Extended-DDH and Lossy Trapdoor Functions

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

[1] University of Michigan
[2] UCLA

Abstract. Lossy Trapdoor Functions (LTFs) were introduced by Peikert and Waters in STOC '08 and since then have found many applications and have proven to be an extremely useful and versatile cryptographic primitive. Lossy trapdoor functions were used to build the first injective trapdoor functions based on DDH, the first IND-CCA cryptosystems based on lattice assumptions, and they are known to imply deterministic encryption, collision resistant hash-functions, oblivious transfer and a host of other important primitives. While LTFs can be instantiated under most known cryptographic hardness assumptions, no constructions until today existed based on generic cryptographic primitives. In this work, we show that any Homomorphic Smooth Hash Proof System, introduced by Cramer and Shoup in EUROCRYPT '02, can be used to construct LTFs. In addition to providing a connection between two important cryptographic primitives – our construction implies the first construction of LTFs based on the QR assumption.

Smooth Hash Proof Systems (SHPs) can be seen as a generalization of the DDH assumption, yet can be built on other cryptographic assumptions, such as the DCR or QR assumptions. Yet, until today, a "translation" of results proven secure under DDH to results under DCR or QR has always been fraught with difficulties. Thus, as our second goal of this paper, we ask the following question: is it possible to streamline such translations from DDH to QR and other primitives? Our second result formally provides this connection. More specifically, we define an Extended Decisional Diffie Hellman (EDDH) assumption, which is a simple and natural generalization of DDH. We show that EDDH can be instantiated under both the DCR and QR assumptions. This gives a much simpler connection between the DDH and the DCR and QR assumptions

⋆ bhemen@umich.edu

⋆⋆ 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.

and provides an easy way to translate proofs from DDH to DCR or QR. That is, the advantage of the EDDH assumption is that most schemes (including LTFs) proven secure under the DDH assumption can easily be instantiated under the DCR and QR assumptions with almost no change to their proofs of security.

1 Introduction

The first practical IND-CCA secure cryptosystem was built by Cramer and Shoup under the Decisional Diffie-Hellman (DDH) assumption [CS98]. In a follow up work, Cramer and Shoup introduced projective hash proofs as a means of generalizing their original DDH-based construction [CS02]. This generalization allowed them to create unified constructions of IND-CCA secure cryptosystems based on Paillier's Decisional Composite Residuosity (DCR) assumption and the Quadratic Residuosity (QR) assumption.

Since their introduction, projective hash proof systems have proven to be an effective tool for generalizing constructions that were originally proven secure under the DDH assumption. Indeed, many important results use the framework of projective hash proofs to take a system built using the DDH assumption and instantiate it using the DCR or QR assumptions.

Cramer and Shoup [CS02] converted the DDH-based construction of IND-CCA encryption [CS98] to one based on the DCR or QR assumptions. Kalai and Halevi [Kal05,HK07] converted the DDH-based construction of OT given by Naor and Pinkas [NP01] to one based on the DCR or QR assumptions. Brakerski and Goldwasser [BG10] converted the DDH-based construction of circular secure encryption given by Boneh, Halevi, Hamburg and Ostrovsky [BHHO08] to one based on the DCR or QR assumptions[3].

This series of works generalizing DDH-based constructions suggests the heuristic that "anything that can be done with DDH can be done with DCR or QR." Like any heuristic it is not completely accurate, but it appears to provide the right intuition.

While projective hash proof systems suggest a means for converting a DDH-based scheme to a DCR or QR based scheme, the generality of projective hash proof systems framework often means that converting the actual proofs of security can be fairly technical. This is evidenced in the works of [CS02,Kal05,HK07,BG10] which provided significant technical contributions beyond the original constructions of [CS98,NP01,BHHO08].

This work makes two contributions: First, we show that Lossy Trapdoor Functions (LTFs) of Peikert and Waters [PW08] can be built under general assumptions, namely any homomorphic smooth hash proof system. This provides a connection between two important cryptographic primitives. Second, we introduce the *Extended Decisional Diffie-Hellman (EDDH)* assumption, and show how it can be instantiated using the DCR and QR assumptions. This second

[3] Brakerski and Goldwasser did not explicitly use the language of projective hash proofs, but their construction fits the framework exactly.

result provides a justification for the heuristic noted above that the DCR and QR assumptions "imply" the DDH assumption. While the EDDH assumption does not appear to be as general as the notion of projective hash proof systems, its simplicity gives it some advantages. In particular, the EDDH assumption provides a much simpler method for identifying which DDH-based constructions can be instantiated under the DCR or QR assumptions, and proofs of security under the EDDH assumption are almost identical to those under the DDH assumption. Using the framework of EDDH, it becomes almost immediate that the DDH constructions of [NP01,BHHO08,PW08] can be instantiated under the DCR or QR assumptions with almost no modifications to the proofs of security.

