Semantic Security Invariance under Variant Computational Assumptions

Eftychios Theodorakis* and John C. Mitchell**

Abstract. A game-based cryptographic proof is a relation that establishes equivalence between probabilistic sequences of actions by real and ideal world players [1]. The author of a proof selects a *hardness assumption system* for their proof upon which to base their subsequent statements. In this paper, we prove the existence of proof-invariant transformations for varying hardness assumptions. We show that for two systems satisfying certain algebraic properties any proof in one system has an equivalent valid proof in the other. This validates Kurosawa's remark [2] about the existence of proof similarities.
Our result implies a correspondence between the Learning With Errors (LWE) problems and both the Elliptic Curve Discrete Log problem (ECDLP) and the Discrete Logarithm (DLOG) problem. To illustrate this result, we provide a series of example transformations in the appendix. The concrete result of this paper is a prototype proof translation tool.

Keywords: semantic security proof, verification, automation, computational assumption, symmetry, invariance

1 Introduction

The foundation of a cryptographic protocol lies in its hardness assumptions. A plethora of such assumptions continues to be proposed [3][4][5][6][7] coinciding with the introduction of innovative new security models. It is common for authors to propose a hardness assumption in order to tackle an open cryptography problem [8][9] or to introduce a new security model [10]. The community later slowly migrates existing protocols to the new proposed assumption in an effort to exploit it further and explore its boundaries beyond the authors' original use. In the process community needs to assess how i) plausible, ii) strong and iii) expressive the assumption is.

In this work we tackle the following question: Knowing a proof of security under assumption $\mathbf{X}$ for functionality ϕ, can one provide a proof of ϕ under a different assumption $\mathbf{Y}$? For instance, if one proves a HIBE construction is fully (or selectively)-secure supposing a bi-linear diffie hellman assumption, can they argue about the existence of a construction (or even better derive one) supposing only factoring is hard instead?

Specifically, we introduce a framework for reducing relations between two algebras to a semantic security correspondence between two hardness assumptions.

* eftychios.theodorakis@gmail.com
** mitchell@cs.stanford.edu

We show in certain cases one can create a correspondence between a new hardness assumption and an existing one, such that any existing protocol with a game-based proof of security can be migrated to utilize the new hardness assumption instead, in a manner that preserves its semantic security proof. That is, there exist proof transformations that preserve its soundness and security guarantees. We show this proof invariance is contingent only on the algebraic properties of the two hardness assumption systems. By the term hardness assumption system we denote the couple of hardness (computational) assumption and algebra $\mathcal{L} = (U, \{+, \dots\})$ over a set U (universe) with a set of operands $\{+, \dots\}$. Common examples are the learning with errors (LWE) [4] and $\mathbb{Z}_q^n$, discrete linear (DLIN) and a bilinear group $(G,\ \hat{G},\ G_T,\ e : G \times \hat{G} \to G_T)$ (e.g. over supersingular elliptic curves).

We show that a relation between hardness assumptions A and B and their respective underlying algebras can imply the existence of a transformation between game-based proofs utilizing assumption A to proofs utilizing B (diagram 1). The strength of this method lies in one's ability to prove correctness and soundness in the simpler or pre-existing framework and implement it using a more practical, novel or robust assumption of that family, congruent to the original via these correspondences. This boosts the currently slow exploration process.

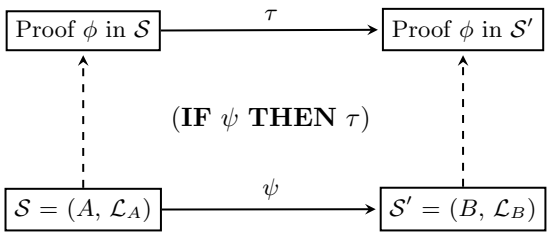


Diagram 1: We reduce any proof transformation (τ) to a hardness assumption system correspondence (ψ). In this case (Hardness Assumption A, Algebra $\mathcal{L}_A$) to (Hardness Assumption B, Algebra $\mathcal{L}_B$).

1.1 Contributions

We obtain proof transformations, i.e. correspondences between semantic security proofs, which differ in their hardness assumption premise. The transformations' soundness is based completely on the relation between the original and target algebra provided a composition preserving transformation between the hardness assumptions. One is able to apply current or new algebraic correspondences to establish equivalences or improve this work regardless of application. We prove these correspondences preserve indistinguishability; specifically one can use a transformation on the original proof to construct a similar one with different assertions. We show the derived proof is sound. If such a transformation is

invertible we call the two systems, i.e. couple of algebra and hardness assumptions, proof symmetric. Specifically, we construct such correspondences for surjective homomorphic algebras. Compared to past work we transform the cryptographic proofs, not the protocol. This allows us to utilize and preserve the proof's logic and structure; we preserve soundness rather than validate it as a last step. See section 9 for a comprehensive exposition of prior work.

Our approach can thus summarize a new lengthy proof into a short list of algebraic transformations, easier to formalize. That is, we derive a certificate of soundness for the transformed proof and do not generate a new one. Existing synthesis and refinement methods are transferable via this invariance – an old refinement method can be used via the transformation in the end system. Concluding, we gain i) an already rich toolkit of protocols ii) an idea of the expressiveness of the new assumption in comparison to existing ones – the "space" of protocols one can prove semantic security for under the new assumption compared to a previous stronger one.

We apply our result to learning with errors and elliptic curve discrete log assumptions as well as the decision linear and bi-linear assumptions. We construct a correspondence from the Decision Learning With Errors (D-LWE) assumption to the Elliptic Curve Discrete Log assumption (ECDLP) and the Discrete Logarithm (DLOG). This extends between the decision linear assumption (DLIN) and LIN-LWE and partially between DDH and DH-LWE. Among other, we produce an IBE construction under LWE and present the correspondence to recent IBE under CDH of Döttling and Garg [11].

Limitations of Current Work The concrete proof correspondence construction we present in this paper is built on top of a surjective homomorphism between the algebras of the origin and desired algebras hardness assumption systems. This provides us with the necessary reflection, yet adds certain restrictions. For instance, the only homomorphisms from non-abelian to abelian rings are the trivial ones. This restricts direct application of the construction to protocols realized under R-LWE to any diffie hellman hardness assumption system in general; however quite a few interesting protocols require thus far an underlying ring, such as Fully-Homomorphic Encryption. This is also in line with previous impossibility results [12].

Future Directions Our work is not restricted to the above assumptions. Pairings (and multi-linear maps) appear to be a fertile ground. Furthermore, a rich amount of work exists on algebraic correspondences. We think, the algebraic nature of the lift, indicates the existence and feasibility of establishing correspondences between interesting new assumptions and existing work. Restrictions to our main theorem (71) are also of interest: For instance, as $\mathbb{Z}_q^n$ ring is non-abelian; thus there is no generic correspondence to abelian (prime) groups. Possible paths on how to circumvent this impossibility and other algebraic restrictions, can provide insight for other interesting constructions.

2 Preliminaries

2.1 Protocol

Security protocols are a concurrent execution of actions executed by finite number of parties. A realized security protocol simulates an ideal protocol where parties can query trusted realizable functionalities. Here we describe protocols in a similar fashion to Hoare's CSP [13] and descendant approaches – like spi calculus [14]. This composability of functionalities view was presented by Canetti in [15]. The differentiating factor of security protocol languages and semantics with communicating protocols in general is the existence of an adversarial environment or participant.

Protocol Language

Definition 1. *We define a protocol as a member of language*

$\langle \Pi \rangle ::= \text{`}\texttt{seq}\text{'} \, [\langle Party \rangle] \, [\langle Func \rangle]$

$\langle Func \rangle ::= \text{`}\texttt{func}\text{'} \, [\langle Expression \rangle]$

$\langle Expression \rangle ::= \text{`}\texttt{while}\text{'} \, \langle Expression \rangle$
$\quad | \quad \langle AlgebraicExpression \rangle$
$\quad | \quad \langle Variable \rangle \; \text{`}\texttt{=}\text{'} \, \langle AlgebraicExpression \rangle$
$\quad | \quad \langle Variable \rangle \; \text{`}\texttt{=}\text{'} \, \langle Distribution \rangle$
$\quad | \quad \langle Expression \rangle \; \text{`}\texttt{==}\text{'} \, \langle Expression \rangle$
$\quad | \quad \langle Expression \rangle \; \text{`}\texttt{>}\text{'} \, \langle Expression \rangle$
$\quad | \quad \langle Expression \rangle \; \text{`}\texttt{!=}\text{'} \, \langle Expression \rangle$
$\quad | \quad \text{`}\texttt{out}\text{'} \, \langle Party \rangle \, \langle Variable \rangle$
$\quad | \quad \langle Expression \rangle \, \langle Term \rangle \, \langle Expression \rangle$

$\langle Party \rangle ::= \text{`}\texttt{Party}\text{'} \, \langle Natural \rangle$

$\langle Natural \rangle ::= .$

$\langle Distribution \rangle ::= .$

$\langle Term \rangle :: = \text{`}\texttt{return}\text{'}$
$\quad | \quad \overset{R}{\leftarrow}$

This approach easily generalizes and applies to other languages. We are directing the user to the particular literature for the intricacies of aforementioned languages. Similarly to spi calculus, assume a basic algebra $\mathcal{L}$ and a series of auxiliary terms. The basic building blocks are then the algebraic operations, send (**out**) and receive (**in**) operations, $\overset{R}{\leftarrow}$ sampling oracle and **return** returning the probability the argument boolean expression is true.

Games Proving the security of a protocol is typically modeled ([1][16][17]) as an exchange of moves between at least two probabilistic processes – an adversary and one or more challengers. Our goal is to show the adversary's strategy is negligibly better than arbitrary choice; a strategy is defined as a weighted list of moves dependent on the current state of the system. A game-based proof steps through a particular probabilistic strategy of the challengers; the cryptographer proceeds to show this strategy is equivalent with an ideal construction.

We follow Shoup's approach which models games as probability space functions [1]; each player's move is a transition to a new probability space. A typical game would start with a set of initial values with probability 1. Then the challenger would sample a variable $x \xleftarrow{R} \mathbb{Z}$, compute $f(x)$ for some function $f(\cdot)$ and give the result to the adversary. In the end the adversary would try to guess the result returning true on success. In the end the game is a function between probability spaces $\omega,\ \omega'$. We start with a null value with probability 1 and map it to a true event – adversary guessed right with a certain probability $[0, 1]$. This has two benefits i) it is easier to show observational equivalence for any two games [17] for an adversary ii) makes it easier to reason about game transformations and composition - as seen in [16].

Example 1. $y = a$ with probability 1 (a constant)
$k \xleftarrow{R} \mathbb{Z}$
$x = k + y$
Guess:
$g = A(y)$
return $x == g$

Formally,

Definition 2. *A game P_l, for a protocol $\mathcal{P}$, is modeled as a function $P_l \in \mathcal{P} : \mathcal{D}_{init} \to \mathcal{D}_{final}$, from an initial distribution $\mathcal{D}_{init}$ over some probability space $X = (\Omega, \mathcal{F}, P)$ to $\mathcal{D}_{final}$ over $X' = (\Omega', \mathcal{F}', P')$, X, X' representing the state of the system.*

For convenience a game,

Party 1:
$x_1 \xleftarrow{R} \{0, 1\}$
out Party 2 x_1
Party 2:
$x_2 = x_1 + 1$

can be written in a more functional fashion as

$$(+)(1,\ \text{Party 2 (out Party 2 }.x_1 =\xleftarrow{R} \{0,1\}(\ \text{Party 1 })(1))) \tag{1}$$

where *Party* $1(1)$ initializes party 1 with an initial distribution *1* – a no operation, out exposes the result to Party 2 . The final distribution $\mathcal{D}_{\text{final}}$ is $\Pr[x_1 = 1] = \Pr[x_1 = 0] = 1/2, \Pr[x_2 = 1] = \Pr[x_2 = 2] = 1/2$. Terms Party and out ensure type soundness and access – which party can modify and access which variables; = provides us with a naming directive.

2.2 Game-based Proofs

We consider game sequence based proofs [1]. A proof then is a sequence of games, starting from an ideal to a realizable game (Real). The real game makes use of no trusted parties or any ideal constructions. We use the notation G_I, G_R for ideal and real game respectively. A complete proof is a game transition from an ideal to a real game. Recall game transitions are an equivalence relation.

