On Homomorphic Encryption and Chosen-Ciphertext Security

Brett Hemenway[1] and Rafail Ostrovsky[2⋆]

[1] University of Michigan
[2] UCLA

Abstract. Chosen-Ciphertext (IND-CCA) security is generally considered the right notion of security for a cryptosystem. Because of its central importance much effort has been devoted to constructing IND-CCA secure cryptosystems.
In this work, we consider constructing IND-CCA secure cryptosystems from (group) homomorphic encryption. Our main results give natural and efficient constructions of IND-CCA secure cryptosystems from any homomorphic encryption scheme that satisfies weak cyclic properties, either in the plaintext, ciphertext or randomness space. Our results have the added benefit of being simple to describe and analyze.

1 Introduction

Since the definition of security against a Chosen-Ciphertext Attack (IND-CCA) was given in [NY90], [RS91], much effort has been devoted to constructing efficient IND-CCA secure cryptosystems under a variety of cryptographic hardness assumptions.

The first construction of an IND-CCA secure cryptosystem was given by Dolev, Dwork and Naor in [DDN91]. Their construction builds on the ideas of Naor and Yung [NY90], and relies on non-interactive zero-knowledge proofs, to prove that a ciphertext was created honestly. The generic non-interactive zero-knowledge proofs used in [DDN91] are too inefficient for practical use, but the idea of including some sort of "proof of validity" in the ciphertext has strongly shaped this area of research, and many of the subsequent IND-CCA secure cryptosystems can be viewed in this light.

[⋆] R. Ostrovsky, University of California Los Angeles, Department of Computer Science and Department of Mathematics, 3732D Boelter Hall, Los Angeles CA 90095-1596, U.S., email: rafail@cs.ucla.edu. Supported in part by NSF grants 0830803, 09165174, 1065276, 1118126 and 1136174, US-Israel BSF grant 2008411, OKAWA Foundation Research Award, IBM Faculty Research Award, Xerox Faculty Research Award, B. John Garrick Foundation Award, Teradata Research Award, and Lockheed-Martin Corporation Research Award. This material is based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014-11-1-0392. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

The first IND-CCA secure cryptosystem efficient enough to be used in practice was given by Cramer and Shoup in [CS98], and the security of their construction rested on the Decisional Diffie-Hellman (DDH) assumption. Since then, there have many fairly efficient IND-CCA secure schemes proposed under a wide variety of cryptographic hardness assumptions.

Constructions based on the DDH assumption include those of [CS98],[CS02] and [PW08]. Recently, new constructions were given based on the Computational Diffie-Hellman (CDH) assumption [HJKS10], [CHK10]. IND-CCA secure cryptosystems based on the RSA assumption are given in [CHK10]. Schemes based on the Quadratic Residuosity (QR) assumption are given in [CS02]. IND-CCA secure cryptosystems based on lattice assumptions like Learning With Errors (LWE) are given in [PW08] and [Pei09]. In the pairing world, IND-CCA secure schemes can be based on the Bilinear Diffie-Hellman (BDH) assumption [CHK04],[BK05],[BCHK07], or the Decisional Linear (D-Lin) assumption [FGK$^+$10]. Chosen-ciphertext secure cryptosystems have also been proposed based on the Syndrome Decoding problem [DMQN09], [FGK$^+$10].

For a notion as fundamental as secure encryption, it is important to consider generic constructions as well as concrete instantiations, and in fact, many of the above constructions are best viewed as part of general frameworks for constructing IND-CCA secure encryption. In [DDN91], IND-CCA secure cryptosystems were built from any one-way trapdoor permutation. In [CS02], Cramer and Shoup gave a general construction based on universal hash proof systems, which can be viewed as an algebraic designated verifier proof system. In [CHK04],[BCHK07], Boneh, Canetti, Halevi and Katz gave a general framework for constructing IND-CCA secure encryption from any Identity-Based Encryption (IBE) scheme. In [PW08], Peikert and Waters created lossy trapdoor functions (LTDFs) as a method for constructing IND-CCA secure encryption. The notion of lossy trapdoor functions has since been relaxed to correlated product secure functions [RS09], and slightly lossy trapdoor functions [MY09], and both relaxations were shown to still be sufficient to construct IND-CCA secure encryption.

These frameworks provide many different constructions of IND-CCA secure encryption, and help to locate IND-CCA secure encryption in the cryptographic landscape. Despite their utility, these frameworks all rely on fairly complicated underlying primitives, and the search continues for the simplest primitive that can be shown to imply IND-CCA secure encryption. Perhaps the simplest primitive that could imply IND-CCA secure encryption is IND-CPA secure encryption. This, however, is widely believed to be false, and the results of Gertner, Malkin and Myers [GMM07] give partial results towards the impossibility of such a construction.