As mentioned above, our first result is a construction of lossy trapdoor functions (LTFs) from general assumptions. Lossy trapdoor functions were introduced by Peikert and Waters [PW08]. LTFs provided the first injective trapdoor functions based on the Decisional Diffie-Hellman (DDH) assumption, and the first chosen ciphertext (IND-CCA) secure cryptosystem based on lattice assumptions. In addition to providing natural constructions of injective trapdoor functions and IND-CCA secure cryptosystems, Peikert and Waters went on to show that LTFs provide very natural constructions of many cryptographic primitives, including pseudo-random generators, collision-resistant hash functions, and oblivious transfer. The extremely intuitive nature of these many constructions provided early evidence of the value of LTFs as a cryptographic primitive. Since the original work of Peikert and Waters, lossy trapdoor functions have been shown to imply many other important cryptographic primitives. In [BFO08], Boldyreva, Fehr and O'Neill showed that LTFs imply deterministic encryption. Deterministic encryption was introduced in [BBO07], and captures the strongest notion of security possible for a deterministic function. In contrast to one-way functions, which do leak the parity of a random subset of the bits of its input [GL89], deterministic encryption does not leak *any fixed function*[4] of its input. Deterministic encryption has applications to efficiently searchable encryption, and securing legacy systems. Lossy trapdoor functions were then shown to imply correlated product secure functions by Rosen and Segev in [RS09]. Roughly a family of correlated product secure functions is a family of functions that remain one-way even when the output of multiple functions is given *on the same input*. In [MY09], Mol and Yilek introduced a relaxation of lossy trapdoor functions called *slightly lossy trapdoor functions*, and showed that even slightly lossy trapdoor functions are sufficient to achieve correlated product secure functions. Lossy functions, (without the need for a trapdoor) have been shown to imply leaky pseudo-entropy functions [BHK11].

Lossy trapdoor functions have been constructed from a variety of concrete hardness assumptions. In [PW08], Peikert and Waters constructed LTFs from the DDH assumption and lattice assumptions, and an efficient construction of LTFs from Paillier's Decisional Composite Residuosity (DCR) assumption was given independently in [BFO08] and [RS08]. In concurrent, independent work, Freeman

[4] independent of the choice of the key for the deterministic encryption.

et al. [FGK+10] give constructions of LTFs from the D-Linear Assumption and constructions of slightly lossy trapdoor functions from the QR assumption.

While we have seen a wide variety of important consequences of lossy trapdoor functions, there remains a lack of general constructions. This work provides the first constructions of LTFs from generic primitives (in this case homomorphic smooth hash proof systems, and diverse group systems) as well as the first construction of fully lossy trapdoor functions from the well-known Quadratic Residuosity (QR) assumption.

This result has a number of other consequences. Applying our construction to the results of [BFO08], we achieve the first construction of deterministic encryption from smooth homomorphic hash proof systems. Applying our results to those of [RS09], we give the only known construction of correlated product secure functions from a generic primitive other than lossy trapdoor functions,[5] and the first known construction of correlated product secure functions from the QR assumption.[6] Applying the separation of Rosen and Segev, we provide a black-box separation of smooth homomorphic hash proof systems and one-way trapdoor permutations.

The second contribution of this work is a development of the connection between the DDH, DCR and QR assumptions. Projective hash proof systems [CS02] showed that many properties of DDH-based protocols could be achieved using the DCR or QR assumptions. In this work, we introduce the Extended DDH (EDDH) assumption, and show how the EDDH assumption is implied by the DDH, DCR and QR assumptions. One formulation of the DDH assumption is that the distributions $\{g, g^a, g^b, g^{ab}\}$, $\{g, g^a, g^b, g^c\}$ are computationally indistinguishable. Equivalently, $\{g, g^a, g^b, g^{ab}\} \approx_c \{g, g^a, g^b, g^{ab}r\}$ for some uniformly chosen element r in the group. The EDDH assumption is the same, except that r is chosen from a subgroup instead of the entire group. Thus the EDDH assumption states that $\{g, g^a, g^b, g^{ab}\}$ and $\{g, g^a, g^b, g^{ab}r\}$ are computationally indistinguishable when r is chosen uniformly from a given subgroup of the universe group. See Definition 6 for the formal definition. The value of the EDDH assumption is that it provides a very simple method for converting constructions based on the DDH assumption into constructions which can be proven secure under the DCR or QR assumptions. Since the semantics of the EDDH assumption are very similar to those of the DDH assumption in many cases proofs of security under the DDH assumption go through almost unchanged under the EDDH assumption.

[5] There are two concrete constructions of correlated product secure functions that are not lossy trapdoor functions. A construction based on the Learning With Error (LWE) problem given by Peikert in [Pei09], and a construction based on the hardness of syndrome decoding given by Freeman et al. in [FGK+10].

[6] A completely different construction of correlated product secure functions from the QR assumption is given in the concurrent, independent work of Freeman et al. [FGK+10].

1.1 Previous Work

Lossy Trapdoor Functions (LTFs) were introduced by Peikert and Waters in [PW08], simultaneously providing the first construction of one-way trapdoor functions from the Decisional Diffie Hellman and the first IND-CCA secure cryptosystem based on lattice assumptions.

Roughly, a family of lossy trapdoor functions is a family of functions with two computationally indistinguishable branches. An injective branch with a trapdoor, and a lossy branch which statistically loses information about its input, in particular the image size of the lossy branch is required to be much smaller than its domain size. If the lossy branch is lossy enough, this immediately implies that the injective branch is an injective one-way trapdoor function. Peikert and Waters gave constructions of lossy trapdoor functions from the DDH assumption and lattice-based assumptions. In [BFO08], [RS08], Boldyreva et al. and Rosen and Segev gave efficient constructions of lossy trapdoor functions from Paillier's DCR assumption. A construction of lossy trapdoor functions from the D-Linear assumption, and slightly lossy trapdoor functions from the QR assumption are given in the concurrent, independent work of [FGK$^+$10].

