed to be privy to the attribute(s) encrypted by the ciphertexts, and it is other parties in the system to whom the attribute(s) must remain concealed. An adversary sees incoming and outgoing ciphertexts, and can potentially request evaluations on arbitrary ciphertexts. We call such a variant *non-universal*. We propose a syntax for a non-universal homomorphic primitive and formulate a security notion to capture attribute-privacy in this context.

1.1   Related Work

There have been several endeavors to characterize homomorphic encryption schemes. Gjøsteen [21] succeeded in characterizing many well-known group homomorphic cryptosystems by means of an abstract construction whose security rests on the hardness of a subgroup membership problem. More recently, Armknecht, Katzenbeisser and Peter [22] gave a more complete characterization and generalized Gjøsteen's results to the IND-CCA1 setting. However, in this work, our focus is at a higher level and not concerned with the underlying algebraic structures. In particular, we do not require the homomorphisms to be unbounded since our aim to provide a more general characterization for homomorphic encryption in the PE setting. Compactness, however, is required; that is, informally, the length of an evaluated ciphertext should be independent of the *size* of the computation.

The notion of receiver-anonymity or key-privacy was formally established by Bellare et al. [23], and the concept of universal anonymity (any user can anonymize a ciphertext) was proposed in [24]. The first universally anonymous IBE scheme appeared in [25]. Prabhakaran and Rosulek [26] consider receiver-anonymity for their definitions of homomorphic encryption.

Finally, since Cocks' IBE scheme [27] appeared, variants have been proposed ([28] and [25]) that achieve anonymity and improve space efficiency. However, the possibility of constructing a homomorphic variant has not received attention to date.

1.2   Organization

Notation and background definitions are set out in Section 2. Our characterization of homomorphic predicate encryption is specified in Section 3; the syntax, correctness conditions and security notions are established, and the properties of such schemes are analyzed. In Section 4, some instantiations are given based on inner-product PE constructions. Our main construction, XOR-homomorphic IBE, is presented in Section 5. Non-universal homomorphic encryption and the abstraction of universal anonymizers is presented in Section 6 towards realizing anonymity for our construction in a weaker setting. Conclusions and future work are presented in Section 7.

2   Preliminaries

A quantity is said to be negligible with respect to some parameter λ, written $\mathsf{negl}(\lambda)$, if it is asymptotically bounded from above by the reciprocal of all polynomials in λ.

For a probability distribution D, we denote by $x \xleftarrow{\$} D$ that x is sampled according to D. If S is a set, $y \xleftarrow{\$} S$ denotes that y is sampled from x according to the uniform distribution on S.

The support of a predicate $f : A \rightarrow \{0, 1\}$ for some domain A is denoted by $\mathsf{supp}(f)$, and is defined by the set $\{a \in A : f(a) = 1\}$.

Definition 1 (Homomorphic Encryption). *A homomorphic encryption scheme with message space M supporting a class of ℓ-input circuits $\mathbb{C} \subseteq M^\ell \rightarrow M$ is a tuple of PPT algorithms* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ *satisfying the property:*
$\forall (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda),\ \forall C \in \mathbb{C}, \forall m_1, \dots, m_\ell \in M$
$\forall c_1, \dots, c_\ell \leftarrow \mathsf{Enc}(\mathsf{pk}, m_1), \dots, \mathsf{Enc}(\mathsf{pk}, m_\ell)$

$$C(m_1, \dots, m_\ell) = \mathsf{Dec}(\mathsf{sk}, \mathsf{Eval}(\mathsf{pk}, C, c_i, \dots, c_\ell))$$

The following definition is based on [29],

Definition 2 (Strongly Homomorphic). *Let $\mathcal{E}$ be a homomorphic encryption scheme with message space M and class of supported circuits $\mathbb{C} \subseteq \{M^\ell \rightarrow M\}$. $\mathcal{E}$ is said to be* strongly homomorphic *iff* $\forall C \in \mathbb{C}$, $\forall (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$, $\forall m_1, \dots, m_\ell$, $\forall c_1, \dots, c_\ell \leftarrow \mathsf{Enc}(\mathsf{pk}, m_1), \dots, \mathsf{Enc}(\mathsf{pk}, m_\ell)$, *the following distributions are statistically indistinguishable*

$$\mathsf{Enc}(\mathsf{pk}, C(m_1, \dots, m_\ell)) \approx (\mathsf{Eval}(\mathsf{pk}, C, c_1, \dots, c_\ell).$$

Definition 3 (Predicate Encryption (Adapted from [9] Definition 1)). *A predicate encryption (PE) scheme for the class of predicates $\mathcal{F}$ over the set of attributes A and with message space M consists of four algorithms* Setup, GenKey, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$ *such that:*

- $\mathsf{PE.Setup}$ *takes as input the security parameter 1^λ and outputs public parameters PP and master secret key MSK.*
- $\mathsf{PE.GenKey}$ *takes as input the master secret key MSK and a description of a predicate $f \in \mathcal{F}$. It outputs a key SK_f.*
- $\mathsf{PE.Encrypt}$ *takes as input the public parameters PP, a message $m \in M$ and an attribute $a \in A$. It returns a ciphertext c. We write this as $c \leftarrow \mathsf{Encrypt}(\mathsf{PP}, a, m)$.*
- $\mathsf{PE.Decrypt}$ *takes as input a secret key SK_f for a predicate f and a ciphertext c. It outputs m iff $f(a) = 1$. Otherwise it outputs a distinguished symbol $\perp$ with all but negligible probability.*

Remark 1. Predicate Encryption (PE) is known by various terms in the literature. PE stems from Attribute-Based Encryption (ABE) with Key Policy, or

simply KP-ABE, and differs from it in its support for attribute privacy. As a result, "ordinary" KP-ABE is sometimes known as PE with public index. Another variant of ABE is CP-ABE (ciphertext policy) where the encryptor embeds her access policy in the ciphertext and a recipient must possess sufficient attributes in order to decrypt. This is the reverse of KP-ABE. In this paper, the emphasis is placed on PE with its more standard interpretation, namely KP-ABE with attribute privacy.

3 Homomorphic Predicate Encryption

3.1 Syntax

Let M be as message space and let A be a set of attributes. Consider a set of operations $\Gamma_M \subseteq \{M^2 \to M\}$ on the message space, and a set of operations $\Gamma_A \subseteq \{A^2 \to A\}$ on the attribute space. We denote by $\gamma = \gamma_A \times \gamma_M$ for some $\gamma_A \in \Gamma_A$ and $\gamma_M \in \Gamma_M$ the operation $(A \times M)^2 \to (A \times M)$ given by $\gamma((a_1, m_1), (a_2, m_2)) = (\gamma_A(a_1, a_2), \gamma_M(m_1, m_2))$. Accordingly, we define the set of permissible "gates" $\Gamma \subseteq \{\gamma_A \times \gamma_M : \gamma_A \in \Gamma_A, \gamma_M \in \Gamma_M\} \subseteq \{(A \times M)^2 \to (A \times M)\}^2$. Thus, each operation on the plaintexts is associated with a single (potentially distinct) operation on the attributes. Finally, we can specify a class of permissible circuits $\mathbb{C}$ built from Γ.

Definition 4. *A homomorphic predicate encryption (HPE) scheme for the non-empty class of predicates $\mathcal{F}$, message space M, attribute space A, and class of ℓ-input circuits $\mathbb{C}$ consists of a tuple of five PPT algorithms* Setup, GenKey, Encrypt, Decrypt *and* Eval. *such that:*

- HPE.Setup, HPE.GenKey, HPE.Encrypt *and* HPE.Decrypt *are as specified in Definition 3.*
- HPE.Eval(PP, $C, c_1, \ldots, c_\ell$) *takes   as   input   the   public   parameters* PP, *an ℓ-input circuit* $C \in \mathbb{C}$, *and ciphertexts* $c_1 \leftarrow$ HPE.Encrypt(PP, a_1, m_1)$, \ldots, c_\ell \leftarrow$ HPE.Encrypt(PP, a_ℓ, m_ℓ).
  It outputs a ciphertext that encrypts the attribute-message pair $C((a_1, m_1), \ldots, (a_\ell, m_\ell))$.

Accordingly, the correctness criteria are defined as follows:

Correctness Conditions
For any (PP, MSK) $\leftarrow$ HPE.Setup(1^λ), $f \in \mathcal{F}$, SK$_f \leftarrow$ HPE.GenKey(PP, MSK, f), $C \in \mathbb{C}$:

1. For any $a \in A, m \in M, c \leftarrow$ HPE.Encrypt(PP, m, a):

$$\text{HPE.Decrypt}(\text{SK}_f, c) = m \iff f(a) = 1$$

---

[2] It is assumed that Γ_A and Γ_M are minimal insofar as $\forall \gamma_A \in \Gamma_A \exists \gamma_M \in \Gamma_M$ s.t. $\gamma_A \times \gamma_M \in \Gamma$ and the converse also holds. In particular, we later assume this of Γ_A.