It is natural, then, to examine what additional properties of an IND-CPA secure cryptosystem are sufficient to construct an IND-CCA secure cryptosystem. One natural property, is that the IND-CPA secure cryptosystem supports a group operation on the plaintext. Such cryptosystems are called *homomorphic.* Indeed, one of the main open questions concerning homomorphic encryption is whether homomorphic encryption implies IND-CCA encryption, and this question has attracted much attention over the years.

In this work, we will call an encryption scheme *homomorphic* if the plaintexts form a group, the ciphertexts form a group, and $E(pk, m_1, r_1) \cdot E(pk, m_2, r_2) = E(pk, m_1+m_2, r^*)$. Unless explicitly stated, we will not assume that $r^* = r_1+r_2$, schemes that satisfy this additional property are said to be *homomorphic over their randomness.*[3] Here we have written the group operation on the ciphertexts multiplicatively and the group operations on the plaintexts additively. This is simply a convention, but it is a natural one since it corresponds to the usual method of writing the groups corresponding to Goldwasser-Micali [GM84], Paillier [Pai99], and (additive) El-Gamal [Gam85]. We do *not* require our encryption schemes to be *fully homomorphic*, as constructed in the breakthrough work of Gentry [Gen09].

The consequences of the existence of homomorphic encryption have been well studied, and many exciting results are known. Homomorphic encryption has been show to imply Private Information Retrieval (PIR) [KO97],[Man98],[IKO05]. Since PIR implies Collision Resistant Hash Functions [IKO05], Oblivious Transfer [CMO00], and lossy encryption [HLOV11], we immediately have constructions of any of these primitives based on any homomorphic encryption. The work of [AKP10] provides a clean abstraction of homomorphic encryption and a discussion of homomorphic encryption and its relations to IND-CCA1 security.

It remains an important open question whether homomorphic encryption implies IND-CCA secure cryptosystems, and in this work we present steps towards closing the gap.

1.1 Previous Work

Chosen-ciphertext security was introduced by Rackoff and Simon in [RS91], and the first cryptosystem provably secure in this model was given in [DDN91], extending the work of [NY90]. Since that time, there has been a vast amount of work done on the topic of IND-CCA secure encryption.

Our work draws most from the works of Cramer and Shoup on universal hash proof systems [CS02], and Peikert and Waters on lossy trapdoor functions [PW08], and we briefly highlight some key ideas of their constructions below.

The first practical IND-CCA secure cryptosystem was given by Cramer and Shoup in [CS98]. In [CS02], Cramer and Shoup created Universal Hash Proof systems, generalizing their work in [CS98], and providing a framework for creating IND-CCA secure encryption. In [CS02], Cramer and Shoup defined a natural algebraic object called a *Diverse Group System*, and showed that diverse group systems imply universal hash proof systems, and diverse group systems are implied by many natural cryptographic hardness assumptions that occur in groups. The algebraic nature of diverse group systems suggests a possible connection

[3] Notice that our definition of homomorphic encryption implies that the randomness space forms a group, since the randomness space is isomorphic to the subgroup of encryptions of 0.

between homomorphic encryption and IND-CCA secure encryption, and in this work we explore this connection.

A different framework for constructing IND-CCA secure cryptosystems was proposed by Peikert and Waters in [PW08]. In their work, Peikert and Waters defined Lossy Trapdoor Functions (LTDFs), and showed that LTDFs imply IND-CCA secure cryptosystems. Roughly, a lossy trapdoor function, is a function that can operate in one of two computationally indistinguishable modes. In injective mode, it is injective and has a trapdoor. In "lossy" mode, the function statistically loses information about its input. In [PW08], Peikert and Waters leveraged the homomorphic properties of the El-Gamal cryptosystem and the Regev [Reg05] cryptosystem to create LTDFs based on the DDH and LWE assumptions. At the highest level, their construction proceeds as follows. The description of an LTDF in injective mode is simply the encryption of the identity matrix using some underlying homomorphic cryptosystem, and the description of an LTDF in lossy mode is the encryption of the zero matrix. To evaluate a function on an input x, viewed as a bit vector, we compute the matrix product of the ciphertext matrix with the input vector. By the homomorphic properties of the underlying cryptosystem, this results in either a ciphertext vector encrypting x, or a ciphertext vector encrypting the zero vector. It is easy to see that the IND-CPA security of the underlying cryptosystem implies that the injective and lossy modes are indistinguishable, and the decryption algorithm provides a trapdoor in injective mode. The difficulty is in showing that the lossy mode *statistically* loses information about its input. Let us examine this further. The output of a lossy function is the encryption of the zero vector, so it is clear that the underlying plaintexts are statistically independent of the input x (since they are all 0). It is, however, unclear whether the *randomness* of the ciphertexts statistically encodes the vector x. The constructions of LTDFs given by Peikert and Waters, modify the underlying homomorphic cryptosystems to ensure that the randomness of the resulting ciphertext vector does not leak too much information about the input x.