Lossy trapdoor functions are known to imply IND-CCA secure encryption. In addition to IND-CCA secure encryption, LTFs were shown to imply collision-resistant hash functions [PW08], deterministic encryption [BFO08], lossy encryption [PVW08] and correlated product secure functions [RS09].

Projective Hash Proof Systems were introduced by Cramer and Shoup in [CS02], generalizing their construction of IND-CCA encryption from the Decisional Diffie-Hellman (DDH) assumption given in [CS98]. In [CS02], Cramer and Shoup defined two types of hash proof systems, smooth projective hash families, which immediately implied IND-CPA secure encryption, and universal hash families, which could be used as a type of designated verifier proof system for the specific class of language given by smooth projective hash families. They went on to show that universal hash proof systems imply smooth projective hash proof systems, so it was sufficient to construct only universal hash proof systems. Their general construction, however, was fairly inefficient, and in all of their constructions they were able to avoid the general construction of smooth projective hash proof systems, and create efficient smooth projective hash proof systems directly. In this work, we will deal only with smooth projective hash proof systems.

In order to construct explicit hash proof systems, Cramer and Shoup defined another primitive called a *Diverse Group System*. Diverse Group Systems seemed to capture the essential part of the algebraic structure of a cyclic group, and they gave a very natural construction of projective hash proof systems from Diverse Group Systems. They went on to construct diverse group systems from the DDH assumption, the Quadratic Residuosity (QR) assumption and the Decisional Composite Residuosity (DCR) assumption.

The first result of this work is a proof that smooth homomorphic hash proof systems imply lossy trapdoor functions. By providing a link between smooth homomorphic hash proof systems, and lossy trapdoor functions, we provide a

number of new connections as well. This work provides the first construction of lossy trapdoor functions from a generic primitive. Additionally, it provides the first construction of deterministic encryption from smooth homomorphic projective hash proof systems.

Our first result uses the framework of smooth projective hashing to generalize the DDH-based construction of LTFs from [PW08]. Smooth projective hash proof systems have been used to generalize DDH-based constructions in the past. Kalai and Halevi [Kal05,HK07] used them to generalize Naor and Pinkas's OT protocol [NP01], and Brakerski and Goldwasser [BG10] generalized the circular secure encryption of Boneh, Halevi, Hamburg and Ostrovsky [BHHO08] using the same framework. This series of results indicates a close relationship between the DDH, DCR and QR assumptions.

The second result of this work is a development of the connection between the DDH, DCR and QR assumptions. One of the most useful features of projective hash proof systems is that they provide a framework for converting cryptographic schemes designed under the DDH assumption into cryptographic schemes that are provably secure under the DCR or QR assumptions. While projective hash proof systems showed a close connection between the DDH, DCR and QR assumptions, generality of projective hash proof systems makes this connection difficult to see. To make the connection between these three hardness assumptions clearer, we introduce the EDDH assumption and show how it can be realized under the DCR and QR assumptions. The benefit of the EDDH assumption is that it is semantically very similar to the DDH assumption, so many existing constructions whose security rests on the DDH assumption (including the construction of LTFs by Peikert and Waters) can immediately be instantiated under the DCR or QR assumptions. In particular, we note that the proof of [PW08] can be instantiated using the EDDH assumption. This gives a novel construction of LTFs from the DCR assumption and the first construction of LTFs from the QR assumption.

1.2 Our Contributions

In this work, we show that smooth homomorphic hash proof systems imply lossy trapdoor functions (LTFs). It was shown in [BFO08] that lossy trapdoor functions imply deterministic encryption, so our results give the first construction of deterministic encryption from smooth homomorphic hash proof systems.

In [RS09], Rosen and Segev introduced correlated product secure functions, and showed that lossy trapdoor functions are correlated product secure. Applying their results to our construction, we have a construction of correlated product secure functions from smooth homomorphic hash proof systems. Finally, combining our results with the black-box separations of Rosen and Segev [RS09], we find that there is a black-box separation between one-way trapdoor permutations and smooth homomorphic hash proof systems.

Our primary results are summarized as follows:

Theorem. *Smooth Homomorphic Projective Hash Proof Systems imply Lossy Trapdoor Functions.*

This theorem has a number of immediate Corollaries. Since Boldyreva et al. [BFO08] showed that LTFs imply deterministic encryption (as defined in [BBO07]), we have

Corollary. *Smooth Homomorphic Projective Hash Proof Systems imply deterministic encryption.*

Since Rosen and Segev [RS09] showed that LTFs imply correlated product secure encryption, and a black-box separation between one-way trapdoor permutations and lossy trapdoor functions, we have

Corollary. *Smooth Homomorphic Projective Hash Proof Systems imply correlated product secure functions.*

Corollary. *There is a black-box separation between Smooth Homomorphic Projective Hash Proof Systems and one-way trapdoor permutations, i.e. there exists an oracle, relative to which the latter exists but the former does not.*

In addition to the new constructions outlined above, in Section 4 we introduce the Extended Decisional Diffie Hellman (EDDH) assumption, which provides a simple way to achieve a DDH-like property under the DCR and QR assumptions. This serves to unify many of the previous constructions (e.g. [NP01] and [Kal05,HK07], [BHHO08] and [BG10]), and provides a more familiar alternative to projective hash proof systems.