Defining hereafter:

$$\mathrm{Adv}_{\mathcal{A}}(\beta, \gamma) \stackrel{\mathrm{def}}{=} \|Pr\left(\mathcal{A}(\beta) = 1\right) - Pr\left(\mathcal{A}(\gamma) = 1\right)\|$$

($\mathcal{A}$ a probabilistic polynomial time (PPT) algorithm) and also:

$$\mathrm{Negl.} \stackrel{\mathrm{def}}{=} 1/n^{O(1)} \tag{2}$$

Hence

$$[equiv] \frac{\forall \mathcal{A},\ \ \mathrm{Adv}_{\mathcal{A}}(G_i, G_j) < \mathrm{Negl.}}{G_i \sim G_j} \tag{3}$$

e the identity element in $\mathcal{L}$ and $\sim$ an equivalence relation.

$$[proves] \frac{G_I^{\phi} \sim G_R^{\phi}}{\mathrm{Proof}^{\phi}} \tag{4}$$

See Shoup [1], Nowak [16] and Barthe et al. [17] for detailed analysis and examples. For convenience, we will use derivation notation to describe proofs (assuming always a true premise); a proof $\mathit{\Pi}$ of R in system $\mathcal{T}$ is the deduction denoted as

$$\mathit{\Pi} \underset{R}{\parallel} \mathcal{T} \tag{5}$$

2.3 Game-based proofs as categories

For the second part of the paper, we shall model games as categories. This allows us to focus on the properties and composability of game transitions as an algebraic consequence. Then a proof being a game transition naturally forms a 2-category itself. Specifically, let protocol $\mathit{\Lambda}$ contain all valid distribution functions, and a game $\lambda(D_i)$ for some distribution D_i and $\lambda \in \mathit{\Lambda}$. A game transition is then

$$\begin{gathered} \gamma : \mathrm{Game} \to \mathrm{Game}' \\ \text{s.t. } \mathrm{Adv}(\mathrm{Game}, \mathrm{Game}') < \mathrm{Negl.} \end{gathered}$$

And a proof $\mathit{\Pi}$ (see diagram 6) is:

$$\begin{gathered} \mathit{\Pi} = (\gamma, G_I, G_R) \\ \text{s.t. } G_R = \gamma(G_I) \end{gathered}$$

Hence here we argue about the existence of game transition transformations ($\gamma \mapsto \gamma'$), that allow one to substitute hardness assumptions. First let us formalize the above notions.

2.4 Category of Games

Lemma 1. *A game sequence for $\mathcal{P}$ set of parties expressed in a protocol language Λ over an algebra L forms a category $C(\Lambda)$:*

- *all subdistributions $\mathcal{D}_0, \mathcal{D}_1, \cdots \in \Lambda$ as its objects*
- *all games $\gamma_i \in \Gamma : \Lambda \to \Lambda$, functions between subdistributions $\mathcal{D}_x \to \mathcal{D}_y$, as its morphisms*
- *$\forall \mathcal{D}_I \in \Lambda,\ \mathcal{D}_I \mapsto \mathcal{D}_I$ as the identity mapping*
- *function composition as the morphism composition*

We denote the category containing all games realizing functionality ϕ $\mathfrak{G}_\phi$ and the category containing all games $\mathfrak{G}$.

Example 2. Consider the object to be the variable $V \in \mathbb{Z}_q$ with morphisms operations *in*, *out* and addition in the $< \mathbb{Z}_q, + >$. Two parties x and y can construct a simple messaging protocol for instance - or a mutual exclusion schema if one assumes atomicity.

2.5 Category of Proofs

As a consequence to our definition above, a security proof belongs to the 2-category. A proof is a game transition between an ideal and a real game, thus the morphisms between games in a category where games are its objects, provided the advantage of any adversary is negligible. Thus, we then need to show what are the sufficient properties for a transformation between proof categoeries to exist, so that game transitions are preserved.

Definition 3. $\mathrm{Morph}\,(\mathcal{C})$ *is the set containing all morphisms of category $\mathcal{C}$.*

Definition 4. $\mathrm{Obj}(\mathcal{C})$ *is the set containing all objects of category $\mathcal{C}$.*

Definition 5. *We define Proof category $\mathcal{P}$ for functionality ϕ*

- *the set of games $\{G\}_{\mathrm{Morph}\,\mathcal{G}_\phi}$ as its objects*
- *set game transitions as morphisms*
- *$\mathrm{id} : G \mapsto G$ as the identity mapping*
- *game transition composition as the composition*

Note the composition is sequential application of game transitions (rule application). In that sense we define the identity morphism as being the null substitution - unique up to isomorphism $\left(\dfrac{\Gamma \vdash \Delta, A \;\; Z \vdash E}{\Gamma \vdash \Delta, A} \overset{\sim}{\to} \dfrac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A}\right)$. Associativity is a direct result of logic application.

Definition 6. *A functor $F : C \to D$ is a transformation from category C to category D that preserves structure, i.e.*

$$\forall A, B \in \mathrm{Obj}(C) \exists F(A),\ F(B) \text{ and } \forall f, g \in \mathrm{Morph}\, C : B = g(A) \Rightarrow$$
$$F(f \circ g) = F(f) \circ F(g) \text{ and } F(\mathrm{id}_A) = id_{F(A)}$$

We can reword our problem as follows now:

Definition 7. *A translator τ_D^C is a functor from proof category C to proof category D.*

Namely, if there is a proof $\text{Proof}_{\mathcal{F}}^C$ under assumption A then, given a functor τ_D^C, there is a proof $\text{Proof}_{\mathcal{F}}^D = \tau_D^C(\text{Proof}_{\mathcal{F}}^C)$ under assumption B. Recall, it is necessary one i) preserves composition, ii) maps game transitions in C to game transitions in D.

2.6 The Diffie-Hellman Family of Assumptions

The Diffie Hellman problem has become the foundation of modern cryptography [18]. In this section we introduce the family of problems succinctly. For more information the reader is directed to [19].

Computational and Decisional Diffie-Hellman Problems Let group G_p of order $\|p\|$, generator g, $n = \log_2 \|p\|$ and $a, b \in \mathbb{Z}$. Then

Definition 8. *Suppose a group $G = (g, p)$ with a randomly chosen generator g. The Computational Diffie-Hellman Assumption states that there is no probablistic polynomial-time algorithm $\mathcal{A}$ able to efficiently compute the value g^{ab} provided with (g, g^a, g^b) with non-negligible probability. Specifically,*

$$\forall \mathcal{A} : \ Pr(\mathcal{A}(G = (g, p), g^a, g^b) = g^{ab}) < \frac{1}{n^{O(1)}} \tag{6}$$

Definition 9. *The Decisional Diffie-Hellman Assumption states that there is no algorithm $\mathcal{A}_D$ solving the Decisional Diffie-Hellman problem with non-negligible probability. Specifically,*

$$\text{Adv}_{\mathcal{A}}((G, g^a, g^b, g^c), (G, g^a, g^b, g^{ab})) < \frac{1}{n^{O(1)}} \tag{7}$$

with g^c uniformly sampled.

2.7 Decision Linear (DLIN)

Definition 10. *The Decision Linear (DLIN Assumption states that there is no PPT algorithm $\mathcal{A}_D$ able to distinguish g^{a+b} from a uniformly sampled g^c with non-negligible probability. Specifically*

$$\text{Adv}_{\mathcal{A}}((G, g^a, g^b, g^c), (G, g^a, g^b, g^{a+b})) < \frac{1}{n^{O(1)}} \tag{8}$$

2.8 LWE and R-LWE Assumptions

The learning with errors (LWE) assumption is based on the hardness of the shortest vector approximation problem $(\gamma - SVP)$[4].

Definition 11. *Learning with Errors assumption implies that any PPT adversary $\mathcal{A}$ is unable to distinguish between $As + e \mod q$ and $u \mod q$ where u is randomly chosen from $\mathbb{Z}^n$ and $A \in \mathbb{Z}^{m \times n}$, $s \in \mathbb{Z}^n$ and e follows a noise distribution $\mathcal{D}$. Hence*

$$Adv_{\mathcal{A}}((A, As + e), (A, u)) < \frac{1}{n^{O(1)}} \tag{9}$$

2.9 Computational Assumptions

Hence a computational hardness assumption is an assertion of a proof, based on the (conjectured) computational infeasibility of a particular problem. In particular,

Definition 12. *[20] A decisional computational assumption $A(\mathcal{D}_0, \mathcal{D}_1)$ is an assertion that a pair of distributions $\mathcal{D}_0, \mathcal{D}_1$ are equivalent for every Probabilistic Polynomial Time (PPT) adversary $\mathcal{A}$. Namely,*

$$\Pr_{b \xleftarrow{R} \{0,1\}, x \xleftarrow{R} \mathcal{D}_b} [\mathcal{A}(x) = b] < 1/2 + \frac{1}{poly(n)} \tag{10}$$

with n input size of the security parameter.

Assumption $A(\mathcal{D}_0, \mathcal{D}_1)$ is thus written as an equivalence relation $\dfrac{R}{T}$ – R being the premise and T the conclusion.

Examples For instance, one can write **DDH** as the pair

$$[\alpha] \frac{g^{ab} \quad a, b \in \mathbb{Z}}{u \quad u \leftarrow \text{sample}\, G} \qquad [\rho] \frac{u \quad u \leftarrow \text{sample}\ G}{g^{ab} \quad a, b \in \mathbb{Z}} \tag{11}$$

implying both $\alpha \underset{R}{\overset{T}{\parallel}} \mathcal{A}$ and $\rho \underset{T}{\overset{R}{\parallel}} \mathcal{A}$. Equivalence of premise and conclusion can be expressed by a pair of game transitions, as the following diagram exhibits.

$$\begin{array}{ccc} X = g, g^a, g^b & \underset{\rho}{\overset{\alpha}{\rightleftarrows}} & X_I \\ \Big\downarrow{\scriptstyle g^{ab}} & & \Big\downarrow{\scriptstyle u \leftarrow \text{sample}\ G} \\ Y & \underset{\rho}{\overset{\alpha}{\rightleftarrows}} & Y_I \end{array}$$

Definition 13. *Similarly, a search computational (search) assumption is an assertion that for every efficient (PPT) algorithm/adversary $\mathcal{A} : X \to Y$, given a pair of polynomial time algorithms $(\mathcal{D}, \mathcal{V})$ (instance sampler and verifier):*

$$\Pr_{r \xleftarrow{R} \{0,1\}^n,\ x = \mathcal{D}(r)} [\mathcal{A}(x) = y \ s.t.\ \mathcal{V}(x, y, r) = 1] < \frac{1}{poly(n)} \tag{12}$$

Here we use the most liberal definition of a privately-verifiable search hardness assumption in [20]. In this case we provide the randomness to the verifier function $\mathcal{R}$. If we restrict access of the randomness for the verifier we define a "classical" search computational assumption. We can also extend the verifier to a t-search problem by bounding the probability of counting $t(n)$ witnesses (for more details see [20]). Hence, a search assumption is an equivalence with a simulated function $S : \_ \to Y$, with no access to x, uniformly sampling Y.

Example 3. **CDH** implies for an adversary $\mathcal{A}$ any function $f : g^a \times g^b \mapsto g^{ab}$ is equivalent to a function $r : g^a \times g^b \mapsto u \xleftarrow{R} G$.

One may then represent a hardness assumption A a a pair of functors

$$F^A : C \rightleftarrows D : G^A \tag{13}$$

Example 4. **DDH** can be written as the following pair of game transitions. Recall these are endofunctors – they map a category to itself:

$$\overrightarrow{\mathcal{DDH}} = \begin{cases} (g^a \times g^b \mapsto g^a \times g^b \times g^{ab}),\ (g^a \times g^b \mapsto g^a \times g^b \times \mathcal{U}_{\mathbb{Z}_p}) \\ \text{id}, \quad \text{otherwise} \end{cases}$$

$$\overleftarrow{\mathcal{DDH}} = \begin{cases} (g^a \times g^b \mapsto g^a \times g^b \times \mathcal{U}_{\mathbb{Z}_p}),\ (g^a \times g^b \mapsto g^a \times g^b \times g^{ab}) \\ \text{id}, \quad \text{otherwise} \end{cases}$$

We denote with $\mathcal{U}_X$ a type with the properties of a random sample from set X:

$$\begin{aligned} \mathcal{U} + v &\approx_c \mathcal{U} \\ v\mathcal{U} &\approx_c \mathcal{U} \\ \forall v &\in X \end{aligned}$$

For instance,

$$(g^a, b, M) \mapsto g^{ab} + M$$

can be written as

$$(g^a, b, M) \mapsto \overrightarrow{\mathcal{DDH}}((g^a, b) \mapsto g^b, g^a, \mathcal{U}) + M$$

Observe a hardness assumptions can be considered as a parametric type proof: given a specific data type one could substitute it with another type with similar operators. We argue this allows us define transformations between hardness assumptions.

Definition 14. *Let functors $F, G : C \to D$. A natural tranformation η is a morphism such that $\eta_X : F(X) \to G(X)$ for every object X of C and for all $f : X \to Y$ holds $F(f) \circ \eta_Y = \eta_X \circ G(f)$.*

Essentially a natural morphism between two hardness assumptions ensures we can write any game transition or functionality in the former assumption using the latter assumption. The converse also holds: if one can transform any functionality from one assumption to a different assumption then that transformation is natural. However, this does not imply game transitions are preserved! Note the natural transformation ensures the preservation of composition.

3 Motivating Example: El Gamal Encryption in Elliptic Curves from LWE public key encryption

Let us try to derive the El Gamal Encryption in Elliptic Curves proof (fig. 3a, fig. 3b) from the following simple public key encryption primitive proof under LWE (see [21]).