Both the works of [CS02] and [PW08] give an indication of the connection between homomorphic encryption and IND-CCA secure encryption, but despite significant effort, no one has, as yet, been able to bridge the gap.

In this work, we show that if we have a homomorphic cryptosystem with some natural cyclic structure, we immediately have IND-CCA secure encryption.

1.2 Our Contributions

In this work, we consider the problem of constructing an IND-CCA secure cryptosystem from homomorphic encryption schemes. By a homomorphic encryption scheme, we mean an IND-CPA secure cryptosystem, for which the plaintext space forms a group, the ciphertext space forms a group, and the group operation on ciphertexts induces a group operation on plaintexts. Cryptosystems of this type arise naturally, e.g. [Gam85,GM84,Pai99,Ben94,OU98,NS98,DJ01,BGN05].

It has been a long standing open question whether an IND-CCA secure cryptosystem can be constructed from any homomorphic encryption scheme. In this work, we give a number of simple properties for a homomorphic encryption scheme, any one of which allows us to construct an IND-CCA secure cryptosystem.

Our results can be summarized as follows:

Lemma (Lemma 1 (informal)). *If there exists a homomorphic encryption with cyclic plaintext group X, and randomness space R, such that $|X| > |R|$, then there exist lossy trapdoor functions.*

Corollary (Corollary 1 (informal)). *If there exists a homomorphic encryption with cyclic ciphertext space, with plaintext group X, and randomness space R, such that $|X| > |R|$, then there exist lossy trapdoor functions.*

Theorem (Main Theorem (informal)). *If there exists a homomorphic encryption with cyclic ciphertext space, then there exist universal hash proof systems, and hence IND-CCA secure encryption.*

2 Preliminaries

2.1 Notation

If $f : X \to Y$ is a function, for any $Z \subset X$, we let $f(Z) = \{f(x) : x \in Z\}$. For example, if E is an encryption algorithm $E(pk, x, R) = \{E(pk, x, r) : r \in R\}$, is the set of all encryptions of x. Similarly, $E(pk, X, R) = \{E(pk, x, r) : x \in X, r \in R\}$ is the ciphertext space of E. If G is a group, and $g_1, \ldots, g_d$ are elements of G, then we use the notation $\langle g_1, \ldots, g_d \rangle$ to denote the subgroup of G generated by $g_1, \ldots, g_d$.

If A is a PPT machine, then we use $a \leftarrow A$ to denote running the machine A and obtaining an output, where a is distributed according to the internal randomness of A. If R is a set, and no distribution is specified, we use $r \leftarrow R$ to denote sampling uniformly from the uniform distribution on R.

If X and Y are families of distributions indexed by a security parameter λ, we say that X is statistically close to Y, (written $X \approx_s Y$) to mean that for all polynomials p and sufficiently large λ, we have $\sum_x |\Pr[X = x] - \Pr[Y = x]| < \frac{1}{p(\lambda)}$.

We say that X and Y are computationally close (written $X \approx_c Y$) to mean that for all PPT adversaries A, for all polynomials p, and for all sufficiently large λ, we have $|\Pr[A^X = 1] - \Pr[A^Y = 1]| < 1/p(\lambda)$.

2.2 Homomorphic Encryption

A public key cryptosystem given by algorithms (G, E, D) is called *homomorphic* if

- The plaintext space forms a group X (written with group operation $+$).
- The ciphertexts are members of a group Y.

- For all $x_0, x_1 \in X$, and for all r_0, r_1 in the randomness space R, there exists an $r^* \in R$ such that

$$E(pk, x_0 + x_1, r^*) = E(pk, x_0, r_0)E(pk, x_1, r_1).$$

Notice that we do not assume that the encryption is also homomorphic over the randomness, as is the case of most homomorphic encryption schemes, e.g. El-Gamal, Paillier, and Goldwasser-Micali. We also do not assume that the image $E(pk, X, R)$ is the whole group Y, only that $E(pk, X, R) \subset Y$. Since the homomorphic property implies closure, we have that $E(pk, X, R)$ is a semi-group.[4] Notice also, that while it is common to use the word "homomorphic" to describe the cryptosystem, encryption is *not* a homomorphism in the mathematical sense (although decryption is).

We now show some basic properties from all homomorphic encryption schemes. These facts are commonly used but, since our definition is weaker than the (implicit) definitions of homomorphic encryption that appear in the literature, it is important to note that they hold under this definition as well.