Applying these results yields lossy trapdoor functions from the DDH, DCR and QR assumptions. When applied to DDH, the construction achieved in this way is identical to the construction of LTFs given by Peikert and Waters in [PW08], however the constructions from the DCR and QR assumptions are new. While our construction of LTFs from the DCR assumption is less efficient than that given by [BFO08] and [RS08], our results provide the first construction of lossy trapdoor functions from the QR assumption.

2 Preliminaries

2.1 Notation

If A is a Probabilistic Polynomial Time (PPT) machine, then we use $a \xleftarrow{\$} A$ 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, we use $r \xleftarrow{\$} R$ to denote sampling uniformly from R.

We use the notation

$$\Pr[r \xleftarrow{\$} R; x \xleftarrow{\$} X : A(x, r) = c],$$

to denote the probability that A outputs c when x is sampled uniformly from X and r is sampled uniformly from R. We define the statistical distance between two distributions X, Y to be

$$\Delta(X, Y) = \frac{1}{2} \sum_x |\Pr[X = x] - \Pr[Y = x]|$$

If X and Y are families of distributions indexed by a security parameter λ, we use $X \approx_s Y$ to mean the distributions X and Y are statistically close, *i.e.*, for all polynomials p and sufficiently large λ, we have $\Delta(X,Y) < \frac{1}{p(\lambda)}$. We use $X \approx_c Y$ to mean X and Y are computationally close, *i.e.*, for all PPT adversaries A, for all polynomials p, then for all sufficiently large λ, we have $|\Pr[A^X = 1] - \Pr[A^Y = 1]| < 1/p(\lambda)$.

2.2 Lossy Trapdoor Functions

We briefly recall the definition of lossy trapdoor functions given in [PW08].

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

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

2.3 Subset Membership Problems

In this section we recall the definition of of a subset membership problem as formalized in [CS02]. Roughly, given sets $L \subset X$, we want L and X to be computationally indistinguishable.

Formally, given a family of sets (X, L, W) indexed by a security parameter λ, we require $L \subset X$, and there is a binary relation $\mathcal{R} : X \times W \to \{0,1\}$. If $\mathcal{R}(x,w) = 1$, we say that w is a witness for x. In this work, we will restrict our attention to relations $\mathcal{R}$ such that for all $x \in L$, there exists a $w \in W$ such that $\mathcal{R}(x,w) = 1$, and for all $x \notin L$, and all $w \in W$, $\mathcal{R}(x,w) = 0$.

We also need the following efficient sampling algorithms.

- **Instance Sampling:** Given a security parameter λ, we can sample (X, L, W) and $\mathcal{R}$.
- **Sampling Without Witness:** Given (X, L, W) we can sample (statistically-close to) uniformly on X.
- **Sampling With Witness:** Given (X, L, W) we can sample x (statistically-close to) uniformly on L, along with a witness w such that $\mathcal{R}(x,w) = 1$.

Definition 1. *A subset membership problem is called* hard *if for all PPT distinguishers,*

$$|\Pr[x \xleftarrow{\$} X : D(x) = 1] - \Pr[x \xleftarrow{\$} L : D(x) = 1]| < \nu(\lambda),$$

for some negligible function ν.

As in [CS02], the security of all of our constructions will rely on the security of some underlying hard subset membership problem. In fact, the hardness assumptions DDH, DCR and QR all have natural formulations in terms of hard subset membership problems [CS02].

2.4 Smooth Hash Proof Systems

We briefly recall the notion of *smooth projective hash* families as defined by Cramer and Shoup in [CS02]. Let H be a function family indexed by keys in the a keyspace K, *i.e.* for each $k \in K$, $H_k : X \to \Pi$. Let $L \subset X$ and a "projection" $\alpha : K \to S$. We require efficient evaluation algorithms such that, for any $x \in X$, $H_k(x)$ is efficiently computable using $k \in K$. Using the terminology of [CS02], this is called the *private evaluation algorithm*. Finally we require efficient sampling algorithms to sample uniformly from X, uniformly from K, and uniformly from L *along with a witness*. The security properties of the system will follow from the indistinguishability of X and L.

Definition 2. *The set* $\mathsf{HPS} = (H, K, X, L, \Pi, S, \alpha)$ *is a* projective hash family *if, for all* $k \in K$*, the action of* H_k *on the subset* L *is completely determined by* $\alpha(k)$*.*

For a projective hash family, $\alpha(k)$ determines the output of H_k on L. Additionally, if $x \in L$ and a witness w for $x \in L$ is known, then we require that $H_k(x)$ is efficiently computable given $x, w, \alpha(k)$. This is called the *public evaluation algorithm*. A *smooth* projective hash family is one in which α does not encode any information about the action of H_k on $X \setminus L$.

Definition 3. *Let* $(H, K, X, L, \Pi, S, \alpha)$ *be a projective hash family, and define two distributions* Z_1, Z_2 *taking values on the set* $X \setminus L \times S \times \Pi$*. For* Z_1*, we sample* $k \xleftarrow{\$} K$*,* $x \xleftarrow{\$} X \setminus L$*, and set* $s = \alpha(k)$*,* $\pi = H_k(x)$*, for* Z_2 *we sample* $k \xleftarrow{\$} K$*,* $x \xleftarrow{\$} X \setminus L$*, and* $\pi \xleftarrow{\$} \Pi$*, and set* $s = \alpha(k)$*. The projective hash family is called* ν-smooth *if* $\Delta(Z_1, Z_2) < \nu$*.*

This means that, given $\alpha(k)$ and $x \in X \setminus L$, $H_k(x)$ is statistically close to uniform on Π.