Init Phase: $L = L(\mathbb{Z}_q^n)$, $(M_0, M_1) =\xleftarrow{R} \mathbb{Z}_q^{m\times 1})$ $s \xleftarrow{R} \mathbb{Z}_q^{n\times 1}$ (Bob's secret) $A \xleftarrow{R} \mathbb{Z}_q^{m\times n}, B = As + e$, (Bob's public key, e noise) **Alice:** $k \xleftarrow{R} \mathbb{Z}_q^{m\times m}$ $a =\xleftarrow{R} \{0,1\})$ $y = kA + e, x = kB + M_a + e$ *out* Bob $.(x, y)$ **Guess:** $b = A(x, y)$ return b==a	**Init Phase:** $(M_0, M_1) =\xleftarrow{R} \{0,1\})$ **Alice:** $a =\xleftarrow{R} \{0,1\})$ (x, y) : $x, y = \mathcal{O}(M_a)$ *out* Bob $.(x, y)$ **Guess:** $b = A(x, y)$ return b==a with $\mathcal{O} : M \to X \times Y$ and $\mathcal{O}_D : X \times Y \to M$ s.t. $\mathcal{O}_D(\mathcal{O}(m)) = m$ and $\mathcal{O}_D(x', y') =\perp$ otherwise.
(a) Real Game for CPA proof of public key encryption from LWE	(b) Ideal Game for CPA proof of public key encryption from LWE

Diagram 2: LWE Public key encryption CPA proof [21]

We can write the real game:

$$\text{El Gamal Public key CPA Game} = \text{Guess} \circ \text{Alice round} \circ \text{Party (Bob, Alice) init}$$

$$\text{Guess} = \text{func return } b == a, b = A(x, y)$$

$$\text{Alice\_Round} = \text{func out Party Bob } .(x, y)(y = kA + e,$$

$$x = kB + M_a + e, k =\xleftarrow{R} \mathbb{Z}_q^{m\times m}, a =\xleftarrow{R} \{0,1\})$$

$$\text{init} = \text{func (Party Bob } (s \xleftarrow{R} \mathbb{Z}_q^{n\times 1}), L = \mathbb{Z}_q^n), A \xleftarrow{R} \mathbb{Z}_q^{m\times n},$$

$$, B = As + e, (M_0, M_1) =\xleftarrow{R} \mathbb{Z}_q^{1\times m})$$

and respectively the ideal one:

$$\text{El Gamal Public key CPA Game} = \text{Guess} \circ \text{Alice round} \circ \text{Party (Bob, Alice) init}$$
$$\text{Guess} = \text{func return } b == a, b = A(x, y)$$
$$\text{Alice\_Round} = \text{func out Party Bob } .(x, y)(y = \mathcal{O}(k), x = \mathcal{O}_{\text{Encrypt}}(\mathcal{O}_{\text{KE}}(k, B), M_a),$$
$$k =^{R}\leftarrow \mathbb{Z}, a =^{R}\leftarrow \{0, 1\})$$
$$\text{init} = \text{func (Party Bob } (s \overset{R}{\leftarrow} \mathbb{Z}), B = \mathcal{O}(s), (M_0, M_1) =^{R}\leftarrow \mathcal{M})$$

with $\mathcal{M}$ an arbitrary large set.

The proofs consists of two game transitions. First we substitute oracle $\mathcal{O}(\cdot)$ sampling queries for public and private parameters with sampling from $\mathbb{Z}_q^n$ (s_a). Afterwards we substitute the encryption and private key retrieval queries with point multiplication operations $(s_{\mathbf{LWE}})$. We can express the real game as the composition of the above game transitions on the ideal game:

$$\text{Real Game} = s_{\mathbf{LWE}} \circ s_a \circ \text{Ideal Game}$$

We write the elliptic curve equivalent of the above El gamal public key encryption as follows (see Koblitz original paper [22]).

$$\text{El Gamal Public key CPA Game} = \text{Guess} \circ \text{Alice round} \circ \text{Party (Bob, Alice) init}$$
$$\text{Guess} = \text{func return } b == a, b = A(x, y)$$
$$\text{Alice\_Round} = \text{func out Party Bob } .(x, y)(y = kP, x = kB + M_a,$$
$$k =^{R}\leftarrow \mathbb{Z}, a =^{R}\leftarrow \{0, 1\})$$
$$\text{init} = \text{func (Party Bob } (s \overset{R}{\leftarrow} \mathbb{Z}), E = E(\mathbb{F}_q), P \in E, B = sP, (M_0, M_1) =^{R}\leftarrow E)$$

We first define the parameters in init: we pick an elliptic curve is E, sample secret s under Bob's context, and pick a point P in E as public parameter. The ideal game is written similarly to the original CPA proof under LWE. Similarly,

$$\text{Real Game El Gamal ECDLP} = s_{\mathbf{ECDLP}} \circ s'_a \circ \text{Ideal Game}$$

To derive the CPA proof for the El Gamal public key encryption (fig. 3) under ECDH from the LWE proof we define the following transformation:

$$\tau = \begin{cases} h : \mathbb{Z}_q^n \twoheadrightarrow E(\mathbb{F}_p) \\ s_{\mathbf{LWE}} \mapsto s_{\mathbf{ECDLP}} \end{cases}$$

and

$$\frac{\tau(f \circ g)}{\tau(f) \circ \tau(g)}, \quad \frac{\tau(x, y)}{\tau(x), \tau(y)}$$

s.t.

$$\begin{aligned}\tau(\text{Real Game LWE}) &= \tau(s_{\mathbf{LWE}}\ ) \circ \tau(s_a) \circ \tau(\text{Ideal Game}) \\ &= s_{\mathbf{ECDLP}}\ \circ s'_a \circ \tau(\text{Ideal Game}) \\ &= \text{Real Game El Gamal ECDLP}\end{aligned}$$

We derived the proof[1] as a transformation of the original LWE proof.

Init Phase: $E = E(\mathbb{F}_q)$, $(M_0, M_1) \xleftarrow{R} E)$ $s \xleftarrow{R} \mathbb{Z}$ (Bob's secret) $P \in E, B = sP$, (Bob's public key) **Alice:** $k \xleftarrow{R} \mathbb{Z}$ $a \xleftarrow{R} \{0,1\})$ (x, y) : $y = kP, x = kB + M_a$ *out* Bob $.(x, y)$ **Guess:** $b = A(x, y)$ return b==a	**Init Phase:** $(M_0, M_1) \xleftarrow{R} \{0,1\})$ **Alice:** $a \xleftarrow{R} \{0,1\})$ (x, y) : $x, y = \mathcal{O}(M_a)$ *out* Bob $.(x, y)$ **Guess:** $b = A(x, y)$ return b==a with $\mathcal{O} : M \to X \times Y$ and $\mathcal{O}_D : X \times Y \to M$ s.t. $\mathcal{O}_D(\mathcal{O}(m)) = m$ and $\mathcal{O}_D(x', y') = \perp$ otherwise.
(a) Real Game for El Gamal Public Key Encryption	(b) Ideal Game for El Gamal Public Key Encryption

Diagram 3: El Gamal CPA proof

4 Main Result and Overview

In this paper we consider computational assumptions and the underlying algebra as proof variables. For example, consider a proof of CCA2-IND semantic security of a new primitive under LWE. One can substitute the ECDH assumption with Elliptic Curve Diffie-Hellman assumption (ECDH) and transform the original proof into a new one. We coin the term *translation* and work on introducing a *translator* τ. Hence, this paper studies the following type of transformations (τ):

$$\tau : \Pi \underset{R}{\|} \mathcal{T}, \mathcal{A} \to \Pi' \underset{\tau \circ R}{\|} \mathcal{T}', \mathcal{A}' \tag{14}$$

[1] We have to consider the soundness proof too. This is simpler as it is a pair of equalities $(x - sy = M)$

4.1 Outline of approach

In the rest of the paper we shall prove the existence and properties of game transition transformations. We divide the problem as follows:

1. Prove the existence of an equivalent ideal game (lemma 4)
2. Prove every mirror transformation exists – $G_{ij} \Rightarrow G'_{ij}$ in the new system (definition & lemma 12)
3. Prove every mirror transformation is a game transition, i.e. an adversary has negligible advantage to distinguish between the two games (lemma 3, lemma 15)

Main Theorems Consequently, we prove (section 7) that:

Theorem 71. *Suppose security parameter s, an algebraic surjective homomorphism $h_s : \mathcal{L}_s \to \mathcal{L}'_s$, with $\{\mathcal{L}_s\}$, $\{\mathcal{L}'_s\}$ families of finite algebras in the standard sense (first isomorphism theorem holds and equipped with an identity element), an S_0 s.t. for all $s > S_0 : \frac{|\mathcal{L}_s|}{|\mathcal{L}'_s|} s^c$ negligible in s for any $c < 0$. Also let theories $T = T_\star \cup \{A\}$ and $T' = T_\star \cup \{A'\}$, such that $\eta : A \to A'$ natural. Then a proof correspondence exists from system $(T, \mathcal{L})$ to $(T', \mathcal{L}')$. Namely, for any functionality ϕ with proof Π_ϕ using security parameter s in $(T, \mathcal{L})$ there is a proof Π'_ϕ in $(T', \mathcal{L}')$ satisfying the same security model.*

Theorem 72. *Suppose algebras $\mathcal{L}$, $\mathcal{L}'$ and consistent theories with T, T' – $T = T_\star \cup \{A\}$ and $T' = T_\star \cup \{A'\}$, with A, A' natural. If there is a weak equivalence between $\mathcal{L}$ and $\mathcal{L}'$ then there exists a proof symmetry between proofs in system $(\mathcal{L}, T)$ and $(\mathcal{L}', T')$. For every proof Π^ϕ of $(\mathcal{L}, T)$ there exists Π'_ϕ of $(\mathcal{L}', T')$ and conversely.*

We start by making a few observations about preserving distribution distance in the following section.

5 Semantic Security Preserving Transformations

5.1 Outline of our argument

Suppose

$$\tau : A \mapsto A_H \tag{15}$$

and for any adversary $\mathcal{A}$

$$\mathrm{Adv}_{\mathcal{A}}(A) \leq \kappa \tag{16}$$

We want to show that there is a τ s.t. any map A_H satisfies an indistinguishability property $V(A_H)$, i.e.

$$\mathrm{Adv}_{\mathcal{A}}(A_H) \leq \kappa \tag{17}$$

with κ a negligible amount for any $\mathcal{A}$ adversary. This can be achieved as follows (see diagram 4): Pick a function $A_H : \mathcal{L}' \to \mathcal{L}'$. Then A_H is in the image of F. Show that if one bounds the advantage of the pre-image of A_H by a quantity δ and assumes the existence of an adversary $\mathcal{B}$ with greater advantage than a $\delta'(\delta)$, then due to reflection relation r there is an adversary $\mathcal{A}'$ that contradicts the originally asserted bound.

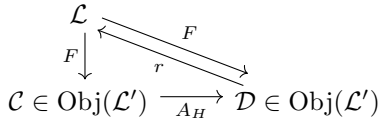


Diagram 4: Let $F : \mathcal{L} \to \mathcal{L}'$. We want to show that there is an implied reflection relation r that affects the adversaries advantage in distinguishing between two distributions.

5.2 Master Lemma and Extensions

We first generalize Lemma 1 in [23] - a group homomorphism preserves uniform distribution - for any algebra. The result follows by applying the fundamental homomophism theorem.

Lemma 2. *Given an (algebraic) surjective homomorphism $h : \mathcal{L}_A \to \mathcal{L}_B$, a uniform random variable X over $\mathcal{L}_A$ then $y \in \mathcal{L}_A$,* $\Pr[h(X) = y] = \frac{\|\ker h\|}{\|G\|}$.

Hence, similarly to [23], Li et al; we can write for the entropy H

$$H(h(X)) = \log \frac{\|\mathcal{L}\|}{\|\ker h\|} \tag{18}$$

Proof.

$$\forall v \in \mathcal{L}_B \Pr[h(X) = v] - \Pr[h(Y) = v] \leq \delta' \tag{19}$$

Given $\Pr[X = u] - \Pr[Y = u] \leq \delta$ and h surjective homomorphism with $\ker(h) = k$, one can see that in worst case all elements of a subset of size $\|k\|$ will map to a single element. Hence

$$\Pr[h(X) = v] - \Pr[h(Y) = v] \leq k\delta = \delta' \tag{20}$$

□

Ideally h has kernel $k = \ker(h)$, $|k| \leq \frac{1}{n^{O(1)}}$. We show in proposition 51 the kernel cardinality is not related to the size of the security variable, but is an

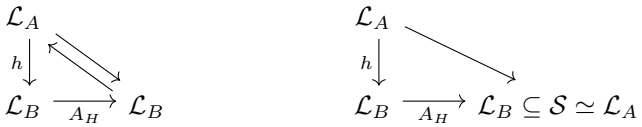


Diagram 5: One way to preserve the original statistical indistinguishability property of $\mathcal{L}_A$ algebra is to find a relation between $\mathcal{L}_A$ and $\mathcal{L}_B$, a mapping $\mathcal{L}_A$ to $\mathcal{L}_B$. For example, showing $\mathcal{L}_B$ is a subset of $\mathcal{L}_A$.

intrinsic value of the homomorphism. This result is not surprising though - any special attributes and characteristics of the algebra used to solve the problem are transplanted into the new algebra via the homomorphism.

Let us consider a toy case. If $\mathcal{L}_B \subseteq \mathcal{L}_A$ we have an arrow $\mathcal{L}_B \to \mathcal{L}_A$ connecting any morphism between domain and codomain. Particularly we have that $A = A_H \circ h$ and hence $\delta' = \delta$.