2. $\forall m_1, \ldots, m_\ell \quad \in \quad M, \quad \forall a_1, \ldots, a_\ell \quad \in \quad A, \quad \forall c_1, \ldots, c_\ell \quad \leftarrow$ HPE.Encrypt$(\mathsf{PP}, a_1, m_1), \ldots,$ HPE.Encrypt$(\mathsf{PP}, a_\ell, m_\ell)$:

   $\forall c' \leftarrow$ HPE.Eval$(\mathsf{PP}, C, c_1, \ldots, c_\ell)$

   (a)
   $$\mathsf{HPE.Decrypt}(\mathsf{SK}_f, c') = m' \iff f(a') = 1$$

   where $(m', a') = C((a_1, m_1), \ldots, (a_\ell, m_\ell))$

   (b)
   $$|c'| < L(\lambda)$$

   where $L(\lambda)$ is a fixed polynomial derivable from PP.

The special case of "predicate only" encryption [9] that excludes plaintexts ("payloads") is modelled by setting $M \triangleq \{\mathbf{0}\}$ for a distinguished symbol $\mathbf{0}$, and setting $\Gamma \triangleq \{\gamma_A \times \mathbf{id_M} : \gamma_A \in \Gamma_A\}$ where $\mathbf{id_M}$ is the identity operation on M.

3.2 Security Notions

The security notions we consider carry over from the standard notions for PE. The basic requirement is IND-CPA security, which is referred to as "payload-hiding". A stronger notion is "attribute-hiding" that additionally entails indistinguishability of attributes. The definitions are game-based with non-adaptive and adaptive variants. The former prescribes that the adversary choose its target attributes at the beginning of the game before seeing the public parameters, whereas the latter allows the adversary's choice to be informed by the public parameters and secret key queries.

Definition 5. *A (H)PE scheme $\mathcal{E}$ is said to be (fully) attribute-hiding (based on Definition 2 in [9]) if an adversary $\mathcal{A}$ has negligible advantage in the following game:*

1. *In the **non-adaptive** variant, $\mathcal{A}$ outputs two attributes a_0 and a_1 at the beginning of the game.*
2. *The challenger $\mathcal{C}$ runs Setup(1^λ) and outputs $(\mathsf{PP}, \mathsf{MSK})$*
3. ***Phase 1***
   $\mathcal{A}$ makes adaptive queries for the secret keys for predicates $f_1, \ldots, f_k \in \mathcal{F}$ subject to the constraint that $f_i(a_0) = f_i(a_1)$ for $1 \le i \le k$.
4. *Remark 2. In the stronger adaptive variant, $\mathcal{A}$ only chooses attributes a_0 and a_1 at this stage.*
5. *$\mathcal{A}$ outputs two messages m_0 and m_1 of equal length. It must hold that $m_0 = m_1$ if there is an i such that $f_i(a_0) = f_i(a_1) = 1$.*
6. *$\mathcal{C}$ chooses a random bit b, and outputs $c \leftarrow$ Encrypt(PP, a_b, m_b)*
7. ***Phase 2***
   A second phase is run where $\mathcal{A}$ requests secret keys for other predicates subject to the same constraint as above.
8. *Finally, $\mathcal{A}$ outputs a guess b' and is said to win if $b' = b$.*

A weaker property referred to as *weakly* attribute-hiding [9] requires that the adversary only request keys for predicates f obeying $f(a_0) = f(a_1) = 0$.

We propose another model of security for non-universal homomorphic encryption in Section 6.

3.3   Attribute Operations

We now characterize HPE schemes based on the properties of their attribute operations (elements of Γ_A).

Definition 6 (Properties of attribute operations). $\forall f \in \mathcal{F}, \quad \forall a_1, a_2 \in A, \quad \forall \gamma_A \in \Gamma_A$:

1.
$$f(\gamma_A(a_1, a_2)) \Rightarrow f(a_1) \wedge f(a_2) \tag{3.1}$$

   (Necessary condition for IND-CPA security)

2.
$$f(\gamma_A(a_1, a_1)) = f(a_1) \tag{3.2}$$

3. $\forall d \in A$:

$$f(a_1) = f(a_2) \Rightarrow f(\gamma_A(d, a_1)) = f(\gamma_A(d, a_2))$$
$$\wedge \ f(\gamma_A(a_1, d)) = f(\gamma_A(a_2, d))$$

$$\tag{3.3}$$

   (Non-monotone Indistinguishability)

4.
$$f(\gamma_A(a_1, a_2)) = f(a_1) \wedge f(a_2) \tag{3.4}$$

   (Monotone Access)

Property 3.1 is a minimal precondition for payload-hiding i.e. IND-CPA security under both adaptive and non-adaptive security definitions.

Property 3.2 preserves access under a homomorphic operation on ciphertexts with the same attribute.

Property 3.3 is a necessary condition for full attribute-hiding.

Property 3.4 enables monotone access; a user only learns a function of a plaintext if and only if that user has permission to learn the value of that plaintext. This implies that (A, γ_A) cannot be a group unless $\mathcal{F}$ is a class of constant predicates. In general, 3.4 implies that $\mathcal{F}$ is monotonic. Monotone access is equivalent to the preceding three properties collectively; that is

$$3.1 \wedge 3.2 \wedge 3.3 \iff 3.4$$

Non-Monotone Access. Non-monotone access is trickier to define and to suitably accommodate in a security definition. It can arise from policies that involve negation. As an example, suppose that it is permissible for a party to decrypt data sets designated as either "geology" or "aviation", but is not authorized to decrypt results with both designations that arise from homomorphic computations on both data sets. Of course it is then necessary to strengthen the restrictions on the adversary's choice of a_0 and a_1 in the security game. Let a_0 and a_1 be the attributes chosen by the adversary. Intuitively, the goal is to show that any sequence of transitions that leads a_0 to a an element outside the support of f, also leads a_1 to an element outside the support of f, and vice versa. Instead of explicitly imposing this non-triviality constraint on the adversary's choice of attributes, one may seek to show that there is no pair of attributes distinguishable under any γ_A and $f \in \mathcal{F}$. This is captured by the property of non-monotone indistinguishability (3.3). Trivially, the constant operations satisfy 3.3. Of more interest is an operation that limits homomorphic operations to ciphertexts with the same attribute. This captures our usual requirements for the (anonymous) IBE functionality, but it is also satisfactory for many applications of general PE where computation need only be performed on ciphertexts with matching attributes. To accomplish this, the attribute space is augmented with a (logical) absorbing element z such that $f(z) = 0 \ \forall f \in \mathcal{F}$. The attribute operation is defined as follows:

$$\delta(a_1, a_2) = \begin{cases} a_1 & \text{if } a_1 = a_2 \\ z & \text{if } a_1 \neq a_2 \end{cases} \tag{3.5}$$

δ models the inability to perform homomorphic evaluations on ciphertexts associated with unequal attributes (identities in the case of IBE). A scheme with this operation can only be fully attribute-hiding in a vacuous sense (it may be such that no restrictions are placed upon the adversary's choice of f but it is unable to find attributes a_0 and a_1 satisfying $f(a_0) = f(a_1) = 1$ for any f.) This is the case for anonymous IBE where the predicates are equality relations, and for the constant map $(a_1, a_2) \mapsto z$ that models the absence of a homomorphic property, although this is preferably modeled by appropriately constraining the class of permissible circuits. More generally, such schemes can only be weakly attribute-hiding because their operations γ_A only satisfy a relaxation of 3.3 given as follows:

Necessary condition for weakly attribute-hiding $\forall a_1, a_2, d \in A$:

$$f(a_1) = f(a_2) = 0 \Rightarrow f(\gamma_A(d, a_1)) = f(\gamma_A(d, a_2))$$
$$\wedge \ f(\gamma_A(a_1, d)) = f(\gamma_A(a_2, d))$$

$$\tag{3.6}$$

Remark 3. In the case of general schemes not satisfying 3.3, placing constraints on the adversary's choice of attributes weakens the security definition. Furthermore, it must be possible for the challenger to efficiently check whether a pair

of attributes satisfies such a condition. Given the added complications, it is tempting to move to a simulation-based definition of security. However, this is precluded by the recent impossibility results of [30] in the case of both weakly and fully attribute-hiding in the NA/AD-SIM models of security. However, for predicate encryption with public index (the attribute is not hidden), this has not been ruled out for 1-AD-SIM and many-NA-SIM where "1" and "many" refer to the number of ciphertexts seen by the adversary. See [30, 31] for more details. In the context of non-monotone access, it thus seems more reasonable to focus on predicate encryption with public index. Our main focus in this work is on schemes that facilitate attribute privacy, and therefore we restrict our attention to schemes that at least satisfy 3.6.