- $E(pk, X, R)$ is a group.
- $E(pk, 0, R)$ is a subgroup of $E(pk, X, R)$.
- For all $x \in X$, $E(pk, x, R)$ is the coset $E(pk, x, r)E(pk, 0, R)$.
- For all $x_0, x_1 \in X$, $|E(pk, x_0, R)| = |E(pk, x_1, R)|$.
- If y is chosen uniformly from $E(pk, 0, R)$, then $yE(pk, x, r)$ is uniform in $E(pk, x, R)$.
- $E(pk, X, R)$ is such that $E(pk, X, R) \simeq X \times E(pk, 0, R)$ and decryption is the homomorphism

$$E(pk, X, R) \to E(pk, X, R)/E(pk, 0, R) \simeq X.$$

- If y is chosen uniformly from $E(pk, 0, R)$, then for any $x \in X$, $yE(pk, x, r)$ is uniformly distributed in $E(pk, X, R)$. This follows because the map

$$\begin{aligned} f : E(pk, 0, R) &\to E(pk, X, R) \\ y &\mapsto yE(pk, x, r) \end{aligned}$$

is an injection because the group element $E(pk, x, r)$ has an inverse in Y (we do not need to assume that the inverse is a valid ciphertext). Thus by counting, we see that f is in fact a bijection. Hence if y is uniformly distributed, so is $f(y)$.

We call a public key cryptosystem a *homomorphic public key encryption scheme*, if it is IND-CPA secure and homomorphic.

[4] A semi-group satisfies the axioms of a group but is not guaranteed to have an identity element or inverses.

2.3 Diverse Group Systems

In [CS02], Cramer and Shoup defined diverse group systems and used them as a foundation for all their constructions of Universal Hash Proof Systems. We review these definitions here.

Let Z, L, Π be finite abelian groups written additively, with $L \subsetneq Z$. Let $\mathrm{Hom}(Z, \Pi)$ be the group of homomorphisms, $\phi : Z \to \Pi$. This is also clearly an abelian group under the operation $(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x)$.

Definition 1 (Group System). *Let Z, L, Π be finite abelian groups with $L \subsetneq Z$. Let $\mathbf{H} \subset \mathrm{Hom}(Z, \Pi)$. We call*

$$\mathbf{G} = (\mathbf{H}, Z, L, \Pi),$$

a group system*.*

Definition 2 (Diverse Group System). *We call a group system $\mathbf{G} = (\mathbf{H}, Z, L, \Pi)$* diverse *if for all $z \in Z \setminus L$, there exists $\phi \in \mathbf{H}$ such that $\phi(\ell) = 0$ for all $\ell \in L$, but $\phi(z) \neq 0$.*

In [CS02] Cramer and Shoup show a natural method for constructing Universal Hash Proof Systems from Diverse Group Systems.

Definition 3 (Hash Proof System Associated to a Diverse Group System). *Let $\mathbf{G} = (\mathbf{H}, Z, L, \Pi)$ be a diverse group system, and let $g_1, \ldots, g_d \in L$ be a set of generators for L. We define the associated Hash Proof system $\mathbf{UHP} = (H, K, Z, L, \Pi, S, \alpha)$,*

- *For uniformly chosen $k \in K$, H_k is uniform on $\mathbf{H}$.*
  Without loss of generality, we may assume $K = \mathbf{H}$, and $k = \phi \in \mathbf{H}$.
  We maintain Universal Hash Proof notation to emphasize that $H_k(\cdot)$ that someone who can calculate $H_k(\cdot)$ on elements of L may not know the underlying homomorphism ϕ.
- *$S = \Pi^d$, and*

$$\begin{aligned} \alpha : K &\to S \\ k &\mapsto (H_k(g_1), \ldots, H_k(g_d)). \end{aligned}$$

2.4 Lossy Trapdoor Functions

We briefly review the notion of *Lossy Trapdoor Functions* (LTDFs) as described in [PW08].

Intuitively, a family of Lossy Trapdoor Functions is a family of functions which have two modes, injective mode, which has a trapdoor, and lossy mode which is guaranteed to have a small image size. In particular, the preimage of any element in the image will have a large size. Formally we have:

Definition 4 (Lossy Trapdoor Functions). *A tuple $(S_{\mathrm{ltdf}}, F_{\mathrm{ltdf}}, F_{\mathrm{ltdf}}^{-1})$ of PPT algorithms is called a family of (n, k)-Lossy Trapdoor Functions if the following properties hold:*