Example 5. Applying the same reasoning solving the roots of a polynomial bounded via the Schwartz-Lippel lemma (as usually applied in the generic group model, e.g. in [24]):

$$\Pr\left[P(r) = 0\right] \leq \frac{d}{\|S\|},\ P \in \mathbb{F}[x_0, \ldots, x_n],\ r \in \mathbb{R}^n \tag{21}$$

for maximum degree d and set S, can be bounded by

$$\Pr[h(P(r)) = 0_h] \leq \frac{d|\ker(h)|}{\|S\|} \tag{22}$$

Lemma 2 gives us $\Pr\left[h(P(r)) = 0_h\right] \leq \frac{d}{\|h(S)\|} = \frac{d|\ker(h)|}{\|S\|}$ – due to following proposition 51.

The above result is a statistical bound for uniform distributions. Next we shall extend the argument to distinguishing between two arbitrary distributions.

5.3 Preserving Distributions

Preserving Distribution Indistinguishability We want to derive an upper bound for the adversarial advantage of any game transition between two games G_0, G_1 in the target system $(T', \mathcal{L}')$. We argue that given two distributions $\mathcal{D}, \mathcal{E}$ in $\mathcal{L}$ with $\mathrm{Adv}_A(\mathcal{D}, \mathcal{E}) \leq \delta$ for all adversaries $A \in PPT(\mathcal{L} \to \mathcal{L})$, we can derive a bound $\mathrm{Adv}_B(\mathcal{D}', \mathcal{E}') \leq \delta'$ for $\mathcal{E}' = h \circ \mathcal{E}, \mathcal{D}' = h \circ \mathcal{D}$ for all adversaries B. Specifically we need δ' to be negligible ($\delta' \leq \delta + \epsilon = \delta + \frac{1}{n^{O(1)}}$). Consider ϵ as the deviation due to incomplete information.

We first argue at this point the cardinality of the kernel of a surjective homomorphism is a constant dependent only on the cardinality of the universes. We will use that to bound the advantage deviation only in terms of the underlying algebras.

Proposition 51. *Suppose $h : \mathcal{L} \to \mathcal{L}'$ as surjective homomorphism. Then its kernel $k = \frac{\|\mathcal{L}\|}{\|\mathcal{L}'\|}$.*

Proof. From the first (generalized) isomorphism theorem of algebra we have that

$$\mathcal{L}/\ker h \simeq Im(h) \tag{23}$$

Because h is onto, it holds

$$\mathcal{L}/\ker h \simeq Im(h) = \mathcal{L}' \tag{24}$$

From the Langrange theorem it follows that

$$|\mathcal{L}| = |\mathcal{L}/\ker h||\ker h| \Rightarrow \tag{25}$$
$$|\mathcal{L}| = |\mathcal{L}'||\ker h| \Rightarrow \tag{26}$$
$$|\ker h| = \frac{|\mathcal{L}|}{|\mathcal{L}'|} \tag{27}$$

□

The following lemma and its corollaries follow.

Lemma 3. *Suppose two distributions $\mathcal{D}, \mathcal{E}$ on $\mathcal{L}$ a finite algebra in the standard sense (satisfying the first isomorphism theorem and having an identity element) with $\mathrm{Adv}_A(\mathcal{D}, \mathcal{E}) \leq \delta$ for any PPT adversary $A : \mathcal{L} \to \mathcal{L}$ and a surjective homomorphism $h : \mathcal{L} \to \mathcal{L}'$. Assume we can compute the algebraic operations of $\mathcal{L}$, $\mathcal{L}'$ in polynomial time. It holds that for any adversary $\mathcal{B}$ in $\mathcal{L}'$, $\mathrm{Adv}_{\mathcal{B}}(h(\mathcal{D}), h(\mathcal{E})) \leq \frac{|\mathcal{L}|}{|\mathcal{L}'|}\delta$. The minimum bound δ is achieved only for an isomorphism.*

Proof. We have that

$$\forall B : \mathcal{L}' \to \mathcal{L}',\ \exists A : \mathcal{L} \to \mathcal{L} \tag{28}$$

s.t.

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{A} & \mathcal{L} \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ \mathcal{L}' & \xrightarrow[B]{} & \mathcal{L}' \end{array}$$

commutes. Then we have that for distributions D', E' on $\mathcal{L}'$:

$$|Pr[B(D') = e] - Pr[B(E') = e]| = \tag{29}$$
$$= |Pr[BhD = e] - Pr[BhE = e]| \tag{30}$$
$$= |Pr[hAD = e] - Pr[hAE = e]| \tag{31}$$
$$= \left| \sum_{g \in \ker h} (Pr_D[A = g] - Pr_E[A = g]) \right| \tag{32}$$
$$\leq \sum_{g \in \ker h} |(Pr_D[A = g] - Pr_E[A = g])| \tag{33}$$
$$\leq |\ker(h)| \, |(Pr_D[A = g] - Pr_E[A = g])| \text{ for some } g \tag{34}$$
$$\leq |\ker(h)| \max_{g \in \ker(h)} |(Pr_D[A = g] - Pr_E[A = g])| \tag{35}$$

Let there be g' maximizing point then there exists A'

$$A^{-1}(g') = A'^{-1}(e)$$

for instance

$$A'(x) = \begin{cases} A(x), \ g \neq x \xleftarrow{R} D \\ e, \ g = x \xleftarrow{R} D \end{cases}$$

If A is a PPT algorithm we can see A' and thus any B are PPT[2]. Conversely, if B is a function computed by a PPT algorithm then A' has to be computed by a PPT algorithm. Then

$$|\ker(h)| \max_{g \in \ker(h)} |(Pr_D[A = g] - Pr_E[A = g])| = \tag{36}$$
$$|\ker(h)| \, |(Pr_D[A' = e] - Pr_E[A' = e])| \tag{37}$$
$$\leq |\ker(h)| \delta = \frac{|\mathcal{L}|}{|\mathcal{L}'|} \delta \tag{38}$$

□

Notice that $\kappa = \frac{|\mathcal{L}|}{|\mathcal{L}'|} \geq 1$, with equality holding only for h isomorphism. This is optimal as we do not gain any further information by applying the transformation. Notice also δ remains negligible in the new security variable as a result.

Corollary 51. *Assume two indistinguishable distributions $\mathcal{D}$, $\mathcal{E}$ with advantage $\mathrm{Adv}_{\mathcal{A}}(\mathcal{D}, \mathcal{E}) \leq \delta$ and a surjective homomorphism h with kernel $\ker(h)$ s.t. $\ker(h)\delta \leq 1/n^{O(1)}$, with n the security variable size. The homomorphism h preserves indistinguishability, i.e. for any adversary $\mathrm{Adv}(h(\mathcal{D}), h(\mathcal{E}))$ is negligible.*

[2] Recall $h(f \circ g) = h(f) \circ h(g)$

$$
\begin{array}{ccccccc}
G_I : X & \xrightarrow{F_{I1}} & G_1 : X & \xrightarrow{F_{12}} & \cdots & \xrightarrow{F_{..R}} & G_R : X \\
\downarrow{\scriptstyle \mu_0^I} & & \downarrow{\scriptstyle \mu_{XY}^1} & & & & \downarrow{\scriptstyle \mu_{XY}^R} \\
G_I : Z & \xrightarrow{F_{I1}} & G_1 : Z & \xrightarrow{F_{12}} & \cdots & \xrightarrow{F_{..R}} & G_R : Z \\
\downarrow{\scriptstyle \mu_{YZ}^I} & & \downarrow{\scriptstyle \mu_{YZ}^1} & & & & \downarrow{\scriptstyle \mu_{YZ}^R} \\
G_I : Y & \xrightarrow{F_{I1}} & G_1 : Y & \xrightarrow{F_{12}} & \cdots & \xrightarrow{F_{..R}} & G_R : Y \\
\downarrow{\scriptstyle \mu_{Z..}^I} & & \downarrow{\scriptstyle \mu_{Z..}^1} & & & & \downarrow{\scriptstyle \mu_{Z..}^R} \\
G_I : \cdots & \xrightarrow{F_{I1}} & G_1 : \cdots & \xrightarrow{F_{12}} & \cdots & \xrightarrow{F_{..R}} & G_R : \cdots
\end{array}
$$

Diagram 6: A proof is a sequence of game transitions F_{ij} from an ideal to a real game. (In particular, $F_{IR} = F_{Ix} \circ \cdots \circ F_{yR}$. A game $G : X \to Y$ itself is a composition of games; for instance hybrid game $G^A_{XY} = \mu^A_{ZY}(\mu^A_{XZ})G^A_X$. The advantage for $\mathcal{A}$ is $\mathrm{Adv}_{\mathcal{A}}(G_I, G_R) = \sum_{A \in [I,\ldots,R-1]} \mathrm{Adv}_{\mathcal{A}}(\mu^A_{ZY}(\mu^A_{XZ})G^A_X, \mu^{A+1}_{ZY}(\mu^{A+1}_{XZ})G^{A+1}_X)$.

6 Constructing a symmetric proof

6.1 Algorithm Outline

In this section we construct an equivalent ideal game (lemma 4). An ideal game describes the functionality as a sequence of message exchanges, trusted party queries and basic algebraic operations. We argue a functor preserves each component and their composition. We show in the next section (5) there are correspondences that preserve computational indistinguishability of a distribution for all PPT algorithms. Specifically, we show the minimal set of properties for such a correspondence to exist and show that a surjective homomorphism between two families of algebras is one. We also show a weak equivalance between two algebras forms such a correspondence. We combine the above to prove our main statement 71, 72 in section 7. We assume we are given an existing proof implied by an asserted assumption (fig. 7a). To ensure a new hardness assumption (fig. 7b) can construct protocols simulating at least the same trusted parties we need a natural mapping between the two hardness assumptions (fig. 7c). Now we can construct all game transitions (fig. 6) leading to aforementioned theorems 71 and 72.

6.2 Generating a Corresponding Ideal Game

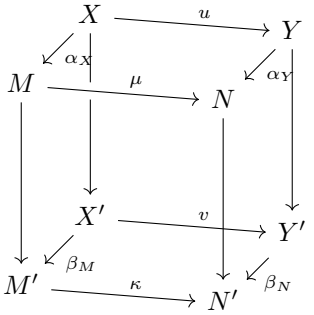
Definition 15. *A security model of a protocol is the collection of security properties the protocol must satisfy against specific adversarial attacks, expressed in the form of an ideal game.*

Common Examples: IND-CPA, IND-CCA1,NM-CPA

Namely, an ideal game is a protocol execution specifying functionality ϕ via abstract or ideal operations. It describes the relationship between the objects

(a) The assumption α in our theory ($u \simeq_c v$) is expressed by the above diagram.

(b) A new assumption β ($\mu \simeq_c \kappa$) expressed by a similar diagram.



(c) There is an algebraic correspondence between assumptions.

of the system, hence highlighting its structure. In that sense it is abstract; one describes how protocol participants interact with each other via ideal trusted functionalities. It is devoid of any hardness assumption constructs and it is consistent. We need then to first provide the specification corresponding to the same security model utilizing the new algebra. Specifically, an ideal game G can be written as

$$G = \text{Game}\, g(\mathcal{F}_0, \mathcal{F}_1, \cdots, \mathcal{F}_k) \tag{39}$$

for ideal trusted functionalities $\boldsymbol{\mathcal{F}} = \{\mathcal{F}_0, \mathcal{F}_1, \cdots, \mathcal{F}_k\}$, a function g, and a type constructor Game.

An ideal game transformation into a new system comprises the composition of other ideal functionalities. Below we show composition is preserved.

Lemma 4. *Suppose a functor F between the two proof categories; then the game $G'_I = F(G_I)$ is ideal, consistent and satisfies the same security model, provided $F(\mathcal{F}_i)$ is ideal functionality for all $\mathcal{F}_i$ and F is fully faithful.*

Proof. An ideal game is a game invoking a collection of ideal functionalities. Consider ideal functionality $\mathcal{F}_Y^C = \mathcal{F}_Y = g_0 \circ \mathcal{F}_0 \circ g_1 \circ \mathcal{F}_1 \circ \cdots \circ g_N \circ \mathcal{F}_N$. Then

$$\mathcal{F}_{Y'}^D = F(\mathcal{F}_Y) = F(g_0) \circ F(\mathcal{F}_0) \circ F(g_1) \circ F(\mathcal{F}_1) \circ \cdots \circ F(g_N) \circ F(\mathcal{F}_N) \tag{40}$$

By assumption $F(\mathcal{F}_i)$ is a process that implements the same ideal functionality as $\mathcal{F}_i$ for all $[1, N]$. Thus $\mathcal{F}_{Y'}^D$ is also a process implementing an ideal functionality in D.

Recall if F is faithful, it is injective and thus:

$$F(\mathcal{F}_X) \circ F(\mathcal{F}_M) = F(\mathcal{F}_Y) \Rightarrow \quad (41)$$

$$\mathcal{F}_X \circ \mathcal{F}_M = \mathcal{F}_Y \text{ for all } \mathcal{F}_X \quad (42)$$

If it is also full then there is $\mathcal{F}_M^D = F(\mathcal{F}_M)$ s.t.

$$\mathcal{F}_M^D \circ \mathcal{F}_{Y'}^D = F(\mathcal{F}_M) \circ F(\mathcal{F}_Y) = F(\mathcal{F}_M \circ \mathcal{F}_Y) \quad (43)$$

$$\text{Thus } Y = Y' \text{respective to all processes realizing functionalities } \{M\}. \quad (44)$$

□

7 Main Theorems

Definition 16. *Theories $T = T_\star \cup \{M\}$ and $T' = T_\star \cup \{M'\}$ are consistent if $\nexists \sigma$ s.t. $T_\star,\ M \vDash \sigma,\ T_\star$ and $M' = \neg\sigma$.*

Now we can derive the two main theorems of the paper.