Delegate Predicate Encryption. A primitive presented in [32] called "Delegate Predicate Encryption" (DPE) [3] enables a user to generate an encryption key associated with a chosen attribute $a \in A$, which does not reveal anything about a. The user can distribute this to certain parties who can then encrypt messages with attribute a obliviously. The realization in [32] is similar to the widely-used technique of publishing encryptions of "zero" in a homomorphic cryptosystem, which can then be treated as a key. In fact, this technique is adopted in [33] to transform a strongly homomorphic private-key scheme into a public-key one. Generalizing from the results of [32], this corollary follows from the property of attribute-hiding

Corollary 1. *An attribute-hiding HPE scheme is a DPE as defined in [32] if there exists a $\gamma \in \Gamma$ such that $(A \times M, \gamma)$ is unital.*

4   Constructions with Attribute Aggregation

In this section, we give some meaningful examples of attribute homomorphisms (all which satisfy monotone access) for some known primitives. We begin with a special case of PE introduced by Boneh and Waters [34], which they call *Hidden Vector Encryption*. In this primitive, a ciphertext embeds a vector $\mathbf{w} \in \{0, 1\}^n$ where n is fixed in the public parameters. On the other hand, a secret key corresponds to a vector $\mathbf{v} \in V \triangleq \{*, 0, 1\}^n$ where $*$ is interpreted as a "wildcard" symbol or a "don't care" (it matches any symbol). A decryptor who has a secret key for some $\mathbf{v}$ can check whether it matches the attribute in a ciphertext.

To formulate in terms of PE, let $A = \{0, 1\}^n$ and define

$$\mathcal{F} \subseteq \{(w_1, \ldots, w_n) \mapsto \bigwedge_{i=1}^{n} (v_i = w_i \vee v_i = *) : \mathbf{v} \in V\}$$

Unfortunately, we cannot achieve a non-trivial homomorphic variant of HVE that satisfies 3.4. To see this, consider the HVE class of predicates $\mathcal{F}$ and an

---

[3] Not to be confused with the different notion of Delegatable Predicate Encryption.

operation γ_A satisfying 3.4. For any $\mathbf{x}, \mathbf{y} \in A$, let $\mathbf{z} = \gamma_A(\mathbf{x}, \mathbf{y})$. Now for 3.4 to hold, we must have that $f(\mathbf{z}) = f(\mathbf{x}) \wedge f(\mathbf{y})$ for all $f \in \mathcal{F}$. Suppose $\mathbf{x}_i \neq \mathbf{y}_i$ and $\mathbf{z}_i = \mathbf{x}_i$. Then there exists an $f \in \mathcal{F}$ with $f(\mathbf{z}) = f(\mathbf{x})$ and $f(\mathbf{z}) \neq f(\mathbf{y})$. It is necessary to restrict V. Accordingly, let $V = \{*, 1\}^n$ Setting the non-equal elements to 0 yields associativity and commutativity. Such an operation is equivalent to component-wise logical AND on the attribute vectors, and we will denote it by $\wedge^n$. $(A, \wedge^n)$ is a semilattice.

Recall that a predicate-only scheme does not incorporate a payload into ciphertexts. Even such a scheme $\mathcal{E}$ with the $\wedge^n$ attribute homomorphism might find some purpose in real-world scenarios. One particular application of $\mathcal{E}$ is secure data aggregation in Wireless Sensor Networks (WSNs), an area which has been the target of considerable research (a good survey is [35]). It is conceivable that some aggregator nodes may be authorized by the sink (base station to which packets are forwarded) to read packets matching certain criteria. An origin sensor node produces an outgoing ciphertext as follows: (1). It encrypts the attributes describing its data using $\mathcal{E}$. (2) It encrypts its sensor reading with the public key of the sink using a *separate* additively (say) homomorphic public-key cryptosystem. (3) Both ciphertexts are forwarded to the next hop.

Since an aggregator node receives packets from multiple sources, it needs to have some knowledge about how to aggregate them. To this end, the sink can authorize it to apply a particular predicate to incoming ciphertexts to check for matching candidates for aggregation. One sample policy may be ["REGION1" $\wedge$ "TEMPERATURE"']. It can then aggregate ciphertexts matching this policy. Additional aggregation can be performed by a node further along the route that has been perhaps issued a secret key for a predicate corresponding to the more permissive policy of ["TEMPERATURE"]. In the scenario above, it would be more ideal if $\mathcal{E}$ were also additively homomorphic since besides obviating the need to use another PKE cryptosystem, more control is afforded to aggregators; they receive the ability to decrypt partial sums, and therefore, to perform (more involved) statistical computations on the data.

It is possible to achieve the former case from some recent inner-product PE schemes that admit homomorphisms on both attributes and payload. We focus on two prominent constructions with different mathematical structures. Firstly, a construction is examined by Katz, Sahai and Waters (KSW) [9], which relies on non-standard assumptions on bilinear groups, assumptions that are justified by the authors in the generic group model. Secondly, we focus on a construction presented by Agrawal, Freeman and Vaikuntanathan (AFV) [36] whose security is based on the learning with errors (LWE) problem.

In both schemes, an attribute is an element of $\mathbb{Z}_m^n$ [4] and a predicate also corresponds to an element of $\mathbb{Z}_m^n$. For $\mathbf{v} \in \mathbb{Z}_m^n$, a predicate $f_{\mathbf{v}} : \mathbb{Z}_m^n \to \{0, 1\}$ is

---

[4] In [9], m is a product of three large primes and n is the security parameter. In [36], n is independent of the security parameter and m may be polynomial or superpolynomial in the security parameter; in the latter case m is the product of many "small" primes. We require that m be superpolynomial here.

defined by

$$f_{\mathbf{v}}(\mathbf{w}) = \begin{cases} 1 & \text{iff } \langle \mathbf{v}, \mathbf{w} \rangle \\ 0 & \text{otherwise} \end{cases}$$

Roughly speaking, in a ciphertext, all sub-attributes (in $\mathbb{Z}_m$) are blinded by the same uniformly random "blinding" element b [5]. The decryption algorithm multiplies each component by the corresponding component in the predicate vector, and the blinding element b is eliminated when the inner product evaluates to zero with all but negligible probability, which allows decryption to proceed.

Let $\mathbf{c_1}$ and $\mathbf{c_2}$ be ciphertexts that encrypt attributes a_1 and a_2 respectively. It can be easily shown that the sum $\mathbf{c'} = \mathbf{c_1} \boxplus^6 \mathbf{c_2}$ encrypts both a_1 and a_2 in a somewhat "isolated" way. The lossiness is "hidden" by the negligible probability of two non-zero inner-products summing to 0. For linear aggregation, this can be repeated a polynomial number of times (or effectively unbounded in practice) while ensuring correctness with overwhelming probability. While linear aggregation is sufficient for the WSN scenario, it is interesting to explore other circuit forms. For the KSW scheme, we observe that all circuits of polynomial depth can be evaluated with overwhelming probability. For AFV, the picture is somewhat similar to the fully homomorphic schemes based on LWE such as [4,5] but without requiring multiplicative gates.

While there are motivating scenarios for aggregation on the attributes, in many cases it is adequate or preferable to restrict evaluation to ciphertexts with matching attributes; that is, by means of the δ operation defined in Section 3.3. Among these cases is anonymous IBE. In the next section, we introduce an IBE construction that supports an unbounded XOR homomorphism, prove that it is strongly homomorphic and then investigate anonymous variants.

5   Main Construction: XOR-Homomorphic IBE

In this section, an XOR-homomorphic IBE scheme is presented whose security is based on the quadratic residuosity assumption. Therefore, it is similar in many respects to the Goldwasser-Micali (GM) cryptosystem [6], which is well-known to be XOR-homomorphic. Indeed, the GM scheme has found many practical applications due to its homomorphic property. In Section 6.3, we show how many of these applications benefit from an XOR-homomorphic scheme in the identity-based setting.

Our construction derives from the IBE scheme due to Cocks [27] which has a security reduction to the quadratic residuosity problem. To the best of our knowledge, a homomorphic variant has not been explored to date.

5.1   Background

Let m be an integer. A quadratic residue in the residue ring $\mathbb{Z}_m$ is an integer x such that $x \equiv y^2 \mod m$ for some $y \in \mathbb{Z}_m$. The set of quadratic residues in $\mathbb{Z}_m$

---

[5] a scalar in KSW and a matrix in AFV.

[6] $\boxplus$ denotes a pairwise sum of the ciphertext components in both schemes.

is denoted $\mathbb{QR}(m)$. If m is prime, it easy to determine whether any $x \in \mathbb{Z}_m$ is a quadratic residue.

Let $N = pq$ be a composite modulus where p and q are prime. Let $x \in \mathbb{Z}$. We write $\left(\dfrac{x}{N}\right)$ to denote the Jacobi symbol of $x \mod N$. The subset of integers with Jacobi symbol +1 (resp. -1) is denoted $\mathbb{Z}_N[+1]$ (resp. $\mathbb{Z}_N[-1]$). The quadratic residuosity problem is to determine, given input $(N, x \in \mathbb{Z}_N[+1])$, whether $x \in \mathbb{QR}(N)$, and it is believed to be intractable.