In [CS02], they showed that smooth projective hash families immediately imply IND-CPA secure encryption by taking $sk = k$, $pk = \alpha(k)$, and to encrypt a message $m \in \Pi$, we sample $x \in L$ along with randomness and output $E(m) = (x, H_k(x) + m)$.

We extend the definition of smooth projective hash proof systems slightly

Definition 4. *If* $\mathsf{HPS} = (H, K, X, L, \Pi, S, \alpha)$ *is a projective hash family, we say that* HPS *is a* homomorphic projective hash family *if* X *is a group, and for all* $k \in K$*, and* $x_1, x_2 \in X$*, we have* $H_k(x_1) + H_k(x_2) = H_k(x_1 + x_2)$*, that is to say* H_k *is a homomorphism for each* k*.*

In [CS02] Cramer and Shoup provide smooth homomorphic projective hash families based on the DDH, DCR and QR assumptions.

3 Lossy Trapdoor Functions from Smooth Homomorphic Hash Proof Systems

Peikert and Waters [PW08] gave a construction of lossy trapdoor functions from the Decisional Diffie-Hellman (DDH) assumption. In this section, we show that a similar construction goes through with smooth homomorphic hash proof systems. This extends the intuition given in [CS02] that projective hashing provides a good generalization of the DDH assumption. We note, however, that although our construction is very similar that of [PW08], the proofs of security are quite different.

Let (X, L, W) be a hard subset membership problem. For notational convenience, we suppress the dependence on the security parameter λ. Let $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ be an associated smooth homomorphic projective hash family.

- **Key Generation:**
  Pick $x_1, \ldots, x_n \in L$.
  Fix $b \in \Pi \setminus \{0\}$.
  Generate the matrix $B = (B_{ij}) \subset \Pi^{n \times n}$, where $B_{ij} = 0$ if $i \neq j$, and
  In lossy mode $B_{ii} = 0$ for all i.
  In injective mode $B_{ii} = b$.

  Sample $k_1, \ldots, k_n \leftarrow K$, and output

$$R = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad A = \begin{pmatrix} H_{k_1}(x_1) + B_{11} & \cdots & H_{k_1}(x_n) + B_{1n} \\ \vdots & \ddots & \vdots \\ H_{k_n}(x_1) + B_{n1} & \cdots & H_{k_n}(x_n) + B_{nn} \end{pmatrix}$$

  The trapdoor will be $(k_1, \ldots, k_n)$.
- **Evaluation:**
  Given a message $z = z_1, \ldots, z_n \in \{0,1\}^n$
  Given a function index R, A, calculate

$$F_{R,A}(z) = (Rz, Az) = \left(\sum_{i=1}^{n} z_i x_i, \begin{pmatrix} \sum_{i=1}^{n} z_i (H_{k_1}(x_i) + B_{1i}) \\ \vdots \\ \sum_{i=1}^{n} z_i (H_{k_n}(x_i) + B_{ni}) \end{pmatrix} \right).$$

- **Trapdoor:**
  Given a value (Rz, Az), and a trapdoor $(k_1, \ldots, k_n)$, we begin by noting that the homomorphic property of H_k guarantees that

$$F_{R,A}(z) = (Rz, Az) = \left(\sum_{i=1}^{n} z_i x_i, \begin{pmatrix} \sum_{i=1}^{n} z_i (H_{k_1}(x_i) + B_{1i}) \\ \vdots \\ \sum_{i=1}^{n} z_i (H_{k_n}(x_i) + B_{ni}) \end{pmatrix} \right)$$

$$= \left(\sum_{i=1}^{n} z_i x_i, \begin{pmatrix} H_{k_1}\left(\sum_{i=1}^{n} z_i x_i\right) + \sum_{i=1}^{n} z_i B_{1i}) \\ \vdots \\ H_{k_n}\left(\sum_{i=1}^{n} z_i x_i\right) + \sum_{i=1}^{n} z_i B_{ni}) \end{pmatrix} \right)$$

Since $\sum_{i=1}^{n} z_i x_i$, and k_i is known, we can calculate $H_{k_i}\left(\sum_{i=1}^{n} z_i x_i\right)$ and subtract it from each component to recover the vector

$$\left(\sum_{i=1}^{n} z_i B_{1i}, \cdots, \sum_{i=1}^{n} z_i B_{ni} \right)^t .$$

Now, in injective mode, $B_{ij} = 0 \in \Pi$ for $i \neq j$, and $B_{ij} = b$ for $i = j$, so

$$\left(\sum_{i=1}^{n} z_i B_{1i}, \cdots, \sum_{i=1}^{n} z_i B_{ni} \right)^t = (z_1 b, \cdots, z_n b) .$$

Since the $z_i \in \{0, 1\}$, and since b is known, we can recover the z_i by inspection.

Remark: Notice that we do not make use of the projection α in our construction, it will appear, however, in the proof of security. Unlike in [CS02], we do not require that α be efficiently computable, merely that it exists.

We now examine the security of this construction.

Lemma 1. *In Lossy Mode, the image of F has size at most $|X|$.*

Proof. Notice that in Lossy Mode, since $B_{ij} = 0$ for all i, j,

$$F_{R,A}(z) = \left(\sum_{i=1}^{n} z_i x_i, \begin{pmatrix} H_{k_1}\left(\sum_{i=1}^{n} z_i x_i\right)) \\ \vdots \\ H_{k_n}\left(\sum_{i=1}^{n} z_i x_i\right)) \end{pmatrix} \right)$$

which depends only on the sum $\sum_{i=1}^{n} z_i x_i \in X$. Thus the size of the image is bounded by $|X|$.