Theorem 71. *Suppose security parameter s, an algebraic surjective homomorphism $h_s : \mathcal{L}_s \to \mathcal{L}'_s$, with $\{\mathcal{L}_s\},\ \{\mathcal{L}'_s\}$ families of finite algebras in the standard sense (first isomorphism theorem holds and equipped with an identity element), an S_0 s.t. for all $s > S_0 :\ \frac{|\mathcal{L}_s|}{|\mathcal{L}'_s|} s^c$ negligible in s for any $c < 0$. Also let theories $T = T_\star \cup \{A\}$ and $T' = T_\star \cup \{A'\}$, such that $\eta : A \to A'$ natural. Then a proof correspondence exists from system $(T, \mathcal{L})$ to $(T', \mathcal{L}')$. Namely, for any functionality ϕ with proof Π_ϕ using security parameter s in $(T, \mathcal{L})$ there is a proof Π'_ϕ in $(T', \mathcal{L}')$ satisfying the same security model.*

Proof. We first apply lemma 4 constructing an ideal game in $(T', \mathcal{L}')$ for $\phi, \mathcal{S}$. We decompose original game transitions comprising of the hardness assumption. For each other game transition s_{ij} ($G_j = s_{ij} G_i$) we apply the master lemma 3, applying $h(s_{ij}^{-1}) = h(s_{ji})$. As $\frac{|\mathcal{L}|}{|\mathcal{L}'|}$ is independent of the security variable s, every new game transition can be bounded by $\frac{1}{\text{poly}(s)}$. Without loss of generality assume a single invocation of the hardness assumption asserted diagram. Then

$$\text{Adv}(G'_I, G'_R) = \text{Adv}(G'_I, G'_X) + \text{Adv}(G'_Y, G'_R) + \text{Adv}(s_{A'}) \quad (45)$$

with $G'_I,\ G'_R$ the new ideal and real games respectively. $G'_Y = s_{A'} G_X$ and the advantage of $s_{A'}$ is negligible due to the hardness assumption. Note that at this point we have constructed only games $[G'_I \dots G'_X]$. Using $A \mapsto A'$ (naturality condition) we can construct a game transition $s_{A'}$ such that $G'_X \simeq_c G'_Y$. Summing the advantages of all new hybrid games we have $\text{Adv}(G'_I, G_R) < \text{Negl}$. □

We call $\mu = \frac{\|\mathcal{L}\|}{\|\mathcal{L}'\|}$ our transition magnification factor. The ratio of the advantage between ideal game and real game of the new proof over the original is the total magnification factor.

We extend the above approach and show that if we define proof systems comprising of weak equivalent arbitrary algebras among other conditions, the equivalence is lifted to the proof system themselves.

Theorem 72. *Suppose algebras $\mathcal{L}$, $\mathcal{L}'$ and consistent theories with $T, T' - T = T_\star \cup \{A\}$ and $T' = T_\star \cup \{A'\}$, with A, A' natural. If there is a weak equivalence between $\mathcal{L}$ and $\mathcal{L}'$ then there exists a proof symmetry between proofs in system $(\mathcal{L}, T)$ and $(\mathcal{L}', T')$. For every proof Π^ϕ of $(\mathcal{L}, T)$ there exists Π'_ϕ of $(\mathcal{L}', T')$ and conversely.*

We work similarly with theorem 71 instead using lemma 15.

Remarks Notice that the converse also holds, i.e. if there exists a surjective homomorphism or a weak equivalence and the naturality condition does not hold we can construct at least one proof for which the correspondence does not work.

Corollary 71. *Assume surjective homomorphism h between algebras $\mathcal{L}$, $\mathcal{L}'$ and theories $T = T_\star \cup \{\phi\}$ and $T' = T_\star \cup \{\phi'\}$ with T, T' consistent, with $\eta : A \to A'$. If a proof symmetry exists between systems $(T, \mathcal{L})$ and $(T', \mathcal{L}')$, i.e. for every proof Π^ϕ of $(\mathcal{L}, T)$ there exists Π'^ϕ of $(\mathcal{L}', T')$, then η is natural.*

Follows by contradiction: suppose there is a proof symmetry, i.e. for every proof there is a corresponding one in the new system; then we see the naturality diagram commutes. In a similar manner:

Corollary 72. *Suppose theories $T = T_\star \cup \{A\}$ and $T' = T_\star \cup \{A'\}$, such that $\eta : A \to A'$ natural. If there is a proof correspondence from system $(T, \mathcal{L})$ to $(T', \mathcal{L}')$ via a transformation τ, then $\tau = (\tau_T, \tau_L)$ satisfies the following properties:*

- *$\tau_L : \mathcal{L} \to \mathcal{L}'$ surjective*
- *$\tau(T, g \circ f) = \tau(T, g) \circ \tau(T, f)$*

8 Connections between various Hardness Assumptions

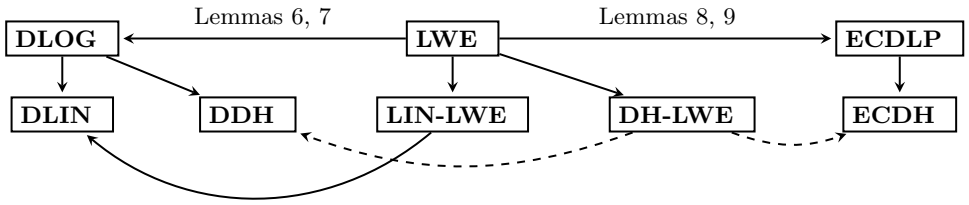


Diagram 8: Proof correspondences between LWE, DLOG, ECDH and their derivations.. Dashed lines imply partial transfomations for key exchange protocols only, as shown in the appendix (propositions C1 and C2).

In this section we give as examples the relationship between some well known and utilized computational assumptions. We construct a surjective homomorphism from lattices Z_q^n to prime group Z_p (q, p prime) and bound the magnification factor and similarly between $\mathbb{Z}_q^n$ to a curve $E(\mathbb{Z}_p)$. We use this to connect LWE to DLOG problem by showing and a natural tranformation exists. We extend this result to define a correspondences between **DH-LWE** and **DDH** and between the LWE - LIN and DLIN assumptions. Both aforementioned homomorphisms are tractable. We do not derive any efficiency guarantees.

Magninification Factor Bound First we are going to bound the magnification factor for a surjective homomorphism between prime groups.

Lemma 5. *Let surjective homomorphism $\psi : \mathbb{Z}_q^n \twoheadrightarrow \mathbb{Z}_p^m$. We can always find two primes p, q s.t. the magnification factor $\rho = \frac{q^n}{p^m}$ of ψ is subpolynomial (in fact O(1)) with the right choices of $n,\ m$.*

Proof. Consider a surjective homomorphism $\psi : \mathbb{Z}_q^n \twoheadrightarrow \mathbb{Z}_p^m$. We have $|\ker(\psi)| = \frac{|\mathbb{Z}_q^n|}{|\mathbb{Z}_p^m|}$. For adversaries $\mathcal{A}, \mathcal{B}$ assume

$$\mathrm{Adv}_{\mathcal{A}} < 1/\operatorname{poly}(s) \tag{46}$$

$$\text{Then } \mathrm{Adv}_{\mathcal{B}}(\psi \circ \sigma) = \mathrm{Adv}_{\mathcal{B}}(\psi \circ \sigma^{-1}) \leq \tag{47}$$

$$\leq \frac{q^n}{p^m} 1/\operatorname{poly}(s) = \frac{q^n}{p^m} 1/\operatorname{poly}(n \log q) \tag{48}$$

If the degree of δ polynomial bound is t we want

$$\frac{q^n}{p^m} = o(n^t \log q) \tag{49}$$

Denote the prime gap as $g_\nu = p_{\nu+1} - p_\nu$ with $p_\nu, p_{\nu+1}$ consecutive primes. We will show that we can tweak our parameters n, m to keep the maginification factor, $\frac{q^n}{p^m}$, subpolynomial (sublinear in fact), assuming large enough $p > x_0$, $x_0 \in \mathbb{N}$. Hoheisel [25] showed initially that $g_n < p_n^\theta$, for $\theta < 1$. Baker and Harman [26] with Pintz [27] improved θ to 0.525. We will consider two cases of interest here.

Case I : We can pick two primes q, p with small gap, i.e. $g_n < \max\{q, p\}$. Then $\lim_{s\to\infty} \frac{q^n}{p^m} = \frac{p^{m(1+\theta)}}{p^m} = 1$.

Case II : We pick $p >> q$ with $q^n > p$ ($m = 1$). Worst case q^n is $p_{\nu+1} - 2$. However we know there exists a prime p s.t. $p_{\nu+1} - p = g < p^\theta$. Then

$$1 \leq \lim_{s\to\infty} \frac{q^n}{p} \leq \lim_{p\to\infty} \frac{(p + p^\theta - 2)}{p} = 1 \tag{50}$$

□

Next we will define explicitly the aforementioned hardness assumptions.

Definition 17. *The Discrete Log (**DLOG**) hardness assumption system is denoted as the tuple* $((\mathcal{D}\vec{\mathcal{L}}\mathcal{OG}, \mathcal{D}\overleftarrow{\mathcal{L}}\mathcal{OG}), (\mathbb{Z}_p, *))$ *with*

$$\mathcal{D}\vec{\mathcal{L}}\mathcal{OG} = \begin{cases} y \mapsto g^y,\ y \mapsto \mathcal{U} \\ \text{id}, \quad \textit{otherwise} \end{cases} \quad \textit{and} \quad \mathcal{D}\overleftarrow{\mathcal{L}}\mathcal{OG} = \begin{cases} y \mapsto \mathcal{U}, y \mapsto g^y \\ \text{id}, \quad \textit{otherwise} \end{cases}$$

endofunctors (they map the category to itself).

Recall a functor maps game transitions.

Definition 18. *The Elliptic Curve Discrete Log (**ECDLP**) hardness assumption system is denoted as the tuple* $((\mathcal{EC}\vec{\mathcal{D}}\mathcal{LP}, \mathcal{EC}\overleftarrow{\mathcal{D}}\mathcal{LP}), (E(\mathbb{F}_q), \cdot))$ *with*

$$\mathcal{EC}\vec{\mathcal{D}}\mathcal{LP} = \begin{cases} s \times P \mapsto s \cdot P,\ s \times P \mapsto \mathcal{U} \\ \text{id}, \quad \textit{otherwise} \end{cases} \quad \textit{and} \quad \mathcal{EC}\overleftarrow{\mathcal{D}}\mathcal{LP} = \begin{cases} s \mapsto \mathcal{U}, s \mapsto s \cdot P \\ \text{id}, \quad \textit{otherwise} \end{cases}$$

endofunctors, $P \in E(\mathbb{F}_p),\ s \in \mathbb{Z}$.

Definition 19. *The Learning With Errors (**LWE**) hardness assumption system is denoted as the tuple* $((\mathcal{D}\vec{\mathcal{L}}\mathcal{WE}, \mathcal{D}\overleftarrow{\mathcal{L}}\mathcal{WE}), (\mathbb{Z}_q^n, +))$ *with*

$$\mathcal{D}\vec{\mathcal{L}}\mathcal{WE} = \begin{cases} A \times s \mapsto A \times As + e,\ s \mapsto \mathcal{U} \\ \text{id}, \quad \textit{otherwise} \end{cases} \quad \textit{and} \quad \mathcal{D}\overleftarrow{\mathcal{L}}\mathcal{WE} = \begin{cases} s \mapsto \mathcal{U},\ A \times s \mapsto A \times As + e \\ \text{id}, \quad \textit{otherwise} \end{cases}$$

endofunctors. $A \in \mathbb{Z}_q^{m \times n}, s \in \mathbb{Z}_q^{n \times 1}, e$ *noise in* $\mathbb{Z}_q^{m \times 1}$.