Define the encoding $\nu : \{0,1\} \to \{-1,1\}$ with $\nu(0) = 1$ and $\nu(1) = -1$. Formally, ν is a group isomorphism between $(\mathbb{Z}_2, +)$ and $(\{-1,1\}, *)$.

In this section, we build on the results of [25] and therefore attempt to maintain consistency with their notation where possible. As in [25], we let $H : \{0,1\}^* \to \mathbb{Z}_N^*[+1]$ be a full-domain hash. A message bit is mapped to an element of $\{-1,1\}$ via ν as defined earlier (0 (1 resp.) is encoded as 1 (-1 resp.)).

5.2   Original Cocks IBE Scheme

- CocksIBE.**Setup**(1^λ):
    1. Repeat: $p, q \xleftarrow{\$} \mathsf{RandPrime}(1^\lambda)$ Until: $p \equiv q \equiv 3 \pmod 4$
    2. $N \leftarrow pq$
    3. Output $(\mathsf{PP} := N, \mathsf{MSK} := (p,q))$
- CocksIBE.**KeyGen**$(\mathsf{PP}, \mathsf{MSK}, \mathsf{id})$:
    1. Parse MSK as (p,q).
    2. $a \leftarrow H(\mathsf{id})$
    3. $r \leftarrow a^{\frac{N+5-p-q}{8}} \pmod N$
       $(\therefore r^2 \equiv a \pmod N$ or $r^2 \equiv -a \pmod N)$
    4. Output $\mathsf{sk_{id}} := (\mathsf{id}, r)$
- CocksIBE.**Encrypt**$(\mathsf{PP}, \mathsf{id}, b)$:
    1. $a \leftarrow H(\mathsf{id})$
    2. $t_1, t_2 \xleftarrow{\$} \mathbb{Z}_N^*[\nu(b)]$
    3. Output $\psi := (t_1 + at_1^{-1}, t_2 - at_2^{-1})$
- CocksIBE.**Decrypt**$(\mathsf{PP}, \mathsf{sk_{id}}, \psi)$:
    1. Parse ψ as (ψ_1, ψ_2)
    2. Parse $\mathsf{sk_{id}}$ as (id, r)
    3. $a \leftarrow H(\mathsf{id})$
    4. If $r^2 \equiv a \pmod N$, set $d \leftarrow \psi_1$. Else if $r^2 \equiv -a \pmod N$, set $d \leftarrow \psi_2$. Else output $\perp$ and abort.
    5. Output $\nu^{-1}(\left(\dfrac{d+2r}{N}\right))$

The above scheme can be shown to be adaptively secure in the random oracle model assuming the hardness of the quadratic residuosity problem.

Anonymity. Cocks' scheme is not anonymous. Boneh et al. [37] report a test due to Galbraith that enables an attacker to distinguish the identity of a ciphertext. This is achieved with overwhelming probability given multiple ciphertexts. It is shown by Ateniese and Gasti [25] that there is no "better" test for attacking anonymity. Briefly, let $a = H(\mathsf{id})$ be the public key derived from the identity $\mathsf{ID_a}$. Let c be a ciphertext in the Cocks' scheme. Galbraith's test is defined as

$$\mathsf{GT}(a, c, N) = \left(\frac{c^2 - 4a}{N} \right)$$

Now if c is a ciphertext encrypted with a, then $\mathsf{GT}(a, c, N) = +1$ with all but negligible probability. For $b \in \mathbb{Z}_N^*$ such that $b \neq a$, the value $\mathsf{GT}(b, c, N)$ is statistically close to the uniform distribution on $\{-1, 1\}$. Therefore, given multiple ciphertexts, it can be determined with overwhelming probability whether they correspond to a particular identity.

5.3   XOR-Homomorphic Construction

Recall that a ciphertext in the Cocks scheme consists of two elements in $\mathbb{Z}_N$. Thus, we have

$$(c, d) \leftarrow \mathsf{CocksIBE.Encrypt(PP, id}, b) \in \mathbb{Z}_N^2$$

for some identity id and bit $b \in \{0, 1\}$. Also recall that only one element is actually used for decryption depending on whether $a := H(\mathsf{id}) \in \mathbb{QR}(N)$ or $-a \in \mathbb{QR}(N)$. If the former holds, it follows that a decryptor has a secret key r satisfying $r^2 \equiv a \pmod{N}$. Otherwise, a secret key r satisfies $r^2 \equiv -a \pmod{N}$. To simplify the description of the homomorphic property, we will assume that $a \in \mathbb{QR}(N)$ and therefore omit the second "component" d from the ciphertext. In fact, the properties hold analogously for the second "component" by simply replacing a with $-a$.

   In the homomorphic scheme, each "component" of the ciphertext is represented by a pair of elements in $\mathbb{Z}_N^2$ instead of a single element as in the original Cocks scheme. As mentioned, we will omit the second such pair for the moment. Consider the following encryption algorithm E_a defined by

$\mathsf{E_a}(b : \{0, 1\}):$
   $t \xleftarrow{\$} \mathbb{Z}_N^*[\nu(b)]$
   return $(t + at^{-1}, 2) \in \mathbb{Z}_N^2.$

Furthermore, define the decryption function $D_a(\mathbf{c}) = \nu^{-1}(c_0 + rc_1)$. The homomorphic operation $\boxplus : \mathbb{Z}_N^2 \times \mathbb{Z}_N^2 \to \mathbb{Z}_N^2$ is defined as follows:

$$\mathbf{c} \boxplus \mathbf{d} = (c_0 d_0 + a c_1 d_1, c_0 d_1 + c_1 d_0) \tag{5.1}$$

It is easy to see that $D_a(\mathbf{c} \boxplus \mathbf{d}) = D_a(\mathbf{c}) \oplus D_a(\mathbf{d})$:

$$
\begin{aligned}
D_a(\mathbf{c} \boxplus \mathbf{d}) &= D_a((c_0d_0 + ac_1d_1, c_0d_1 + c_1d_0)) \\
&= \nu^{-1}((c_0d_0 + ac_1d_1) + r(c_0d_1 + c_1d_0)) \\
&= \nu^{-1}(c_0d_0 + rc_0d_1 + rc_1d_0 + r^2c_1d_1) \\
&= \nu^{-1}((c_0 + rc_1)(d_0 + rd_1)) \\
&= \nu^{-1}(c_0 + rc_1) \oplus \nu^{-1}(d_0 + rd_1) \\
&= D_a(\mathbf{c}) \oplus D_a(\mathbf{d}) \qquad\qquad\qquad\qquad (5.2)
\end{aligned}
$$

Let $R_a = \mathbb{Z}_N[x]/(x^2 - a)$ be a quotient of the polynomial ring $R = \mathbb{Z}_N[x]$. It is more natural and convenient to view ciphertexts as elements of R_a and the homomorphic operation as multiplication in R_a. Furthermore, decryption equates to evaluation at the point r. Thus the homomorphic evaluation of two ciphertext polynomials $c(x)$ and $d(x)$ is simply $e(x) = c(x) * d(x)$ where $*$ denotes multiplication in R_a. Decryption becomes $\nu^{-1}(e(r))$. Moreover, Galbraith's test is generalized straightforwardly to the ring R_a:

$$
\mathsf{GT}(a, c(x)) = \left(\frac{c_0^2 - c_1^2 a}{N} \right).
$$

We now formally describe our variant of the Cocks scheme that supports an XOR homomorphism.

Remark 4. We have presented the scheme in accordance with Definition 4 for consistency with the rest of the paper. Therefore, it uses the circuit formulation, which we would typically consider superfluous for a group homomorphic scheme.

Let $\mathbb{C} \triangleq \{\mathbf{x} \mapsto \langle \mathbf{t}, \mathbf{x} \rangle : \mathbf{t} \in \mathbb{Z}_2^\ell\} \subset \mathbb{Z}_2^\ell \to \mathbb{Z}_2$ be the class of arithmetic circuits characterized by linear functions over $\mathbb{Z}_2$ in ℓ variables. As such, we associate a representative vector $V(C) \in \mathbb{Z}_2^\ell$ to every circuit $C \in \mathbb{C}$. In order to obtain a strongly homomorphic scheme, we use the standard technique of re-randomizing the evaluated ciphertext by homomorphically adding an encryption of zero.