- ***Sampling Injective Functions:*** *$S_{\mathrm{ltdf}}(1^\lambda, 1)$ outputs s, t where s is a function index, and t its trapdoor. We require that $F_{\mathrm{ltdf}}(s, \cdot)$ is an injective deterministic function on $\{0,1\}^n$, and $F^{-1}_{\mathrm{ltdf}}(t, F_{\mathrm{ltdf}}(s, x)) = x$ for all x.*
- ***Sampling Lossy Functions:*** *$S_{\mathrm{ltdf}}(1^\lambda, 0)$ outputs $(s, \perp)$ where s is a function index and $F_{\mathrm{ltdf}}(s, \cdot)$ is a function on $\{0,1\}^n$, where the image of $F_{\mathrm{ltdf}}(s, \cdot)$ has size at most 2^{n-k}.*
- ***Indistinguishability:*** *The first outputs of $S_{\mathrm{ltdf}}(1^\lambda, 0)$ and $S_{\mathrm{ltdf}}(1^\lambda, 1)$ are computationally indistinguishable.*

3 Implications of Homomorphic Encryption

Much effort has been devoted studying the implications of homomorphic encryption, and many results are now known. It is known that homomorphic encryption implies Private Information Retrieval (PIR) [KO97],[Man98],[IKO05], and since PIR implies Collision Resistant Hash Functions [IKO05], Oblivious Transfer [CMO00], and lossy encryption [HLOV11], we immediately have constructions of these primitives based on any homomorphic encryption. It remains open, however, whether homomorphic encryption implies IND-CCA secure cryptosystems.

Our main contributions are a step towards resolving this long-standing open question.

3.1 Constructing Lossy Trapdoor Functions

As in Section 2.2, throughout the following section, let (G, E, D) be a homomorphic encryption with plaintext group X, and randomness space R. We write the group operation on X additively and the group operation on ciphertexts multiplicatively.

We begin by attempting to generalize the construction of lossy trapdoor functions from the Damgård-Jurik cryptosystem given by [BFOR08], [RS08] and [FGK+10].

- **Sampling Injective Functions:** $S_{\mathrm{ltdf}}(1^\lambda, 1)$, runs $(pk, sk) \leftarrow G(1^\lambda)$, and chooses $r \leftarrow R$, and sets $e = E(pk, 1, r)$. The function index $s = (pk, e)$, and the trapdoor $t = sk$.
- **Sampling Lossy Functions:** $S_{\mathrm{ltdf}}(1^\lambda, 0)$, runs $(pk, sk) \leftarrow G(1^\lambda)$, and chooses $r \leftarrow R$, and sets $e = E(pk, 0, r)$. The function index $s = (pk, e)$, and the trapdoor $t = \perp$.
- **Evaluation:** Given $s = e$ and an input $a \in \{0, 1, \ldots, B-1\}$,

$$F_{\mathrm{ltdf}}(s, a) = e^a$$

- **Inversion:** Given $t = sk$, and a value c, set $a = D(sk, c)$.

Fig. 1: Generalizing the DCR-based LTDFs

Lemma 1. *Let (G, E, D) be a homomorphic encryption such that the plaintext group X is cyclic, with $|X| \geq B > |R|$, for some publicly known bound $B \in \mathbb{Z}$, then the construction given in Figure 1 is a family of lossy trapdoor functions.*

Proof. Note that the homomorphic property of the cryptosystem ensures that the product of two ciphertexts can be computed efficiently, so e^a can be computed efficiently using the square-and-multiply algorithm. Correctness of inversion follows immediately from the correctness of decryption. The indistinguishability of modes follows immediately from the IND-CPA security of (G, E, D). It remains only to consider the lossiness of the lossy mode.

The output of the function in lossy mode is $F_{\text{ltdf}}(s, a) = e^a$, where $e = E(pk, 0, r)$, thus $F_{\text{ltdf}}(s, a)$ is a valid encryption of 0, i.e. $F_{\text{ltdf}}(s, a) \in E(pk, 0, R)$. Since the size of $|E(pk, 0, R)| \leq |R|$, and there are B choices for a, with $B > |R|$, the function is lossy. It is clear as well that as the ratio of B to $|R|$ grows, the functions become more lossy. If the size of X is efficiently computable, then it is natural to take $B = |X|$.

Lemma 1 has an immediate corollary, that if we assume instead that the ciphertext space is cyclic, we obtain the same result.

Corollary 1. *If (G, E, D) is a homomorphic encryption such that the group $E(pk, X, R)$ is cyclic with $|X| > |R|$, then the construction in Lemma 1 is a family of lossy trapdoor functions.*

Proof. The decryption algorithm provides an isomorphism between $E(pk, X, R)/E(pk, 0, R)$ and X, and since the quotient group of a cyclic group is cyclic, we conclude that X must be cyclic, and the result follows from Lemma 1.