8.1 LWE To DLOG Proof Correspondence

Relation between $\mathbb{Z}_q^n$ and $\mathbb{Z}_p$

Lemma 6. *There is a surjective homomorphism* $(\mathbb{Z}^n/q\mathbb{Z}, +) \to (\mathbb{Z}_p, *)$ *for some* q, p *co-prime and some* $n > N$ *constant.*

Proof. Let g be generator of Z_p and

$$A = [a_0, \ldots, a_n] \in \mathbb{Z}_q^n$$

We define y s.t.

$$h(x, A) = g^{y(x,A)} \mod p = g^{\sum_{i=0}^{n-1} a_i x^{n-i-1}} \mod p$$

h homomorphism for some x. Let us set x=q.

then h is surjective as $q^n\mathbb{Z}_q + q^{n-1}\mathbb{Z}_q + \cdots + \mathbb{Z}_q \cap [0, p) = [0, p)$ for some $n > N$
given that $(kp = \alpha q + r)$ for some $k, \alpha, r < q$

We can find p from lemma 5. □

Naturality Condition

Lemma 7. *There is a natural transformation η between $\mathcal{DL}\overrightarrow{\mathcal{W}}\mathcal{E}$ and $\mathcal{DL}\overrightarrow{\mathcal{O}}\mathcal{G}$. Same for their opposite $\mathcal{DL}\overleftarrow{\mathcal{W}}\mathcal{E}$ and $\mathcal{DL}\overleftarrow{\mathcal{O}}\mathcal{G}$.*

Proof. We want to show there is η s.t. for every game transition $f : X \to Y$, $\eta_X \circ \mathcal{DL}\overrightarrow{\mathcal{W}}\mathcal{E} = \mathcal{DL}\overrightarrow{\mathcal{O}}\mathcal{G} \circ \eta_Y$. Construct η so it maps $s \mapsto U \to (A \times s \mapsto A \times As + e)$ transitions to $y \mapsto U \to (y \mapsto g^y)$. Utilizing the homomorphism $A \sum s \twoheadrightarrow g^{\sum y}$ we get the above equality for every transition f. □

8.2 LWE to ECDLP Proof Correspondence

Relation between $E(\mathbb{C})$ and $\mathbb{Z}_q^n$

Lemma 8. *There is a surjective homomorphism $(\mathbb{Z}_q^n, +) \to (E(\mathbb{Z}_p), +)$*

Proof. Assume $h_k : \mathbb{Z}_q^n \twoheadrightarrow \mathbb{Z}_k$ surjective homomorphism for $k \in \{w, m\}$, with k co-prime to w and m. We have that $E(\mathbb{Z}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/w\mathbb{Z}$.

$$\mathbb{Z}_q^{2n} \xrightarrow{\sim} \mathbb{Z}^{2n}/q\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}^n/q\mathbb{Z} \times \mathbb{Z}^n/q\mathbb{Z} \twoheadrightarrow h_m(\mathbb{Z}/m\mathbb{Z}) \times h_w(\mathbb{Z}/w\mathbb{Z}) \quad \square$$

Naturality Condition

Lemma 9. *There is a natural transformation η between $\mathcal{DL}\overrightarrow{\mathcal{W}}\mathcal{E}$ and $\mathcal{EC}\overrightarrow{\mathcal{D}}\mathcal{LP}$. Same for their opposite $\mathcal{DL}\overleftarrow{\mathcal{W}}\mathcal{E}$ and $\mathcal{EC}\overleftarrow{\mathcal{D}}\mathcal{LP}$.*

Proof. As above. □

Note lemmas 6, 7 and 8, 9 satisfy theorem 71.

Lemma 10 (LWE to DLOG proof correspondence). *There is a proof correspondence from $((\mathcal{DL}\overrightarrow{\mathcal{W}}\mathcal{E}, \mathcal{DL}\overleftarrow{\mathcal{W}}\mathcal{E}), (\mathbb{Z}_q^n, +))$ hardness assumption system to $((\mathcal{DL}\overrightarrow{\mathcal{O}}\mathcal{G}, \mathcal{DL}\overleftarrow{\mathcal{O}}\mathcal{G}), (\mathbb{Z}_p, *))$.*

Proof. We apply the main theorem 71, considering lemmas 6 and 7. □

Lemma 11 (LWE to ECDLP proof correspondence). *There is a proof correspondence from $((\mathcal{DL}\overrightarrow{\mathcal{W}}\mathcal{E}, \mathcal{DL}\overleftarrow{\mathcal{W}}\mathcal{E}), (\mathbb{Z}_q^n, +))$ hardness assumption system to $((\mathcal{EC}\overrightarrow{\mathcal{D}}\mathcal{LP}, \mathcal{EC}\overleftarrow{\mathcal{D}}\mathcal{LP}), (E(\mathbb{F}_q), \cdot))$.*

Proof follows in a similar manner.

9 Prior Work & Motivation

The literature is inundated with elaborate hardness assumptions. Pairing-based assumptions [10][28] utilizing bilinear maps have a richer repertoire of trapdoors compared to the discrete log assumption, allowing for innovative cryptographic schemes. The advent of quantum computing shed the spotlight to quantum-resistant suspected computational assumptions such as the Learning With Errors (LWE) [4], R-LWE [21] (multiple protocols proposed [29][30]) and to more intricate varieties, such as Strong Isogenes Elliptical Curves [31][32]. The fragility of security protocol design also manifested itself (see [33]). Several assumptions remain impractical; for instance, the recently suggested multilinear subgroup elimination assumption [34] does not hold for multilinear groups [35][36].

In response to the introduction of such complicated assumptions, there has been a focus to i) simplify the analysis of hardness assumptions, ii) mechanize proof generation, iii) automatically synthesize protocols. One tool for vetting the plausibility of an assumption is the generic group model, introduced by Nechaev [37] and Shoup [38]. The generic group model, like the random oracle model, exposes group operations only, hiding intrinsic group structure – the adversary thus can not exploit any properties of the particular group. It is inadequate, however, for evaluating and comparing a new hardness assumption with past work; we miss the tangible link between the different group structures.

Naor [39] suggested the notion of falsifiability, the ability to efficiently verify an adversary's success of breaking the hardness assumption. This allows one to validate whether a proposed computational assumption encompasses the security proof in question. One can then reason about the protocol's provable security. This notion was later extended and simplified by Gentry and Wichs [40]. Goldwasser and Kalai [20] took a step further classifying assumptions into general and concrete, search and decision ones. In this paper we focus primarily on concrete computational hardness assumptions. Our results though naturally extend to generic ones. Boneh et al. introduced a master theorem to vet and associate bilinear pairing assumptions – utilized initially in [41] and detailed in [42]. Barthe et al. in [24] took a step further and introduced a mechanized algorithm for reducing and falsifying hardness assumptions under the generic group model to well-established basic assumptions.

This semi-automated verification is inspired by [43], where Halevi envisioned and argued the need for computer-assisted cryptographic proofs. This vision has seen other recent advances – Easycrypt [44][45][46][17] provides proof assistance by reducing game equivalence of probabilistic Hoare logic to SMT statements. Building on Halevi's dream, one could imagine the scenario where one provides a proof based on an incorrect premise or asking for a protocol alteration or refinement: the proof assistant would derive the new proofs of security and correctness based on the original proof.

These aspects remain unattainable, however, as the nature of formal proof generation is still laborious. Currently, the user first needs to provide a sequence of games and a series of asserted lemmas. The tool reduces game equivalence to a series of subgoal lemmas solved via SMT solver and user collaboration. Altering

a hardness assumption or an assertion implies re-validation and rewriting a substantial subset of the goals. As a result, formal verification is an afterthought for completeness for the cryptographer, instead of an integral design step of the thought process.

Automated protocol synthesis algorithms like recent work of Hoang, Katz and Malozemoff [47] aim to solve this problem via automated synthesis. However, the synthesis is based on an authenticated encryption template, which entails a final validation step which ensures soundness along with other desired properties.

Another approach is translation between systems. Akineyele, Garman and Hohenberger [48] provide a translation tool between Type I ($G = \hat{G}$) to Type III (no tractable homomorphism between $G, \hat{G}$ and vice versa) pairing schemes.

In comparison, we reduce transformations of proofs between different computational assumptions down to algebraic requirements. As a result our work is not restricted to a particular protocol type or class of assumptions, as in the above work focused only on pairing schemes. Proof similarities between different systems have been noted before. Our inspiration stems from Kurosawa et al. [2] – they produced an IBE protocol under the DLIN intractability assumption similar in structure to previous work of Agrawal et al. [49]. They note certain similarities may be the result of a connection of DLIN and LWE systems.

The general idea of establishing protocol existence via algebraic properties is not new either; earlier Ostrovsky and Skeith III [50][12] derived constraints on fully homomorphic encryption based on cardinality bounds between maps to provide an impossibility result. Barto in his work [51][52] uses the symmetry provided by the existence of polymorphisms (e.g. Taylor) for CSP instances to prove they can be solved in polynomial time. In this work we take a step further, establishing classes of hardness assumptions.

References

1. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive **2004** (2004) 332
2. Kurosawa, K., Trieu Phong, L.: Leakage resilient ibe and ipe under the dlin assumption. In Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R., eds.: Applied Cryptography and Network Security. Volume 7954 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 487–501
3. Pass, R., Seth, K., Telang, S.: Indistinguishability obfuscation from semantically-secure multilinear encodings. In: International Cryptology Conference, Springer (2014) 500–517
4. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) **56**(6) (2009) 34
5. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the forty-first annual ACM symposium on Theory of computing, ACM (2009) 333–342
6. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: Proceedings of the forty-fifth annual ACM symposium on Theory of computing, ACM (2013) 575–584

7. Blum, A., Kalai, A., Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM (JACM) **50**(4) (2003) 506–519
8. Pandey, O., Pass, R., Vaikuntanathan, V.: Adaptive one-way functions and applications. In: Annual International Cryptology Conference, Springer (2008) 57–74
9. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Advances in Cryptology–CRYPTO 2004, Springer (2004) 41–55
10. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Annual International Cryptology Conference, Springer (2001) 213–229
11. Döttling, N., Garg, S.: Identity-based encryption from the diffie-hellman assumption. In: Annual International Cryptology Conference, Springer (2017) 537–569
12. Ostrovsky, R., Skeith Iii, W.E.: Communication complexity in algebraic two-party protocols. In: Annual International Cryptology Conference, Springer (2008) 379–396
13. Hoare, C.A.R., et al.: Communicating sequential processes. Volume 178. Prentice-hall Englewood Cliffs (1985)
14. Abadi, M., Gordon, A.D.: A calculus for cryptographic protocols: The spi calculus. In: Proceedings of the 4th ACM conference on Computer and communications security, ACM (1997) 36–47
15. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on, IEEE (2001) 136–145
16. Nowak, D.: A framework for game-based security proofs. In: International Conference on Information and Communications Security, Springer (2007) 319–333
17. Barthe, G., Grégoire, B., Zanella Béguelin, S.: Formal certification of code-based cryptographic proofs. ACM SIGPLAN Notices **44**(1) (2009) 90–101
18. Diffie, W., Hellman, M.E.: New directions in cryptography. Information Theory, IEEE Transactions on **22**(6) (1976) 644–654
19. Boneh, D.: The decision diffie-hellman problem. In: Algorithmic number theory. Springer (1998) 48–63
20. Goldwasser, S., Kalai, Y.T.: Cryptographic assumptions: A position paper. In: Theory of Cryptography Conference, Springer (2016) 505–522
21. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. Journal of the ACM (JACM) **60**(6) (2013) 43
22. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of computation **48**(177) (1987) 203–209
23. Li, H., Chong, E.K.: On connections between group homomorphisms and the ingleton inequality. In: 2007 IEEE International Symposium on Information Theory, IEEE (2007) 1996–1999
24. Barthe, G., Fagerholm, E., Fiore, D., Mitchell, J., Scedrov, A., Schmidt, B.: Automated analysis of cryptographic assumptions in generic group models. In: International Cryptology Conference, Springer (2014) 95–112
25. Hoheisel, G.: Primzahlprobleme in der analysis... Walter de Gruyter. (1930)
26. Baker, R.C., Harman, G.: The difference between consecutive primes. Proceedings of the London Mathematical Society **3**(2) (1996) 261–280
27. Baker, R.C., Harman, G., Pintz, J.: The difference between consecutive primes, ii. Proceedings of the London Mathematical Society **83**(3) (2001) 532–562
28. Boldyreva, A., Gentry, C., O'Neill, A., Yum, D.H.: Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. In: Proceedings of the 14th ACM conference on Computer and communications security, ACM (2007) 276–285

29. Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In: Security and Privacy (SP), 2015 IEEE Symposium on, IEEE (2015) 553–570
30. Costello, C., Longa, P., Naehrig, M.: Efficient algorithms for supersingular isogeny diffie-hellman
31. Galbraith, S., Stolbunov, A.: Improved algorithm for the isogeny problem for ordinary elliptic curves. Applicable Algebra in Engineering, Communication and Computing **24**(2) (2013) 107–131
32. Childs, A., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology **8**(1) (2014) 1–29
33. Koblitz, N., Menezes, A.: The brave new world of bodacious assumptions in cryptography. Notices of the American Mathematical Society **57**(3) (2010) 357–365
34. Gentry, C., Lewko, A.B., Sahai, A., Waters, B.: Indistinguishability obfuscation from the multilinear subgroup elimination assumption. In: Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on, IEEE (2015) 151–170
35. Minaud, B., Fouque, P.A.: Cryptanalysis of the new multilinear map over the integers. IACR Cryptology ePrint Archive **2015** (2015) 941
36. Cheon, J.H., Fouque, P.A., Lee, C., Minaud, B., Ryu, H.: Cryptanalysis of the new clt multilinear map over the integers. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer (2016) 509–536
37. Nechaev, V.I.: Complexity of a determinate algorithm for the discrete logarithm. Mathematical Notes **55**(2) (Feb 1994) 165–172
38. Shoup, V. In: Lower Bounds for Discrete Logarithms and Related Problems. Springer Berlin Heidelberg, Berlin, Heidelberg (1997) 256–266
39. Naor, M.: On cryptographic assumptions and challenges. In: Annual International Cryptology Conference, Springer (2003) 96–109
40. Gentry, C., Wichs, D.: Separating succinct non-interactive arguments from all falsifiable assumptions. In: Proceedings of the forty-third annual ACM symposium on Theory of computing, ACM (2011) 99–108
41. Boneh, D., Boyen, X., Goh, E.J.: Hierarchical identity based encryption with constant size ciphertext. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer (2005) 440–456
42. Boyen, X.: The uber-assumption family. In: International Conference on Pairing-Based Cryptography, Springer (2008) 39–56
43. Halevi, S.: A plausible approach to computer-aided cryptographic proofs. IACR Cryptology ePrint Archive **2005** (2005) 181
44. Barthe, G., Grégoire, B., Heraud, S., Béguelin, S.Z.: Computer-aided security proofs for the working cryptographer. In: Annual Cryptology Conference, Springer (2011) 71–90
45. Barthe, G., Crespo, J.M., Grégoire, B., Kunz, C., Lakhnech, Y., Schmidt, B., Zanella-Béguelin, S.: Fully automated analysis of padding-based encryption in the computational model. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM (2013) 1247–1260
46. Barthe, G., Grégoire, B., Béguelin, S.Z.: Probabilistic relational hoare logics for computer-aided security proofs. In: International Conference on Mathematics of Program Construction, Springer (2012) 1–6
47. Hoang, V.T., Katz, J., Malozemoff, A.J.: Automated analysis and synthesis of authenticated encryption schemes. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM (2015) 84–95