- xhIBE.**Encrypt**$(\mathsf{PP}, \mathsf{id}, b)$:
    1. $a \leftarrow H(\mathsf{id})$
    2. As a subroutine (used later), define
       $E(\mathsf{PP}, a, b)$:
       (a) $t_1, t_2 \xleftarrow{\$} \mathbb{Z}_N^*[\nu(b)]$
       (b) $g_1, g_2 \xleftarrow{\$} \mathbb{Z}_N^*$
       (c) $c(x) \leftarrow (t_1 + ag_1^2t_1^{-1}) + 2g_1x \in \mathbb{Z}_N[x]$
       (d) $d(x) \leftarrow (t_2 + ag_2^2t_2^{-1}) + 2g_2x \in \mathbb{Z}_N[x]$
       (e) Repeat steps (a) - (d) until $\mathsf{GT}(a, c(x)) = 1$ and $\mathsf{GT}(-a, d(x)) = 1$.
       (f) Output $(c(x), d(x))$
    3. Output $\psi := (E(\mathsf{PP}, a, b), a)$
- xhIBE.**Decrypt**$(\mathsf{PP}, \mathsf{sk}_{\mathsf{id}}, \psi)$:
    1. Parse ψ as $(c(x), d(x), a)$

2. Parse $\mathsf{sk_{id}}$ as (id, r)
3. If $r^2 \equiv a \pmod{N}$ and $\mathsf{GT}(a, c(x)) = 1$, set $e(x) \leftarrow c(x)$. Else if $r^2 \equiv -a$ $\pmod{N}$ and $\mathsf{GT}(-a, c(x)) = 1$, set $e(x) \leftarrow d(x)$. Else output $\bot$ and abort.
4. Output $\nu^{-1}(\left(\dfrac{e(r)}{N}\right))$

$\mathsf{xhIBE.Eval}(\mathsf{PP}, C, \psi_1, \ldots, \psi_\ell)$:
1. Parse ψ_i as $(c_i(x), d_i(x), a_i)$ for $1 \le i \le \ell$
2. If $a_i \ne a_j$ for $1 \le i, j \le \ell$, abort with $\bot$.
3. Let $a = a_1$ and let $R_a = \mathbb{Z}_N[x]/(x^2 - a)$
4. $v \leftarrow V(C)$
5. $J \leftarrow \{1 \le i \le \ell : v_i = 1\}$
6. $(c'(x), d'(x)) \leftarrow (\prod_{i \in J} c_i(x) \mod (x^2 - a), \prod_{i \in I} d_i(x)) \mod (x^2 + a)$
7. $(c_z(x), d_z(x)) \leftarrow E(\mathsf{PP}, a, 0)$ (E is defined as a subroutine in the specification of $\mathsf{xhIBE.Encrypt}$)
8. Output $(c'(x) * c_z(x) \mod (x^2 - a), d'(x) * d_z(x) \mod (x^2 + a), a)$.

We now prove that our scheme is group homomorphic and strongly homomorphic. A formalization of group homomorphic public-key schemes is given in [38]. Our adapted definition for the PE setting raises some subtle points. The third requirement in [38] is more difficult to formalize for general PE; we omit it from the definition here and leave a complete formalization to the full version [7]. We remark that this property which relates to distinguishing "illegitimate ciphertexts" during decryption is not necessary to achieve IND-ID-CPA security.

Definition 7 (Adapted from Definition 1 in [38]). *Let $\mathcal{E} = (G, K, E, D)$ be a PE scheme with message space M, attribute space A, ciphertext space $\hat{\mathcal{C}}$ and class of predicates $\mathcal{F}$. The scheme $\mathcal{E}$ is group homomorphic with respect to a non-empty set of attributes $A' \subseteq A$ if for every $(\mathsf{PP}, \mathsf{MSK}) \leftarrow G(1^\lambda)$, every $f \in \mathcal{F} : A' \subseteq \mathsf{supp}(f)$, and every $\mathsf{sk}_f \leftarrow K(\mathsf{MSK}, f)$, the message space $(M, \cdot)$ is a non-trivial group, and there is a binary operation $\Box : \hat{\mathcal{C}}^2 \to \hat{\mathcal{C}}$ such that the following properties are satisfied for the restricted ciphertext space $\hat{\mathcal{C}}_f = \{c \in \hat{\mathcal{C}} : D_{\mathsf{sk}_f}(c) \ne \bot\}$:*

1. *The set of all encryptions $\mathcal{C} := \{c \in \hat{\mathcal{C}}_f \mid c \leftarrow E(\mathsf{PP}, a, m), a \in A', m \in M\}$ under attributes in A' is a non-trivial group under the operation $\Box$.*
2. *The restricted decryption $D^*_{\mathsf{sk}_f} := D_{\mathsf{sk}_f|\mathcal{C}}$ is surjective and $\forall c, c' \in \mathcal{C} \quad D_{\mathsf{sk}_f}(c \Box c') = D_{\mathsf{sk}_f}(c) \cdot D_{\mathsf{sk}_f}(c')$.*
3. ***IBE only (generalized in the full version)** If $\mathcal{E}$ is an IBE scheme, then $\hat{\mathcal{C}}_f$ is also required to be a group, and it is required to be computationally indistinguishable from $\mathcal{C}$; that is:*

$$\{(\mathsf{PP}, f, \mathsf{sk}_f, S, c) \mid c \xleftarrow{\$} \mathcal{C}, S \subset \{\mathsf{sk}_g \leftarrow K(g) : g \in \mathcal{F}\}\}$$
$$\underset{C}{\approx} \{(\mathsf{PP}, f, \mathsf{sk}_f, S, \hat{c}) \mid \hat{c} \xleftarrow{\$} \hat{\mathcal{C}}_f, S \subset \{\mathsf{sk}_g \leftarrow K(g) : g \in \mathcal{F}\}\}.$$

---

[7] Available at `http://arxiv.org/abs/1302.1192`.

Informally, the above definition is telling us that for a given subset of attributes A' satisfying a predicate f, the set of honestly generated encryptions under these attributes forms a group that is epimorphic to the plaintext group. It does not say anything about ciphertexts that are not honestly generated except in the case of IBE, where we require that all ciphertexts that do not decrypt to $\bot$ under a secret key are indistinguishable.

For the remainder of this section, we show that xhIBE fulfills the definition of a group homomorphic scheme, and that it is IND-ID-CPA secure under the quadratic residuosity assumption in the random oracle model. To simplify the presentation of the proofs, additional notation is needed. In particular, we inherit the notation from [25], and generalize it to the ring R_a.

Define the subset $G_a \subset R_a$ as follows:

$$G_a = \{c(x) \in R_a : \mathsf{GT}(a, c(x)) = 1\}$$

Define the subset $S_a \subset G_a{}^8$:

$$S_a = \{2hx + (t + ah^2t^{-1}) \in G_a \mid h, t, (t + ah^2t^{-1}) \in \mathbb{Z}_N^*\}$$

We have the following simple lemma:

Lemma 1.

1. $(G_a, *)$ is a multiplicative subgroup of R_a.
2. $(S_a, *)$ is a subgroup of G_a

Proof. We must show that G_a is closed under $*$. Let $c(x), d(x) \in G_a$, and let $e(x) = c(x) * d(x)$.

$$
\begin{aligned}
\mathsf{GT}(a, e(x)) &= \left(\frac{e_0^2 - ae_1^2}{N} \right) \\
&= \left(\frac{(c_0d_0 + ac_1d_1)^2 - a(c_0d_1 + c_1d_0)^2}{N} \right) \\
&= \left(\frac{(c_0^2 - ac_1^2)(d_0^2 - ad_1^2)}{N} \right) \\
&= \left(\frac{(c_0^2 - ac_1^2)}{N} \right) \left(\frac{(d_0^2 - ad_1^2)}{N} \right) \\
&= \mathsf{GT}(a, c(x)) \cdot \mathsf{GT}(a, d(x)) \\
&= 1
\end{aligned}
$$

Therefore, $e(x) \in G_a$.

It remains to show that every element of G_a is a unit. Let $z = c_0^2 - ac_1^2 \in \mathbb{Z}_N$. An inverse $d_1x + d_0$ of $c(x)$ can be computed by setting $d_0 = \frac{c_0}{z}$ and $d_1 = \frac{-c_1}{z}$ if it holds that z is invertible in $\mathbb{Z}_N$. Indeed such a $d_1x + d_0$ is in G_a. Now if z

---

[8] This definition is stricter than its analog in [25] in that all elements are in G_a.

is not invertible in $\mathbb{Z}_N$ then $p|z$ or $q|z$, which implies that $\left(\dfrac{z}{p}\right) = 0$ or $\left(\dfrac{z}{q}\right) = 0$. But $\mathsf{GT}(a, c(x)) = \left(\dfrac{z}{N}\right) = \left(\dfrac{z}{p}\right)\left(\dfrac{z}{q}\right) = 1$ since $c(x) \in G_a$. Therefore, z is a unit in $\mathbb{Z}_N$, and $c(x)$ is a unit in G_a.