Thus by taking $n > \log(|X|)$, we can make the lossy mode of F as lossy as desired.

Lemma 2. *The Injective and Lossy Modes are computationally indistinguishable.*

The proof can be found in the full version of this work. We remark that this construction *does not* make use of the projection α. The projective property *is* used, however, since we condition on $H_k(x)$ for $x \in L$, which leaves at least as much entropy in k as conditioning on $\alpha(k)$, since $\alpha(k)$ determines $H_k(x)$.

A similar construction and proof goes through for Diverse Group Systems (see the full version of this work for details). Thus we arrive at

Theorem 1. *Smooth Homomorphic Projective Hash Proof Systems imply Lossy Trapdoor Functions, and Diverse Group Systems imply Lossy Trapdoor Functions.*

This theorem has a number of immediate Corollaries. Since Boldyreva et al. [BFO08] showed that LTFs imply deterministic encryption (as defined in [BBO07]), we have Corollary 1. Since Rosen and Segev [RS09] showed that LTFs imply correlated product secure encryption, we have Corollary 2. Since Rosen and Segev showed a black-box separation between one-way trapdoor permutations and lossy trapdoor functions, we have Corollary 3.

Corollary 1. *Smooth Homomorphic Projective Hash Proof Systems imply deterministic encryption.*

Corollary 2. *Smooth Homomorphic Projective Hash Proof Systems imply correlated product secure functions.*

Corollary 3. *There is a black-box separation between Smooth Homomorphic Projective Hash Proof Systems and one-way trapdoor permutations, i.e. there exists an oracle, relative to which the latter exists but the former does not.*

4 The Extended DDH Assumption

In this section, we introduce the Extended Decisional Diffie Hellman (EDDH) assumption. Let $\mathbb{G}$ be commutative group (written multiplicatively). The DDH assumption states that

Definition 5 (The DDH Assumption). *Assume $\mathbb{G}$ is a group with an efficient sampling algorithm, and $K = \{1, \ldots, |\mathbb{G}|\}$. Then the DDH assumption states that*

$$\{(g, g^a, g^b, g^{ab}) : g \xleftarrow{\$} G, a, b \xleftarrow{\$} K\} \approx_c \{(g, g^a, g^b, g^c) : g \xleftarrow{\$} G, a, b, c \xleftarrow{\$} K, \}$$

When $\mathbb{G}$ is a cyclic group, this can be rephrased as

$$\{(g, g^a, g^b, g^{ab}) : g \xleftarrow{\$} G, a, b \xleftarrow{\$} K\} \approx_c \{(g, g^a, g^b, g^{ab}h) : g \xleftarrow{\$} G, a, b \xleftarrow{\$} K, h \xleftarrow{\$} \mathbb{G}\}$$

We introduce a slight modification of the DDH assumption, called the *Extended Decisional Diffie Hellman (EDDH)* assumption.

Definition 6 (The EDDH Assumption). *For a group $\mathbb{G}$, and a (samplable) subgroup $\mathbb{H} \triangleleft \mathbb{G}$, the* extended decisional diffie hellman (EDDH) *problem is said to be hard if there exists a samplable set $G \subset \mathbb{G}$ and samplable sets $K \subset \mathbb{Z}$ such that the following two distributions are computationally indistinguishable:*

$$\{(g, g^a, g^b, g^{ab}) : g \xleftarrow{\$} G, a, b \xleftarrow{\$} K\} \approx_c \{(g, g^a, g^b, g^{ab}h) : g \xleftarrow{\$} G, a, b \xleftarrow{\$} K, h \xleftarrow{\$} \mathbb{H}\}$$

It is not hard to see:

Lemma 3. *If $K = \{1, \ldots, |\mathbb{G}|\}$, and $\mathbb{H} = \mathbb{G}$, then the EDDH assumption is just the DDH assumption in the group $\mathbb{G}$.*

The utility of this assumption is that it extracts the essential properties of the DDH assumption, yet it can be instantiated under the QR assumption and the DCR assumption. See the full version of this work for example applications of the EDDH assumption.

We begin by showing that the DCR assumption [Pai99] implies the EDDH assumption.

Theorem 2 (DCR implies EDDH). *Let p, q be safe primes*[7] *and define:*

- $N = pq$,
- $\mathbb{G} = \{x : x \xleftarrow{\$} \mathbb{Z}^*_{N^2}, \left(\frac{x}{N}\right) = 1\}$,
- $G = \{g^{2N} \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\}$,
- $K = \{0, \ldots, \lfloor N^2/4 \rfloor\} = \{0, \ldots, (N^2-1)/4\}$,
- $\mathbb{H} = \{(1+aN) : a \in \mathbb{Z}_N\} = \{(1+N)^a \mod N^2 : a \in \mathbb{Z}_N\}$.

Then under the DCR assumption the EDDH assumption is hard in the group $\mathbb{G}$.