48. Akinyele, J.A., Garman, C., Hohenberger, S.: Automating fast and secure translations from type-i to type-iii pairing schemes. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM (2015) 1370–1381
49. Agrawal, S., Boneh, D., Boyen, X.: Lattice basis delegation in fixed dimension and shorter ciphertext hierarchical ibe. In: Proc. of Crypto'10. Volume 6223 of LNCS. (2010) 98–115
50. Ostrovsky, R., Skeith III, W.E.: Algebraic lower bounds for computing on encrypted data. IACR Cryptology ePrint Archive **2007** (2007) 64
51. Barto, L.: The constraint satisfaction problem and universal algebra. The Bulletin of Symbolic Logic (2015) 319–337
52. Barto, L., Kozik, M., Niven, T.: Graphs, polymorphisms and the complexity of homomorphism problems. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. STOC '08, New York, NY, USA, ACM (2008) 789–796
53. Rabin, M.O.: How to exchange secrets with oblivious transfer. IACR Cryptology ePrint Archive **2005** (2005) 187
54. Kilian, J.: Founding crytpography on oblivious transfer. In: Proceedings of the twentieth annual ACM symposium on Theory of computing, ACM (1988) 20–31
55. Naor, M., Pinkas, B.: Efficient oblivious transfer protocols. In: Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms, Society for Industrial and Applied Mathematics (2001) 448–457
56. Naor, M., Pinkas, B.: Oblivious transfer and polynomial evaluation. In: Proceedings of the thirty-first annual ACM symposium on Theory of computing, ACM (1999) 245–254
57. Naor, M., Pinkas, B.: Oblivious transfer with adaptive queries. In: Advances in Cryptology—CRYPTO'99, Springer (1999) 573–590
58. Ding, J., Xie, X., Lin, X.: A simple provably secure key exchange scheme based on the learning with errors problem. IACR Cryptology ePrint Archive **2012** (2012) 688
59. Peikert, C.: Lattice cryptography for the internet. In: International Workshop on Post-Quantum Cryptography, Springer (2014) 197–219
60. Singh, V.: A practical key exchange for the internet using lattice cryptography. IACR Cryptology ePrint Archive **2015** (2015) 138
61. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange-a new hope. In: USENIX Security Symposium. Volume 2016. (2016)
62. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Theory of Cryptography Conference, Springer (2009) 474–495
63. Boneh, D., Papakonstantinou, P., Rackoff, C., Vahlis, Y., Waters, B.: On the impossibility of basing identity based encryption on trapdoor permutations. In: Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on, IEEE (2008) 283–292
64. Yao, A.C.: Protocols for secure computations. In: Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on, IEEE (1982) 160–164

A Lemmas for Theorem 72

Next we show that faithful functors reflect semantic security and a proof equivalence arises in the case of equivalence of two proof categories. This extends our results to arbitrary algebras. The lemmas below conclude to theorem 72.

A.1 Soundness preserving Functors

Lemma 12. *Given a functor $F : \mathcal{C} \to \mathcal{D}$ we can construct functor $F' : P(C) \to D$ that preserves soundness, i.e. for any $u, v \in \mathrm{Morph}(\mathcal{C})$*

$$\Pr_{x \xleftarrow{R} X, X \in \mathrm{Obj}(C)} [u(x) = v(x)] \geq 1 - \epsilon \Rightarrow \tag{51}$$

$$\Pr_{z \xleftarrow{R} F(X)} [F(u)(z) = F(v)(z)] \geq (1 - \epsilon) \tag{52}$$

for arbitrary ϵ.

A.2 Faithful functors reflect indistinguishability

Similarly, we can make a contrapositive statement assuming a reflective transformation. Suppose the assertion A_H is indistinguishable from random for an adversary $\mathcal{A}$ – see diagram 4. If transformation h reflects indistinguishability and $h \circ A = A_H$, then A is also indistinguishable for $\mathcal{A}_{\mathcal{C}}$.

Lemma 13. *Let $\mathcal{A}, D, \mu$ PPT algorithms, X game.* $\mathrm{Adv}_{\mathcal{A}}(u, v) \leq \delta$ *for all $\mathcal{A}$ is equivalent to*

$$\forall D \forall \mu : \Pr_{x \sim X} [D(u \circ \mu(x)) = D(v \circ \mu(x))] \geq 1 - \delta \tag{53}$$

$\mu : X \to X$.

Proof. Proved by contradiction. Assume there is a distinguisher pair for which $\Pr_{x \xleftarrow{R} X} [D(u \circ \mu(x)) = D(v \circ \mu(x))] < 1 - \delta$ then we can build an adversary with advantage greater than δ. Converse follows similarly.

□

Lemma 14. *Suppose there is a faithful functor $F : C \to D$ and for some $f, g : X \to Y \in \mathrm{Morph}(C)$ it holds:* $\mathrm{Adv}_{\mathcal{A}}(f, g) \leq \kappa$ *for all $\mathcal{A}$ PPT algorithms in C. Also $F(X) \sim X$. Then it holds that* $\mathrm{Adv}_{\mathcal{A}_C}(F \circ f, F \circ g) \leq \kappa$, *for all $\mathcal{A}_C$ PPT.*

The result follows by applying the puncturing method, lemma 13 and faithful functor definition.

A.3 Weak equivalence preserves indistinguishability

Consider a functor $F : C \to D$ between C, D locally small categories. F implies the $F_{X,Y} : \hom_C(X, Y) \to \hom_D(F(X), F(Y))$ mapping.

Definition 20. *F is a full functor if and only if $F_{X,Y}$ is surjective for each set of mappings $(F(X), F(Y))$.*

Definition 21. *F is a faithful functor if and only if each function $F_{X,Y}$ is injective.*

Definition 22. *Let C, D proof categories. A strong translator is an injective on game transitions (faithful) proof transformation $\tau_C^D : C \to D$. Namely for all games $f, g \in \mathrm{Obj}(C)$ if $\tau_C^D \circ g = \tau_C^D \circ f$ then $f = g$ and*

$$f \simeq_c g \Leftrightarrow \tau_C^D \circ f \simeq_c \tau_C^D \circ g$$

$\simeq_c$ denotes computational indistinguishability.

We remark here that a strong translator also preserves the proof structure, i.e. all subproofs are also valid.

Lemma 15. *A full and faithful functor $F : C \to D$ with a left adjoint $G : D \to C$ is a strong translator τ_D^C.*

The existence of a full and faithful functor with a left adjoint implies weak equivalence of the two categories. Recall then that F is object surjective. We state the proof in the next section.

B Supplemental Proofs

Deferred proofs follow.

B.1 Proof of lemma 12

Puncturing method Given a concrete category C with functions $u, v : X \to Y$ as morphisms and functor $F : C \to D$ for which holds

$$\begin{aligned} r \leq & \Pr_{x \xleftarrow{R} X, X \in \mathrm{Obj}(C)}[u(x) = v(x)] = \\ = & \Pr_{\tilde{v}_r, \tilde{x} \in X, X \in \mathrm{Obj}(C)}[u(\tilde{x}) = \tilde{v}_r(\tilde{x})] \end{aligned}$$

We construct P(C) with

$$\tilde{v}_r = \begin{cases} u, & \text{with probability r} \\ v_{\sim u} \ s.t. u \neq v_{\sim u}, & \text{otherwise} \end{cases}$$

Then we have

$$\begin{aligned} \Pr_{x \xleftarrow{R} X, X \in \mathrm{Obj}(C)}[F(u(x)) = F(v(x))] &= \frac{1}{\|Z\|} \sum_{z \in Z} \mathbb{1}(F(u)(z) = F(\tilde{v}_r)(z)) \\ &= \frac{1}{\|Z\|}(r\|Z\| + (1-r)\mathbb{1}(F(u)(z) = F(\tilde{v}_{\sim u})(z)) \geq r \end{aligned}$$

Lemma 12. *Given a functor $F : \mathcal{C} \to \mathcal{D}$ we can construct functor $F' : P(C) \to D$ that preserves soundness, i.e. for any $u, v \in \mathrm{Morph}(\mathcal{C})$*

$$\Pr_{x \xleftarrow{R} X, X \in \mathrm{Obj}(C)}[u(x) = v(x)] \geq 1 - \epsilon \Rightarrow \tag{51}$$

$$\Pr_{z \xleftarrow{R} F(X)}[F(u)(z) = F(v)(z)] \geq (1 - \epsilon) \tag{52}$$

for arbitrary ϵ.

We use next this insight in the proof of lemma 14. Note $P(C) \subseteq C$, as every game in $\mathrm{Morph}(P(C))$ is by definition also a morphism of C. Note also that if we have essential surjectivity, i.e. object surjectivity, equality holds.

B.2 Proof of lemma 13

Lemma 13. *Let $\mathcal{A}, D, \mu$ PPT algorithms, X game.* $\mathrm{Adv}_{\mathcal{A}}(u, v) \leq \delta$ *for all $\mathcal{A}$ is equivalent to*

$$\forall D \forall \mu : \Pr_{x \sim X}[D(u \circ \mu(x)) = D(v \circ \mu(x))] \geq 1 - \delta \tag{53}$$

$\mu : X \to X$.

Proof. Suppose a game X and two game transitions u, v. Let us assume

$$\forall \mathcal{A} : \quad \delta > \Pr_{x \sim X}[\mathcal{A}(v)(x) = e] - \Pr_{x \sim X}[\mathcal{A}(u)(x) = e] = \tag{54}$$

$$= \Pr_{x \sim X}[\mathbb{1}(\mathcal{A}(v)(x) = e) - \mathbb{1}(\mathcal{A}(v)(x) = e)] \tag{55}$$

($\mathbb{1}$ the indicator function). Denote $\Delta(\mathcal{A}, c)(u) = \begin{cases} e, & \mathcal{A}(u) = e \\ c, & \text{otherwise} \end{cases}$ Then:

$$\Pr_{x \sim X}[\mathcal{A}(v) = e] - \Pr_{x \sim X}[\mathcal{A}(u) = e] = \tag{56}$$

$$= \Pr[\mathbb{1}(\Delta(\mathcal{A}, 2)(u)(x) \neq \Delta(\mathcal{A}, 3)(v)(x))] = \tag{57}$$

$$= 1 - \Pr[\mathbb{1}(\Delta(\mathcal{A}, 2)(u)(x) = \Delta(\mathcal{A}, 3)(v)(x)] \tag{58}$$

for some PPT μ. If there is a pair of (D, μ) s.t.

$$\Pr_{x \sim X}[D(u \circ \mu(x)) = D(v \circ \mu(x))] \leq 1 - \delta \tag{59}$$

then

$$\delta \leq 1 - \Pr_{x \sim X}[D(u \circ \mu(x)) = D(v \circ \mu(x))] = \tag{60}$$

$$= \Pr_{x \sim X}[\mathbb{1}(D(u \circ \mu(x)) \neq D(v \circ \mu(x)))] \tag{61}$$

$$= \Pr_{x \sim X}[\mathbb{1}(B(x, u) \neq B(x, v))] \tag{62}$$

Suppose an adversary $A'_v(u)(x) = \mathbb{1}(B(x, u) \neq B(x, v))$ with v as a parameter. Its advantage then is greater than δ; this contradicts our initial assumption. Similarly if there is an adversary with advantage greater than δ we can construct a pair(D', μ') with $\Pr_{x \sim X}[D'(u \circ \mu'(x)) = D'(v \circ \mu'(x))] \leq 1 - \delta$. □

B.3 Proof of lemma 14

Lemma 14. *Suppose there is a faithful functor $F : C \to D$ and for some $f, g : X \to Y \in \mathrm{Morph}(C)$ it holds: $\mathrm{Adv}_{\mathcal{A}}(f, g) \leq \kappa$ for all $\mathcal{A}$ PPT algorithms in C. Also $F(X) \sim X$. Then it holds that $\mathrm{Adv}_{\mathcal{A}_C}(F \circ f, F \circ g) \leq \kappa$, for all $\mathcal{A}_C$ PPT.*

Proof. Suppose for all adversaries $\mathcal{A}$:

$$\kappa \leq \mathrm{Adv}_{\mathcal{A}}(f, g) = \tag{63}$$

$$= 1 - \Pr_{x \sim X}[D(f \circ \mu(x)) = D(g \circ \mu(x))] \forall D,\ \mu \tag{64}$$