The construction outline in Figure 1 leaves much to be desired, the three primary drawbacks are:

1. This construction requires a known public bound B, separating the size of the plaintext and randomness spaces. This condition seems extremely mild, however, since the definition of IND-CPA security requires the plaintext space be efficiently samplable, and the group is cyclic.
2. The requirement that the messages be longer than the randomness in Lemma 1 is rather strong. In fact, the Damgård-Jurik cryptosystem is the only homomorphic cryptosystem known to have this property.[5] In the next section, we show how to remove this restriction on the size of the plaintext space.
3. Decryption involves a somewhat more subtle difficulty. A careful look at the functions in Lemma 1 shows that the input is $a \in \{0, \ldots, B - 1\}$, yet the trapdoor reveals $1 \cdot a \in X$. If $a \in \mathbb{Z}$ can be recovered from $1 \cdot a \in X$ (i.e. the Discrete Log Problem is easy in X[6]), this will not be an issue.

[5] It is trivial to construct non-homomorphic cryptosystems that have this property by extending the randomness using a PRG.

[6] As is the case with the Damgård-Jurik cryptosystem.

In the case that the discrete-log problem is hard in the plaintext group X, we can still apply F_{ltdf} on random inputs, which may be enough for some applications. To see this, notice that we can sample pairs $x, F_{\mathrm{ltdf}}(s,x)$, by sampling $a \leftarrow \{0,1,\ldots,B-1\}$, setting $x = 1 \cdot a \in X$, and setting $F_{\mathrm{ltdf}}(s,x) = e^a$. With this (slightly modified) definition, inversion becomes efficient. We can no longer evaluate, $F_{\mathrm{ltdf}}(s,\cdot)$ on given values of x, but we can sample pairs $x, F_{\mathrm{ltdf}}(s,x)$, where x is chose (almost) uniformly. This is not a serious restriction, however, since one-wayness only makes sense when applying a function to a high min-entropy input.

Unfortunately, this is *not* enough to apply the constructions of IND-CCA secure encryption from LTDFs given in [PW08,RS09,MY09]. Although these constructions require applying $F_{\mathrm{ltdf}}(s,\cdot)$ on a random input, the decryption algorithm requires inverting one function and then evaluating the All-But-One function to the recovered input. This second evaluation cannot be performed when the discrete-log problem is hard in the plaintext space X.

We can quantify the lossiness of the functions given in Figure 1 based on the ratio of B to $|R|$. If $\frac{B}{|R|} = \omega(\lambda)$, then we obtain strong lossy trapdoor functions, as required for the constructions in [PW08]. If we only have $B/|R| > 1 + 1/\mathrm{poly}(\lambda)$, then we obtain slightly lossy trapdoor functions as defined by Mol and Yilek [MY09]. The results of Mol and Yilek show that this is in fact sufficient for constructing Correlated Product Secure Functions [RS09], and IND-CCA secure cryptosystems.[7]

3.2 Constructing Diverse Group Systems

The generalization of the construction of the [BFOR08,RS08,FGK+10] given in Section 3.1 leaves much to be desired. In this section, by applying a different method, we are able to obtain a stronger result[8] than in Section 3.1 under a slightly different assumption. In particular, we show that any homomorphic encryption with cyclic ciphertext space (e.g. Goldwasser-Micali, Paillier), immediately implies Diverse Group Systems as defined by Cramer and Shoup in [CS02]. This method does not suffer from many of the drawbacks of the previous method.

Theorem 1. *Let (G, E, D) be a homomorphic encryption with plaintext group X and ciphertext group Y. If the group $E(pk, X, R)$ is cyclic, then $\mathbf{G} = (\mathbf{H}, Z, L, \mathit{\Pi})$ is a* Diverse Group System. *Let $\gamma = |E(pk, X, R)|$.*

- *$Z = E(pk, X, R) \subset Y$, is the group of all encryptions.*

[7] Again, we reiterate, that to apply the results of [PW08,RS09,MY09], the discrete-log problem must be solvable in X.

[8] We will construct a Diverse Group System which is known to imply LTDFs by [HO12].

- $\mathbf{H}$ *is the set of homomorphisms given by exponentiating in the group, i.e. for* $k \in \{0, 1, \ldots, \gamma\}$*, and* $z \in Z$*,* $H_k(z) = z^k$*. So* $|\mathbf{H}| = |E(pk, X, R)| = |Z|$*.*
- $L = E(pk, 0, R)$ *is the group of all encryptions of* 0*.*
- $\Pi = Z = E(pk, X, R)$*.*

Proof. To show that $\mathbf{G}$ is *diverse*, we must show that for all $z \in Z \setminus L$, there exists a $\phi \in \mathbf{H}$ such that $\phi(L) = \langle 0 \rangle$, but $\phi(z) \neq 0$.