Proof. Define the following distributions Let $\hat{G} = \{g^{2N}(1+N) \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\}$.

$$\begin{aligned}
\Lambda_1 &= \{(g, g^a, g^b, g^{ab}) : g \xleftarrow{\$} G, a \xleftarrow{\$} K, b \xleftarrow{\$} K\} \\
\Lambda_2 &= \{(g, x, g^b, x^b) : g \xleftarrow{\$} G, x \xleftarrow{\$} \hat{G}, b \xleftarrow{\$} K\} \\
\Lambda_3 &= \{(g, x, g^b, x^b h) : g \xleftarrow{\$} G, x \xleftarrow{\$} \hat{G}, b \xleftarrow{\$} K, h \xleftarrow{\$} \mathbb{H}\} \\
\Lambda_4 &= \{(g, g^a, g^b, g^b h) : g \xleftarrow{\$} G, a \xleftarrow{\$} K, b \xleftarrow{\$} K, h \xleftarrow{\$} \mathbb{H}\}
\end{aligned}$$

1. The DCR assumption says $\{g^2 \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\} \approx_c \{g^{2N} \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\}$. Thus

$$\begin{aligned}
G &= \{g^{2N} \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\} \\
&\approx_c \{g^2 \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\} \\
&= \{g^2(1+N) \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\} \\
&\approx_c \{g^{2N}(1+N) \mod N^2 : g \xleftarrow{\$} \mathbb{Z}_{N^2}\} \\
&= \hat{G}.
\end{aligned}$$

Now, notice that for a fixed generator g of G,

$$\{g^a \mod N^2 : a \xleftarrow{\$} K\} \approx_s \{g^a \mod N^2 : a \xleftarrow{\$} \{0, 1, \ldots, \varphi(N)/4\}\} \approx_s G$$

[7] Choosing p, q safe primes makes the analysis slightly simpler. See the full version of this work for a complete discussion.

(See the full version of this work for a rigorous proof of this fact). We also know that with all but negligible probability a uniformly chosen element $g \xleftarrow{\$} G$ will be a generator for G, so this implies $\Lambda_1 \approx_c \Lambda_2$.

2. If $x = g_1^{2N}(1+N)$, then $x^b = g_1^{2Nb}(1+N)^b = g_1^{2N(b \mod N\varphi(N)/4)}(1+N)^{b \mod N} \mod N^2$. Since the distribution of b is statistically close to uniform modulo $N\varphi(N)/4$, we have that b is statistically close to uniform modulo N even conditioned on any value of b modulo $\varphi(N)/4$. Since the order of g is $\varphi(N)/4$, the distribution of b modulo N is statistically close to uniform conditioned on g^b. Thus, even conditioned on g^b, the distribution of x^b is statistically close to $g_1 h$ where $g_1 \xleftarrow{\$} G$, and $h \xleftarrow{\$} \mathbb{H}$, which shows $\{(g, x, g^b, x^b)\} \approx_s \{(g, x, g^b, x^b h)\}$. Thus $\Lambda_2 \approx_s \Lambda_3$.
3. We have already observed that $G \approx_c \hat{G}$, so $\Lambda_3 \approx_c \Lambda_4$.

It is standard to conserve randomness by sampling $a \xleftarrow{\$} \{0, \ldots, (N-1)/4\}$, and $b \xleftarrow{\$} \{0, \ldots, (N^2-1)/4\}$. It is easy to see that security is preserved in this case as well. Since the exposition is cleaner if they are sampled from the same space, and a few DDH applications require it, our scheme samples them from the same larger space.

Next, we show that the QR assumption implies the EDDH assumption.

Theorem 3 (QR Implies EDDH). *Let p, q be safe primes with $p = q = 3 \mod 4$, and define:*

- $N = pq$,
- $\mathbb{G} = \{x : x \xleftarrow{\$} \mathbb{Z}_N^*, \left(\frac{x}{N}\right) = 1\}$,
- $G = \{g^2 \mod N : g \xleftarrow{\$} \mathbb{Z}_N\}$,
- $K = \{0, \ldots, \lfloor N/2 \rfloor\}$,
- $\mathbb{H} = \{\pm 1\}$.

Then under the QR assumption the EDDH assumption is hard in the group $\mathbb{G}$.

Proof. Since $p = q = 3 \mod 4$, -1 is a quadratic non-residue modulo N with jacobi symbol 1.

Define the following distributions

$$\Lambda_1 = \{(g, g^a, g^b, g^{ab}) : g \xleftarrow{\$} G, a \xleftarrow{\$} K, b \xleftarrow{\$} K\}$$
$$\Lambda_2 = \{(g, x, g^b, x^b) : g \xleftarrow{\$} G, x \xleftarrow{\$} \mathbb{G}, b \xleftarrow{\$} K\}$$
$$\Lambda_3 = \{(g, x, g^b, x^b h) : g \xleftarrow{\$} G, x \xleftarrow{\$} \mathbb{G}, b \xleftarrow{\$} K, h \xleftarrow{\$} \mathbb{H}\}$$
$$\Lambda_4 = \{(g, g^a, g^b, g^b h) : g \xleftarrow{\$} G, a \xleftarrow{\$} K, b \xleftarrow{\$} K, h \xleftarrow{\$} \mathbb{H}\}$$

1. The QR assumption says

$$\mathbb{G} = \{x : x \xleftarrow{\$} \mathbb{Z}_N^*, \left(\frac{x}{N}\right) = 1\} \approx_c \{g^2 \mod N : g \xleftarrow{\$} \mathbb{Z}_N\} = G$$

   Now, notice that for a fixed generator g of G,

$$\{g^a \mod N : a \xleftarrow{\$} K\} \approx_s \{g^a \mod N : a \xleftarrow{\$} \{0, 1, \ldots, \varphi(N)/4\}\} \approx_s G$$