Finally, to prove (2), note that the members of S_a are exactly the elements $c(x)$ such that $c_0^2 - c_1^2 a$ is a square, and it is easy to see that this is preserved under $*$ in R_a. $\qquad \square$

We will also need the following corollary

Corollary 2 (Extension of Lemma 2.2 in [25]). *The distributions* $\{(N, a, t + ah^2t^{-1}, 2h) : N \leftarrow \mathsf{Setup}(1^\lambda), a \xleftarrow{\$} \mathbb{Z}_N^*[+1], t, h \xleftarrow{\$} \mathbb{Z}_N^*)\}$ *and* $\{(N, a, z_0, z_1) : N \leftarrow \mathsf{Setup}(1^\lambda), a \xleftarrow{\$} \mathbb{Z}_N^*[+1], z_0 + z_1 x \xleftarrow{\$} G_a \backslash S_a\}$ *are indistinguishable assuming the hardness of the quadratic residuosity problem.*

Proof. The corollary follows immediately from Lemma 2.2 in [25] Let $\mathcal{A}$ be an efficient adversary that distinguishes both distributions. Lemma 2.2 in [25] shows that the distributions $d_0 := (\{(N, a, t + at^{-1}) : N \leftarrow \mathsf{Setup}(1^\lambda), a \xleftarrow{\$} \mathbb{Z}_N^*[+1], t\}$ and $d_1 := \{(N, a, z_0) : N \leftarrow \mathsf{Setup}(1^\lambda), a \xleftarrow{\$} \mathbb{Z}_N^*[+1], z_1 x + z_0 \xleftarrow{\$} G_a \backslash S_a \mid z_2 = 2\}$ are indistinguishable. Given a sample (N, a, c), the simulator generates $h \xleftarrow{\$} \mathbb{Z}_N^*$ and computes $b := h^{-2}a$. It passes the element $(N, b, c, 2h)$ to $\mathcal{A}$. The simulator aborts with the output of $\mathcal{A}$. $\qquad \square$

Theorem 1. xhIBE *is a group homomorphic scheme with respect to the group operation of* $(\mathbb{Z}_2, +)$.

Proof. Let $a = H(\mathsf{id})$ for any valid identity string id. Assume that the secret key r satisfies $r^2 \equiv a \mod N$. The analysis holds analogously if $r^2 \equiv -a \mod N$; therefore, we omit the second component of the ciphertexts for simplicity.

By definition, $S_a = \{c(x) \in R_a \mid \psi := (c(x), d(x), a) \leftarrow \mathsf{xhIBE.Encrypt}(\mathsf{PP}, \mathsf{id}, m), m \in M\}$. By corollary 2, it holds that $S_a \underset{C}{\approx} G_a$ without the master secret key. The decryption algorithm only outputs $\bot$ on input $\psi := (c(x), d(x), a)$ if $c(x) \notin G_a$ or $d(x) \notin G_{-a}$. Thus, omitting the second component, we have that S_a corresponds to $\mathcal{C}$ and G_a corresponds to $\hat{\mathcal{C}}_f$ in Definition 7 (in this case f is defined as $f(\mathsf{id}') = 1$ iff $\mathsf{id}' = \mathsf{id}$). It follows that the third requirement of Definition 7 is satisfied.

By Lemma 1, G_a is a group and S_a is a non-trivial subgroup of G_a. The surjective homomorphism between $\mathcal{C} := S_a$ and $M := \mathbb{Z}_2^*$ has already been shown in the correctness derivation in equation 5.2. This completes the proof. $\qquad \square$

Remark 5. It is straightforward to show that xhIBE also meets the criteria for a shift-type homomorphism as defined in [38].

Corollary 3. xhIBE *is strongly homomorphic.*

Proof. Any group homomorphic scheme can be turned into a strongly homomorphic scheme by rerandomizing an evaluated ciphertext. Indeed this follows from Lemma 1 in [38]. Rerandomization is achieved by multiplying the evaluated ciphertext by an encryption of the identity, as in xhIBE.Eval. Details follow for completeness.

Let id be an identity and let $a = H(\text{id})$. For any circuit $C \in \mathbb{C}$, any messages $b_1, \ldots, b_\ell$ and ciphertexts $\psi_\mathbf{1}, \ldots, \psi_\ell \leftarrow$ xhIBE.Encrypt$(\text{PP}, b_1, \text{id}), \ldots,$ xhIBE.Encrypt$(\text{PP}, b_\ell, \text{id})$, we have

$$(c'(x), d'(x), a) \leftarrow \text{xhIBE.}\mathbf{Eval}(\text{PP}, C, \psi_\mathbf{1}, \ldots, \psi_\ell).$$

From the last step of xhIBE.Eval, we see that $c'(x) \leftarrow c''(x) * r(x)$ where $r(x) \xleftarrow{\$} S_a^{(0)}$ and $c''(x)$ is the result of the homomorphic evaluation. Suppose that $c''(x)$ encrypts a bit b. Since S_a is a group, it follows that $c'(x)$ is uniformly distributed in the coset $S_a^{(b)}$ (of the subgroup $S_a^{(0)}$) and is thus distributed according to a "fresh" encryption of b. □

Theorem 2. xhIBE *is IND-ID-CPA secure in the random oracle model under the quadratic residuosity assumption.*

Proof. Let $\mathcal{A}$ be an adversary that breaks the IND-ID-CPA security of xhIBE. We use $\mathcal{A}$ to construct an algorithm $\mathcal{S}$ to break the IND-ID-CPA security of the Cocks scheme with the same advantage. $\mathcal{S}$ proceeds as follows:

1. Uniformly sample an element $h \xleftarrow{\$} \mathbb{Z}_N^*$. Receive the public parameters PP from the challenger $\mathcal{C}$ and pass them to $\mathcal{A}$.
2. $\mathcal{S}$ answers a query to H for identity id with $H'(\text{id}) \cdot h^{-2}$ where H' is $\mathcal{S}$'s random oracle. The responses are uniformly distributed in $\mathbb{Z}_N[+1]$.
3. $\mathcal{S}$ answers a key generation query for id with the response $K(\text{id}) \cdot h^{-1}$ where K is its key generation oracle.
4. When $\mathcal{A}$ chooses target identity id^*, $\mathcal{S}$ relays id^* to $\mathcal{C}$. Assume w.l.o.g that H has been queried for id, and that $\mathcal{A}$ has not made a secret key query for id^*. Further key generation requests are handled subject to the condition that $\text{id} \neq \text{id}^*$ for a requested identity id.
5. Let $a = H(\text{id}^*)$. On receiving a challenge ciphertext (c, d) from $\mathcal{C}$, compute $c(x) \leftarrow 2hx + c \in R$ and $d(x) \leftarrow (2hx + d) * r(x) \in R$ where $r(x) \xleftarrow{\$} S_{-a}^{(0)}$ and $S_{-a}^{(0)}$ is the second component of the set of legal encryptions of 0. From corollary 3, $d(x)$ is uniformly distributed in $S_{-a}^{(b)}$ where the ciphertext (c, d) in the Cocks scheme encrypts the bit b. It follows that $(c(x), d(x))$ is a perfectly simulated encryption of b under identity id^* in xhIBE. Give $(c(x), d(x))$ to $\mathcal{A}$.
6. Output $\mathcal{A}$'s guess b'.

Since the view of $\mathcal{A}$ in an interaction with $\mathcal{S}$ is indistinguishable from its view in the real game, we conclude that the advantage of $\mathcal{S}$ is equal to the advantage of $\mathcal{A}$.

□

In the next section, attention is drawn to obtaining an anonymous variant of our construction.

6 Anonymity

Cocks' scheme is notable as one of the few IBE schemes that do not rely on pairings. Since it appeared, there have been efforts to reduce its ciphertext size and make it anonymous. Boneh, Gentry and Hamburg [28] proposed a scheme with some elegant ideas that achieves both anonymity and a much reduced ciphertext size for multi-bit messages at the expense of performance, which is $O(n^4)$ for encryption and $O(n^3)$ for decryption (where n is the security parameter). Unfortunately the homomorphic property is lost in this construction.

As mentioned earlier (cf. Section 5.2), another approach due to Ateniese and Gasti [25] achieves anonymity and preserves performance, but its per-bit ciphertext expansion is much higher than in [28]. However, an advantage of this scheme is that it is universally anonymous (anyone can anonymize the message, not merely the encryptor [24]).

On the downside, anonymizing according to this scheme breaks the homomorphic property of our construction, which depends crucially on the public key a. More precisely, what is forfeited is the *universal homomorphic* property mentioned in the introduction (i.e. anyone can evaluate on the ciphertexts without additional information). There are applications where an evaluator is aware of the attribute(s) associated with ciphertexts, but anonymity is desirable to prevent any other parties in the system learning about such attributes. This motivates a variant of HPE, which we call non-universal HPE, denoted by $\mathsf{HPE}_{\bar{U}}$.

6.1 Non-Universal HPE

Motivation. "Non-universal" homomorphic encryption is proposed for schemes that support attribute privacy but require some information that is derivable from the public key (or attribute in the case of PE) in order to perform homomorphic evaluation. Therefore, attribute privacy must be surrendered to an evaluator. If this is acceptable for an application, while at the same time there is a requirement to hide the target recipient(s) from other entities in the system, then "non-universal" homomorphic encryption may be useful. Consider the following informal scenario. Suppose a collection of parties $P_1, \ldots, P_\ell$ outsource a computation on their encrypted data sets to an untrusted remote server S. Suppose S sends the result (encrypted) to an independent database DB from which users can retrieve the encrypted records. For privacy reasons, it may be desirable to limit the information that DB can learn about the attributes associated with the ciphertexts retrieved by certain users. Therefore, it may desirable for the encryption scheme to provide attribute privacy. However, given the asymmetric relationship between the delegators $P_1, \ldots, P_\ell$ and the target recipient(s), it might be acceptable for S to learn the target attribute(s) provided there is no collusion between S and DB. In fact, the delegators may belong to a different organization than the recipient(s).