Let $\eta = |L|$, and $\gamma = |Z|$. Since Z was assumed to be cyclic, and L is a subgroup of Z, we know that L is cyclic and $\eta = |L|$ divides $|Z| = \gamma$. Now, it is also a basic fact about cyclic groups that L is exactly the subgroup of elements of Z whose order divides η, i.e. $L = \{z : z \in Z, z^\eta = 1\}$. For any $z \in Z \setminus L$, Let d be the order of z, i.e. d is the smallest positive integer such that $z^d = 1$. Since $z \notin L$, we know that d doesn't divide η. Thus we may set $k = \eta$, (or any multiple of η not divisible by d). In which case, we have $H_k(z) = z^\eta \neq 0$. But $H_k(\ell) = \ell^\eta = 0$ for all $\ell \in L$. This shows that any cyclic group (with a proper subgroup) gives rise to a Diverse Group System.

To prove security, however, we need to show that L and Z are indistinguishable. This follows easily, however, since L is the set of encryptions of 0, and Z is the set of all encryptions, they are indistinguishable by the IND-CPA security of (G, E, D).

Applying the results of [CS02], which show that Diverse Group Systems imply universal hash proof systems, and universal hash proof systems imply IND-CCA secure cryptosystems, we arrive at the following result.

Corollary 2. *Homomorphic encryption with cyclic ciphertext space implies IND-CCA secure encryption.*

Applying the results of [HO12], which show that Diverse Group Systems imply Lossy Trapdoor Functions, we have

Corollary 3. *Homomorphic encryption with cyclic ciphertext space implies Lossy Trapdoor Functions.*

Applying the results of [BFOR08], we have

Corollary 4. *Homomorphic encryption with cyclic ciphertext space implies Deterministic Encryption.*

Corollary 5. *If* (G, E, D) *is a homomorphic encryption with cyclic* randomness *space, and there is an element* $x_0 \in X$ *such that the order of* x_0 *in the group* X *is relatively prime to* $|R|$*, then there is an IND-CCA secure cryptosystem.*

Proof. We define a new cryptosystem (G', E', D'), with plaintext space X', and randomness space R'. We set $X' = \langle x_0 \rangle \subset X$, and $R' = R$. We define $G' = G$, $E'(pk, x, r) = E(pk, x, r)$, for $x \in X'$, and $D' = D$. We claim that the ciphertext space of (G', E', D') is cyclic. To see this, notice first that the map $R \to E(pk, 0, R)$, given by $r \mapsto E(pk, 0, r)$ is a surjective homomorphism, thus $E(pk, 0, R)$ is isomorphic to a quotient group of R. Since R is cyclic, all its quotient groups are cyclic, so we see that $E(pk, 0, R)$ is also cyclic, in addition $|E(pk, 0, R)|$ divides $|R|$. Since $E(pk, 0, R) = E'(pk, 0, R')$, we have $|E'(pk, 0, R')|$ divides $|R|$, and is thus relatively prime to the order of the cyclic group $|\langle x_0 \rangle|$, which has size equal to the order of x_0. Thus the group $\langle x_0 \rangle \times E'(pk, 0, R')$ is cyclic, but this group is isomorphic to $E'(pk, X', R')$, so we may apply Theorem 1 to construct an IND-CCA secure cryptosystem.

4 Conclusion

In this work, we examined the connection between homomorphic encryption and chosen-ciphertext (IND-CCA) secure encryption. In particular, we showed that any homomorphic encryption with a large cyclic plaintext space implies Lossy Trapdoor Functions, and when the discrete-log problem is easy in the plaintext group, then this implies IND-CCA encryption.

More importantly, we showed that any homomorphic encryption with a cyclic ciphertext space implies universal hash proof systems, and hence both Lossy Trapdoor Functions and IND-CCA secure encryption.

Homomorphic encryption schemes arise naturally in many contexts, where the security rests on a computational hardness assumption about groups. This makes homomorphic encryption a natural candidate for creating more complex cryptographic primitives.

Our constructions of IND-CCA secure cryptosystems from homomorphic encryption over a cyclic space are efficient, and have the benefit of simple proofs of security. Our results extend what is known to follow from homomorphic encryption, and bring us one step closer to the long sought-after goal of a generic construction of IND-CCA secure encryption from any homomorphic cryptosystem.

References

[AKP10] Frederik Armknecht, Stefan Katzenbeisser, and Andreas Peter. Group homomorphic encryption. IACR ePrint Archive 2010/501, 2010.

[BCHK07] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2007.