   (See the full version for a rigorous proof of this fact.) We also know that with all but negligible probability a uniformly chosen element $g \xleftarrow{\$} G$ will be a generator for G, so this implies $\Lambda_1 \approx_c \Lambda_2$.
2. If $x = -g_1^2$, then $x^b = g_1^{2b}(-1)^b = g_1^{2(b \mod \varphi(N)/4)}(-1)^{b \mod 2} \mod N$. Since the distribution of b is statistically close to uniform modulo $\varphi(N)/2$, we have that b is statistically close to uniform modulo 2 even conditioned on any value of b modulo $\varphi(N)/4$. Since the order of g is $\varphi(N)/4$, the distribution of b modulo 2 is statistically close to uniform conditioned on g^b. Thus, even conditioned on g^b, the distribution of x^b is statistically close to $g_1 h$ where $g_1 \xleftarrow{\$} G$, and $h \xleftarrow{\$} \{\pm 1\}$, which shows $\{(g, x, g^b, x^b)\} \approx_s \{(g, x, g^b, x^b h)\}$. Thus $\Lambda_2 \approx_s \Lambda_3$.
3. We have already observed that $G \approx_c \mathbb{G}$, so $\Lambda_3 \approx_c \Lambda_4$.

As in the case of the DCR based schemes, it is standard to conserve randomness by sampling a from a smaller space than b. In particular, we can sample $a \xleftarrow{\$} \{0, \ldots, (N-1)/4\}$, and $b \xleftarrow{\$} \{0, \ldots, (N^2-1)/4\}$. For the reasons outlined above we present this simpler (though slightly less efficient) variant.

It is not too hard to see that the construction of LTFs given by Peikert and Waters in [PW08] carries through under the EDDH assumption. This immediately gives new constructions of LTFs based on the QR assumption and the DCR assumption. See the full version of this work for details.

This provides the first construction of full LTFs from the QR assumption, and a novel construction of LTFs from the DCR assumption.

5 Conclusion

In this work, we showed that the intuition that hash proof systems are a natural generalization of the Decisional Diffie-Hellman (DDH) assumption holds in the case of lossy trapdoor functions as well. In particular, we showed that the construction of lossy trapdoor functions from DDH given in [PW08] can be made to work with any smooth homomorphic projective hash (or any diverse group system). This shows an interesting connection between these two powerful primitives and provides the first generic[8] construction of lossy trapdoor functions from *any* primitive.

[8] i.e. not based on specific number theoretic assumptions

When applied to the results of [BFO08], we obtain the first construction of deterministic encryption from smooth homomorphic hash proof systems. Combining our work with the negative results of [RS09], we obtain a black-box separation between one-way trapdoor permutations and smooth homomorphic hash proof systems.

To reinforce the intuition that the DCR and QR assumptions can be used to replace the DDH assumption, we introduced the Extended Decisional Diffie Hellman (EDDH) assumption and showed that the DCR and QR assumptions imply the EDDH assumption. This provides a simple method for converting most DDH-based protocols into protocols whose security can be based on either the DCR or QR assumptions. In particular, this framework gives novel constructions of LTFs from the DCR assumption, and the first known constructions of fully lossy trapdoor functions from the QR assumption.

References

BBO07. Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and efficiently searchable encryption. In *CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 535–552. Springer Berlin / Heidelberg, 2007.

BFO08. Alexandra Boldyreva, Serge Fehr, and Adam O'Neill. On notions of security for deterministic encryption, and efficient constructions without random oracles. In David Wagner, editor, *CRYPTO '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 335–359. Springer, 2008.

BG10. Zvika Brakerski and Shafi Goldwasser. Circular and leakage resilient public-key encryption under subgroup indistinguishability. In *Proceedings of the 30th annual conference on Advances in cryptology*, CRYPTO'10, pages 1–20, Berlin, Heidelberg, 2010. Springer-Verlag.

BHHO08. Dan Boneh, Shai Halevi, Mike Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In *CRYPTO '08*, 2008.

BHK11. Mark Braverman, Avinatan Hassidim, and Yael Tauman Kalai. Leaky pseudo-entropy functions. In *ICS '11*, 2011.

CS98. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25, 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.

FGK+10. David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev. More constructions of lossy and correlation-secure trapdoor functions. In *PKC '10*, 2010.

GL89. Oded Goldreich and L. Levin. A hard-core predicate for all one-way functions. In *STOC '89*, pages 25–32. ACM, 1989.

HK07. Shai Halevi and Yael Tauman Kalai. Smooth projective hashing and two-message oblivious transfer. Cryptology ePrint Archive, Report 2007/118, 2007. http://eprint.iacr.org/2007/118.

Kal05. Yael Tauman Kalai. Smooth projective hashing and two-message oblivious transfer. In *EUROCRYPT '05*, pages 78–95, 2005.

MY09. Petros Mol and Scott Yilek. Chosen-ciphertext security from slightly lossy trapdoor functions. http://eprint.iacr.org/2009/524, 2009.

NP01. Moni Naor and Benny Pinkas. Efficient oblivious transfer protocols. In *SODA '01*, pages 448–457. ACM/SIAM, 2001.

Pai99. Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *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.

PVW08. Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David Wagner, editor, *CRYPTO '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2008.

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.

RS08. Alon Rosen and Gil Segev. Efficient lossy trapdoor functions based on the composite residuosity assumption. http://eprint.iacr.org/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.