In this paper, we introduce a syntax and security model for non-universal homomorphic IBE. The main change in syntax entails an additional input α that is supplied to the Eval algorithm. The input $\alpha \in \{0,1\}^d$ (where $d = poly(\lambda)$) models the additional information needed to compute the homomorphism(s). A description of an efficient map $Q_A : A \to \{0,1\}^d$ is included in the public parameters. We say that two attributes(i.e. identities in IBE) $a_1, a_2 \in A$ satisfying $Q_A(a_1) = Q_A(a_2)$ belong to the same attribute class.

One reason that the proposed syntax is not general enough for arbitrary PE functionalities is that it only facilitates evaluation on ciphertexts whose attributes are in the same attribute class, which suffices for (relatively) simple functionalities such as IBE.

We now formulate the security notion of attribute-hiding for non-universal homomorphic IBE. Our security model provides the adversary with an evaluation oracle whose identity-dependent input α is fixed when the challenge is produced. Accordingly, for a challenge identity $\mathsf{id} \in A$, and binary string $\alpha = Q_A(\mathsf{id}) \in \{0,1\}^d$, the adversary can query $\mathsf{IBE}_{\bar{U}}.\mathsf{Eval}(\mathsf{PP}, \alpha, \cdot, \cdot)$ for any circuit in $\mathbb{C}$ and any ℓ-length sequence of ciphertexts.

Formally, consider the experiment

Experiment $\bar{\mathsf{U}}\mathsf{Priv}(\mathcal{A}_1, \mathcal{A}_2)$[9]

    $(\mathsf{PP}, \mathsf{MSK}) \leftarrow \mathsf{IBE}.\mathsf{Setup}(1^\lambda)$

    $(\mathsf{id}_0, m_0), (\mathsf{id}_1, m_1), \sigma \leftarrow \mathcal{A}_1^{\mathsf{IBE}_{\bar{U}}.\mathsf{KeyGen}(\mathsf{MSK},\cdot)}(\mathsf{PP})$ $\triangleright$ σ denotes the adversary's state

    $b \xleftarrow{\$} \{0,1\}$

    $\alpha \leftarrow Q_A(\mathsf{id}_b)$

    $c \leftarrow \mathsf{IBE}.\mathsf{Encrypt}(\mathsf{PP}, \mathsf{id}_b, m_b)$

    $b' \leftarrow \mathcal{A}_2^{\mathsf{IBE}_{\bar{U}}.\mathsf{KeyGen}^*(\mathsf{MSK},\cdot), \mathsf{IBE}_{\bar{U}}.\mathsf{Eval}(\mathsf{PP}, \alpha, \cdot, \cdot)}(\mathsf{PP}, c, \sigma)$

    return 1 iff $b' = b$ and 0 otherwise.

Define the advantage of an adversary $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ in the above experiment for a $\mathsf{IBE}_{\bar{U}}$ scheme $\mathcal{E}$ as follows:

$$\mathbf{Adv}_{\mathcal{E}}^{\bar{\mathsf{U}}\mathsf{Priv}}(\mathcal{A}) = \Pr\left[\bar{\mathsf{U}}\mathsf{Priv}(\mathcal{A}) \Rightarrow 1\right] - \frac{1}{2}.$$

A $\mathsf{IBE}_{\bar{U}}$ scheme $\mathcal{E}$ is said to be attribute-hiding if for all pairs of PPT algorithms $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$, it holds that $\mathbf{Adv}_{\mathcal{E}}^{\bar{\mathsf{U}}\mathsf{Priv}}(\mathcal{A}) \leq \mathsf{negl}(\lambda)$. Note that the above definition assumes adaptive adversaries, but can be easily modified to accommodate the non-adaptive case.

6.2 Universal Anonymizers

We now present an abstraction called a *universal anonymizer*. With its help, we can transform a universally-homomorphic, non-attribute-hiding IBE scheme

---

[9] In the random oracle model, the adversary is additionally given access to a random oracle. This is what the results in this paper will use.

$\mathcal{E}$ into a non-universally homomorphic, attribute-hiding scheme $\mathcal{E}'$. In accordance with the property of universal anonymity proposed in [24], any party can anonymize a given ciphertext.

Let $\mathcal{E} := (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt}, \mathsf{Eval})$ be a PE scheme parameterized with message space M, attribute space A, class of predicates $\mathcal{F}$, and class of circuits $\mathbb{C}$. Denote its ciphertext space by $\mathcal{C}$. Note that this definition of a universal anonymizer only suffices for simple functionalities such as IBE.

Definition 8. *A universal anonymizer $U_{\mathcal{E}}$ for a PE scheme $\mathcal{E}$ is a tuple $(\mathcal{G}, \mathcal{B}, \mathcal{B}^{-1}, Q_A, Q_{\mathcal{F}})$ where $\mathcal{G}$ is a deterministic algorithm, $\mathcal{B}$ and $\mathcal{B}^{-1}$ are randomized algorithms, and Q_A and $Q_{\mathcal{F}}$ are efficient maps, defined as follows:*

- *$\mathcal{G}(\mathsf{PP})$:*
  On input the public parameter of an instance of $\mathcal{E}$, output a parameters structure params. This contains a description of a modified ciphertext space $\hat{\mathcal{C}}$ as well as an integer $d = \mathsf{poly}(\lambda)$ indicating the length of binary strings representing an attribute class.
- *$\mathcal{B}(\mathsf{params}, \mathbf{c})$:*
  On input parameters params and a ciphertext $\mathbf{c} \in \mathcal{C}$, output an element of $\hat{\mathcal{C}}$.
- *$\mathcal{B}^{-1}(\mathsf{params}, \alpha, \hat{\mathbf{c}})$:*
  On input parameters params, a binary string $\alpha \in \{0,1\}^d$ and an element of $\hat{\mathcal{C}}$, output an element of $\mathcal{C}$
- *Both maps Q_A and $Q_{\mathcal{F}}$ are indexed by params: $Q_{A\,\mathsf{params}} : A \to \{0,1\}^d$ and $Q_{\mathcal{F}\,\mathsf{params}} : \mathcal{F} \to \{0,1\}^d$*

Note: params can be assumed to be an implicit input; it will not be explicitly specified to simplify notation.

The binary string α is computed by means of a map $Q_A : A \to \{0,1\}^d$. In order for a decryptor to invert $\mathcal{B}$, α must also be computable from any predicate that satisfies an attribute that maps onto α. Therefore, the map $Q_{\mathcal{F}} : \mathcal{F} \to \{0,1\}^d$ has the property that for all $a \in A$ and $f \in \mathcal{F}$:

$$f(a) = 1 \Rightarrow Q_A(a) = Q_{\mathcal{F}}(f).$$

We define an equivalence relation $\sim$ on $\mathcal{F}$ given by

$$f_1 \sim f_2 \triangleq Q_{\mathcal{F}}(f_1) = Q_{\mathcal{F}}(f_2).$$

We have that

$$f \sim g \iff \exists h_1, \ldots, h_k \in \mathcal{F} \quad \mathsf{supp}(f) \cap \mathsf{supp}(h_1) \neq \emptyset \wedge \ldots \wedge \mathsf{supp}(h_k) \cap \mathsf{supp}(g) \neq \emptyset.$$

It follows that each α is a representative of an equivalence class in $\mathcal{F}/\sim$. As a result, as mentioned earlier, our definition of a universal anonymizer above is only meaningful for "simple" functionalities such as IBE. For example, $|\mathcal{F}/\sim| = |\mathcal{F}|$ for an IBE scheme whose ciphertexts leak the recipient's identity.

Let c be a ciphertext associated with an attribute a. Let $\alpha = Q_A(a)$. Informally, $c' := \mathcal{B}^{-1}(\alpha, \mathcal{B}(c))$ should "behave" like c; that is, (1) it should have the same homomorphic "capacity" and (2) decryption with a secret key for any f should have the same output as that for c. A stronger requirement captured in our formal correctness criterion defined in the full version is that c and c' should be indistinguishable even when a distinguisher is given access to MSK.

A universal anonymizer is employed in the following generic transformation from a universally-homomorphic, non-attribute-hiding IBE scheme $\mathcal{E}$ to a non-universally homomorphic, attribute-hiding scheme $\mathcal{E}'$.