[Ben94] Josh Cohen Benaloh. Dense probabilistic encryption. In *Proceedings of the Workshop on Selected Areas in Cryptography*, pages 120–128, 1994.

[BFOR08] Mihir Bellare, Marc Fischlin, Adam O'Neill, and Thomas Ristenpart. Deterministic encryption: Definitional equivalences and constructions without random oracles. In David Wagner, editor, *CRYPTO '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2008.

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In Joe Killian, editor, *TCC '05*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–342. Springer, 2005.

[BK05] Dan Boneh and Jonathan Katz. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In *CT-RSA '05*, pages 87–103. Springer Berlin / Heidelberg, 2005.

[CHK04] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In *Eurocrypt '04*, volume 3027 of *Lecture Notes in Computer Science*, pages 207–222, 2004.

[CHK10] Ronald Cramer, Dennis Hofheinz, and Eike Kiltz. A twist on the naor-yung paradigm and its application to efficient cca-secure encryption from hard search problems. In *TCC '10*, 2010.

[CMO00] Giovanni Di Crescenzo, Tal Malkin, and Rafail Ostrovsky. Single database private information retrieval implies oblivious transfer. In *EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 122–138. Springer Berlin / Heidelberg, 2000.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO '98*, volume 1462, pages 1–13. Springer Verlag, 1998.

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In - *EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64, 2002. Full version available at `http://eprint.iacr.org` Cryptology ePrint Archive, Report 2001/085.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *STOC '91*, pages 542–552, 1991.

[DJ01] Ivan Damgård and Mads Jurik. A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In *PKC '01: Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography*, pages 119–136, London, UK, 2001. Springer-Verlag.

[DMQN09] Rafael Dowsley, Jörn Müller-Quade, and Anderson C. Nascimento. A CCA2 secure public key encryption scheme based on the McEliece assumptions in the standard model. In *CT-RSA '09*, pages 240–251, Berlin, Heidelberg, 2009. Springer-Verlag.

[FGK$^+$10] David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev. More constructions of lossy and correlation-secure trapdoor functions. In *Public Key Cryptography 2010 (PKC 2010)*, Lecture Notes in Computer Science, pages 279–295, 2010.

[Gam85] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC '09*, pages 169–178, New York, NY, USA, 2009. ACM.

[GM84] Shafi Goldwasser and Sylvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.

[GMM07] Yael Gertner, Tal Malkin, and Steven Myers. Towards a separation of semantic and CCA security for public key encryption. In *TCC '07*, volume 4392 of *Lecture Notes in Computer Science*, pages 434–455. Springer Verlag, 2007.

[HJKS10] Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, and Victor Shoup. Simple and efficient public-key encryption from computational diffie-hellman in the standard model. In *PKC '10*, pages 1–18, 2010.

[HLOV11] Brett Hemenway, Benoît Libert, Rafail Ostrovsky, and Damien Vergnaud. Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. In *ASIACRYPT '11*, 2011.

[HO12] Brett Hemenway and Rafail Ostrovsky. Extended-DDH and lossy trapdoor functions. In *PKC 2012*, 2012.

[IKO05] Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Sufficient conditions for collision resistant hashing. In *TCC '05*, volume 3378, pages 445–456. Springer Berlin / Heidelberg, 2005.

[KO97] Eyal Kushilevitz and Rafail Ostrovsky. Replication is not needed: Single database, computationally-private information retrieval. In *FOCS '97*, pages 364–373. ACM, 1997.

[Man98] Eran Mann. Private access to distributed information. Master's thesis, Technion - Israel Institute of Technology, 1998.

[MY09] Petros Mol and Scott Yilek. Chosen-ciphertext security from slightly lossy trapdoor functions. In *PKC '10*, pages 296–311, 2009.

[NS98] David Naccache and Jacques Stern. A new public key cryptosystem based on higher residues. In *CCS '98: Proceedings of the 5th ACM conference on Computer and communications security*, pages 59–66, New York, NY, USA, 1998. ACM Press.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC '90*, pages 427–437, 1990.

[OU98] Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. In *Eurocrypt '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318. Springer Berlin / Heidelberg, 1998.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer Berlin / Heidelberg, 1999.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 333–342, New York, NY, USA, 2009. ACM.

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 187–196, New York, NY, USA, 2008. ACM.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes and cryptography. In *STOC '05*, pages 84–93. ACM, 2005.

[RS91] Charles Rackoff and Daniel Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *CRYPTO '91*, pages 433–444, 1991.

[RS08] Alon Rosen and Gil Segev. Efficient lossy trapdoor functions based on the composite residuosity assumption. Cryptology ePrint Archive, Report 2008/134, 2008.

[RS09] Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. In *TCC '09: Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*, pages 419–436, Berlin, Heidelberg, 2009. Springer-Verlag.