The transformation is achieved by setting:

- $\mathcal{E}'.\mathsf{Encrypt}(\mathsf{PP}, a, m) :=$
    $\mathcal{B}(\mathcal{E}.\mathsf{Encrypt}(\mathsf{PP}, a, m))$
- $\mathcal{E}'.\mathsf{Decrypt}(\mathsf{SK}_f, c) :=$
    $\mathcal{E}.\mathsf{Decrypt}(\mathsf{SK}_f, \mathcal{B}^{-1}(Q_{\mathcal{F}}(f), c))$
- $\mathcal{E}'.\mathsf{Eval}(\mathsf{PP}, \alpha, C, c_1, \ldots, c_\ell) :=$
    return $\mathcal{B}(\mathcal{E}.\mathsf{Eval}(\mathsf{PP}, C, \mathcal{B}^{-1}(\alpha, c_1), \ldots, \mathcal{B}^{-1}(\alpha, c_\ell)))$

Denote the above transformation by $T_{U_\mathcal{E}}(\mathcal{E})$. We leave to future work the task of establishing (generic) sufficient conditions that $\mathcal{E}$ must satisfy to ensure that $\mathcal{E}' := T_{U_\mathcal{E}}(\mathcal{E})$ is an attribute-hiding $\mathsf{HPE}_{\bar{U}}$ scheme.

An instantiation of a universal anonymizer for our XOR homomorphic scheme is given in the full version.

6.3   Applications (Brief Overview)

It turns out that XOR-homomorphic cryptosystems have been considered to play an important part in several applications. The most well-known and widely-used *unbounded* XOR-homomorphic public-key cryptosystem is Goldwasser-Micali (GM) [6], which is based on the quadratic residuosity problem. Besides being used in protocols such as private information retrieval (PIR), GM has been employed in some specific applications such as:

- Peng, Boyd and Dawson (PBD) [39] propose a sealed-bid auction system that makes extensive use of the GM cryptosystem.
- Bringer et al. [40] apply GM to biometric authentication. It is used in two primary ways; (1) to achieve PIR and (2) to assist in computing the hamming distance between a recorded biometric template and a reference one.

Perhaps in some of these applications, a group-homomorphic identity-based scheme may be of import, although the authors concede that no specific usage scenario has been identified so far.

With regard to performance, our construction requires 8 multiplications in $\mathbb{Z}_N$ for a single homomorphic operation in comparison to a single multiplication

in GM. Furthermore, the construction has higher ciphertext expansion than GM by a factor of 4. Encryption involves 2 modular inverses and 6 multiplications (only 4 if the strongly homomorphic property is forfeited). In comparison, GM only requires 1.5 multiplications on average.

7   Conclusions and Future Work

We have presented a characterization of homomorphic encryption in the PE setting and classified schemes based on the properties of their attribute homomorphisms. Instantiations of certain homomorphic properties were presented for inner-product PE. However, it is clear that meaningful attribute homomorphisms are limited. We leave to future work the exploration of homomorphic encryption with access policies in a more general setting .

In this paper, we introduced a new XOR-homomorphic variant of the Cocks' IBE scheme and showed that it is strongly homomorphic. However, we failed to fully preserve the homomorphic property in anonymous variants; that is, we could not construct an anonymous universally-homomorphic variant. We leave this as an open problem. As a compromise, however, a weaker primitive (non-universal IBE) was introduced along with a related security notion. Furthermore, a transformation strategy adapted from the work of Ateniese and Gasti [25] was exploited to obtain anonymity for our XOR-homomorphic construction in this weaker primitive.

In future work, it is hoped to construct other group homomorphic IBE schemes, and possibly for more general classes of predicates than the IBE functionality.

Noteworthy problems, which we believe are still open:

1. Somewhat-homomorphic IBE scheme (even non-adaptive security in the ROM)
2. (Unbounded) Group homomorphic IBE schemes for $(\mathbb{Z}_m, +)$ where $m = O(2^\lambda)$ and $(\mathbb{Z}_p^*, *)$ for prime p. Extensions include anonymity and support for a wider class of predicates beyond the IBE functionality.

References

1. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing, STOC 2009, p. 169 (2009)
2. Smart, N.P., Vercauteren, F.: Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 420–443. Springer, Heidelberg (2010)
3. van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully Homomorphic Encryption over the Integers. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 24–43. Springer, Heidelberg (2010)
4. Brakerski, Z., Vaikuntanathan, V.: Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011)

5. Brakerski, Z., Vaikuntanathan, V.: Efficient Fully Homomorphic Encryption from (Standard) LWE. Cryptology ePrint Archive, Report 2011/344 (2011), http://eprint.iacr.org/

6. Goldwasser, S., Micali, S.: Probabilistic encryption & how to play mental poker keeping secret all partial information. In: Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing, STOC 1982, pp. 365–377. ACM, New York (1982)

7. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)

8. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms 31, 469–472 (1985)

9. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)

10. Boneh, D., Sahai, A., Waters, B.: Functional Encryption: Definitions and Challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011)

11. Gennaro, R., Gentry, C., Parno, B.: Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 465–482. Springer, Heidelberg (2010)

12. López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the 44th Symposium on Theory of Computing, STOC 2012, pp. 1219–1234. ACM, New York (2012)

13. Naccache, D.: Is theoretical cryptography any good in practice? Talk given at CHES 2010 and Crypto 2010 (2010)

14. Brakerski, Z., Vaikuntanathan, V.: Efficient Fully Homomorphic Encryption from (Standard) LWE. Cryptology ePrint Archive, Report 2011/344 Version: 20110627:080002 (2011), http://eprint.iacr.org/

15. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008, pp. 197–206. ACM, New York (2008)

16. Gentry, C., Halevi, S., Vaikuntanathan, V.: A Simple BGN-Type Cryptosystem from LWE. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 506–522. Springer, Heidelberg (2010)

17. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF Formulas on Ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005)

18. Benaloh, J.: Dense probabilistic encryption. In: Proceedings of the Workshop on Selected Areas of Cryptography, pp. 120–128 (1994)

19. Galbraith, S.D.: Elliptic Curve Paillier Schemes. J. Cryptology 15, 129–138 (2002)

20. Golle, P., Jakobsson, M., Juels, A., Syverson, P.F.: Universal re-encryption for mixnets. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 163–178. Springer, Heidelberg (2004)

21. Gjøsteen, K.: Homomorphic cryptosystems based on subgroup membership problems. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 314–327. Springer, Heidelberg (2005)

22. Armknecht, F., Katzenbeisser, S., Peter, A.: Group homomorphic encryption: characterizations, impossibility results, and applications. Designs, Codes and Cryptography, 1–24 (2012)

23. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 566–582. Springer, Heidelberg (2001)

24. Hayashi, R., Tanaka, K.: Universally Anonymizable Public-Key Encryption. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 293–312. Springer, Heidelberg (2005)

25. Ateniese, G., Gasti, P.: Universally anonymous IBE based on the quadratic residuosity assumption. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32–47. Springer, Heidelberg (2009)

26. Prabhakaran, M., Rosulek, M.: Homomorphic encryption with CCA security. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 667–678. Springer, Heidelberg (2008)

27. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)

28. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: FOCS, pp. 647–657. IEEE Computer Society (2007)

29. Goldwasser, S.: Lecture: Introduction to homomorophic encryption (2011), http://www.cs.bu.edu/~reyzin/teaching/s11cs937/notes-shafi-1.pdf (last Checked on March 31, 2013)

30. Agrawal, S., Gorbunov, S., Vaikuntanathan, V., Wee, H.: Functional encryption: New perspectives and lower bounds. Cryptology ePrint Archive, Report 2012/468 (2012), http://eprint.iacr.org/

31. Bellare, M., O'Neill, A.: Semantically-secure functional encryption: Possibility results, impossibility results and the quest for a general definition. Cryptology ePrint Archive, Report 2012/515 (2012), http://eprint.iacr.org/

32. Wei, R., Ye, D.: Delegate predicate encryption and its application to anonymous authentication. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ASIACCS 2009, pp. 372–375. ACM, New York (2009)

33. Rothblum, R.: Homomorphic Encryption: From Private-Key to Public-Key. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 219–234. Springer, Heidelberg (2011)

34. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)

35. Alzaid, H., Foo, E., Nieto, J.G.: Secure data aggregation in wireless sensor network: a survey. In: Proceedings of the Sixth Australasian Conference on Information Security, AISC 2008, vol. 81, pp. 93–105. Australian Computer Society, Inc., Darlinghurst (2008)

36. Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: Functional encryption for inner product predicates from learning with errors. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 21–40. Springer, Heidelberg (2011)

37. 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)

38. Armknecht, F., Katzenbeisser, S., Peter, A.: Group homomorphic encryption: Characterizations, impossibility results, and applications. Cryptology ePrint Archive, Report 2010/501 (2010), `http://eprint.iacr.org/`
39. Peng, K., Boyd, C., Dawson, E.: A Multiplicative Homomorphic Sealed-Bid Auction Based on Goldwasser-Micali Encryption. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 374–388. Springer, Heidelberg (2005)
40. Bringer, J., Chabanne, H., Izabachène, M., Pointcheval, D., Tang, Q., Zimmer, S.: An application of the goldwasser-micali cryptosystem to biometric authentication. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 96–106. Springer, Heidelberg (2007)