Also for all adversaries:

$$\kappa \geq \mathrm{Adv}_{\mathcal{A}}(F \circ f, F \circ g) \tag{65}$$

By definition of faithfulness we have that

$$F \circ u = F \circ v \Rightarrow u = v \tag{66}$$

as it holds that

$$\mathrm{Morph}(X, Y) \to \mathrm{Morph}(F \circ X, F \circ Y) \tag{67}$$

is an injection. We have due to eq. (65)

$$\forall D, \mu :\ 1 - \kappa \leq \Pr_{z \sim F(X)}[D(F \circ f \circ \mu(z)) = D(F \circ g \circ \mu(z))] \tag{68}$$

$$\Leftrightarrow \kappa \geq \mathrm{Adv}_{\mathcal{A}}(F \circ f, F \circ g) \tag{69}$$

It holds that $\forall D', \mu' \in \mathrm{Morph}(C)$ there are D, μ s.t.:

$$F(D') = D,\ F(\mu') = \mu \tag{70}$$

Hence

$$\Pr_{z \sim F(X)}[F(D' \circ f \circ \mu')(z) = F(D' \circ g \circ \mu')(z)] \tag{71}$$

$$= \sum_{z \in F(X)} \mathbb{1}(F(D' \circ f \circ \mu')(z) = F(D' \circ g \circ \mu')(z)) p_z \tag{72}$$

We have that distributions $F(X)$, X are similar, thus there is subset $A' \subseteq A$ and $B' \subseteq B$ with $A \simeq B$ s.t.

$$F(X) = (B, \sigma(B), P) \text{ and } X = (A, \sigma(A), P) \text{ s.t.} \tag{73}$$

$$S = (A', \sigma(A'), P) \text{ and } U = (B', \sigma(B'), P) \tag{74}$$

By definition $S \in \mathrm{Obj}(C),\ U \in \mathrm{Obj}(D)$ thus:

$$\sum_{z \in F(X)} \mathbb{1}(F(D' \circ f \circ \mu')(z) = F(D' \circ g \circ \mu')(z))p_z \tag{75}$$

$$= \sum_{z \in U} \mathbb{1}(F(D' \circ f \circ \mu')(z) = F(D' \circ g \circ \mu')(z))p_z + \tag{76}$$

$$\sum_{z \in U^c} \mathbb{1}(F(D' \circ f \circ \mu')(z) = F(D' \circ g \circ \mu')(z))p_z \tag{77}$$

$$= \sum_{x \in S} \mathbb{1}(F(D' \circ f \circ \mu')(x) = F(D' \circ g \circ \mu')(x))p_x + 0 \tag{78}$$

$$= \sum_{x \in S} \mathbb{1}(D' \circ f \circ \mu'(x) = D' \circ g \circ \mu'(x))p_x \tag{79}$$

$$= \Pr_{x \sim S}(D' \circ f \circ \mu(x) = D' \circ g \circ \mu(x)) \tag{80}$$

$$\geq \Pr_{x \sim X}(D' \circ f \circ \mu(x) = D' \circ g \circ \mu(x)) = \tag{81}$$

$$= 1 - \mathrm{Adv}_{\mathcal{A}}(f, g) \tag{82}$$

□

B.4 Proof of lemma 15

Lemma 15. *A full and faithful functor $F : C \to D$ with a left adjoint $G : D \to C$ is a strong translator τ_D^C.*

Proof. Note that by definition the existence of a full and faithful functor with a left adjoint implies weak equivalence of the two categories. Recall then that $F : C \to D$ is essentially (object) surjective. That means

$$\forall y \in \mathrm{Obj}(D),\ \exists x :\ F(x) \simeq y \tag{83}$$

We have that G is full and faithful from D to C and for all objects $y \in \mathrm{Obj}(C)$ it holds that

$$\exists x \in \mathrm{Obj}(D) :\ G(x) \simeq y \Rightarrow |G(x)| = |y| \tag{84}$$

Then we apply lemma 14. If for all adversaries:

$$\mathrm{Adv}_{\mathcal{A}}(u, v) \leq \kappa,\ u, v \in \mathrm{Morph}(C) \tag{85}$$

then for all adversaries it also holds $\mathrm{Adv}_{\mathcal{A}}(G \circ u, G \circ v) \leq \kappa$ for any distribution of $y \in \mathrm{Obj}(D)$ as it is isomorphic to a $x \in \mathrm{Obj}(C)$. Converse follows in exactly the same way for left adjoint. □

C Selected Step by Step Examples

Oblivious Transfer: Oblivious Transfer was introduced by Rabin under the RSA assumption in 1981 [53]. Kilian showed later in [54] the completeness of the primitive. Naor and Pinkas produced a more efficient protocol in [55].

C.1 Outline

In this section we first present an Oblivious Transfer construction and proof of security based on ring-LWE. We then proceed and derive the original Naor-Pinkas Oblivious Transfer (1 out of 2), as introduced in [56][57] under the CDH assumption. Furthermore, we derive a construction under the ECDH hardness assumption. Observe that there are no natural transformations between the two hardness assumptions. We show how to utilize lemma 3 and show we can construct each game transition.

The Ring-LWE assumption was introduced initially by Singh in [58] and later improved by Peikert [59] and [60] to construct a generic key-exchange primitive for lattice-based cryptography; Bos, Costello, Naehrig and Stebilla introduced later a TLS implementation utilizing DH-LWE in [29] and later by Alkim, Ducas and Pöppelmann in [61]. For convenience, we define below the abstract DH-LWE assumption, based on the [59][29] DDH-like problem of R-LWE.

We explicitly define the problem below:

Definition 23. *DH-LWE problem and hardness assumption system Let q be the integer modulus and χ a distribution over $\mathbb{Z}$. We define the DH-LWE hardness assumption as follows:*

$$\mathrm{Adv}_{\mathcal{A}}((A, As+n, yA+n', yAs+n''), (A, As+n, yA+n', \mathcal{U})) < \frac{1}{s^{O(1)}} \quad (86)$$

s security variable, $A \in \mathbb{Z}_p^{n\times n}$, $s \in \mathbb{Z}_p^n, y \in \mathbb{Z}_p^{1\times n}, \mathcal{U} \xleftarrow{R} \mathbb{Z}_p$.

Now we can define the hardness assumption system to work on:

Definition 24. *The Learning With Errors (**DH-LWE**) hardness assumption system is denoted as the tuple $((\mathcal{DH} \overset{\rightarrow}{-} \mathcal{LWE}, \mathcal{DH} \overset{\leftarrow}{-} \mathcal{LWE}), (\mathbb{Z}_q^n, +))$ with*

$$\mathcal{DH} \overset{\rightarrow}{-} \mathcal{LWE} = \begin{cases} A \times s \times y \mapsto A \times yAs + e, \ s \times y \mapsto \mathcal{U} \\ \mathrm{id}, \quad \textit{otherwise} \end{cases}$$

and

$$\mathcal{DH} \overset{\leftarrow}{-} \mathcal{LWE} = \begin{cases} s \times y \mapsto \mathcal{U}, \ A \times s \times y \mapsto A \times yAs + e \\ \mathrm{id}, \quad \textit{otherwise} \end{cases}$$

endofunctors. $A \in \mathbb{Z}_q^{m\times n}, s \in \mathbb{Z}_q^{n\times 1}, y \in \mathbb{Z}^{1\times 1}$ e noise in $\mathbb{Z}_q$.

Unlike Peikert's definition we define specificallly over $\mathbb{Z}$. Next we can derive a basic transformation between the hardness assumptions. Note there is no natural one.

Proposition C1 (DH-LWE to CDH hardness assumption system transformation)**.** *There is a transformation η for key exchange primitives between $\mathcal{DH} \overset{\rightarrow}{-} \mathcal{LWE}$ and $\mathcal{C}\overset{\rightarrow}{\mathcal{DH}}$. Same for their opposite $\mathcal{DH} \overset{\leftarrow}{-} \mathcal{LWE}$ and $\mathcal{C}\overset{\leftarrow}{\mathcal{DH}}$.*

Proof. We construct the transformation as

$$\vec{\mathcal{CDH}} \circ G \circ \mathcal{DH} - \overleftarrow{\mathcal{LWE}} \tag{87}$$

where G is a mapping $\mathbb{Z}_p^n \to \mathbb{Z}_q$ that resamples random variables from the matrix group to $\mathbb{Z}_q$. Notice by definition of R-LWE and DH

$$(yA)s + n \cong y(As) + n \leftrightarrow (g^b)^a = (g^a)^b \tag{88}$$

the key exchange case is preserved. □

Similarly:

Proposition C2 (DH-LWE to ECDH hardness assumption system transformation)**.** *There is a transformation η for key exchange primitives between $\mathcal{DH} - \vec{\mathcal{LWE}}$ and $\mathcal{ECDH}$. Same for their opposite $\mathcal{DH} - \overleftarrow{\mathcal{LWE}}$ and $\mathcal{EC}\overleftarrow{\mathcal{DH}}$.*

C.2 Reconstructing Oblivious Transfer under CDH assumption from DH-LWE Oblivious Transfer protocol

Diagrams 9f to 9d present a proof of security for Oblivious Transfer under the Learning With Errors assumption, while 9c to 9a the new (re-)derivation of sender's security proof for the original Naor-Pinkas oblivious Transfer protocol [55].

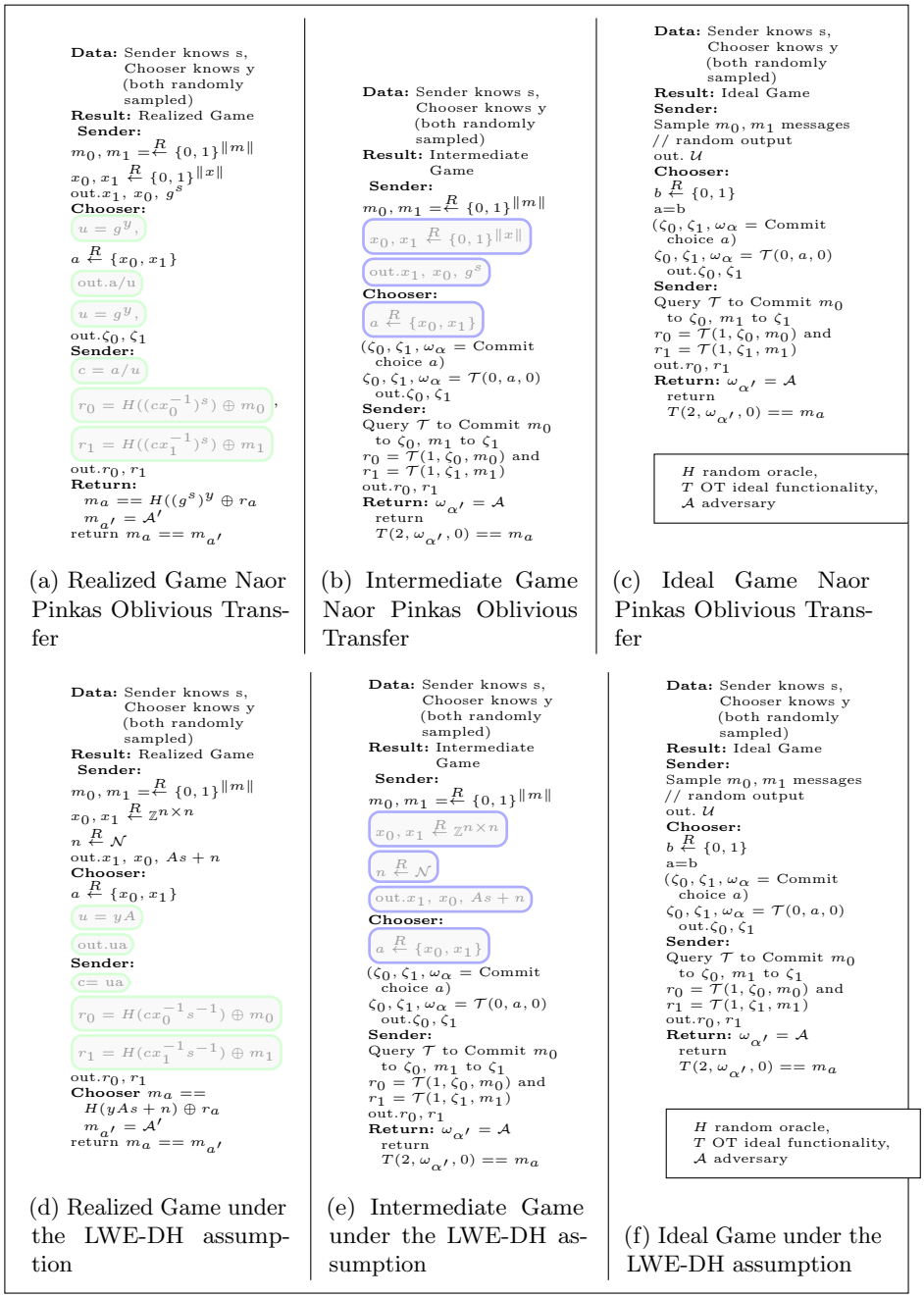
The proposed protocol as the reader can see had information theoretic security for the Chooser and computational indistinguishability for the Sender's security. It is worth noting that first chooser response is constructed in a similar fashion as [29], deriving an equivalent to elliptical curve diffie hellman (ECDH) key exchange primitive.

Ideal Functionality To describe the ideal game we utilize the following ideal functionality:

$$\mathcal{T}(e,x,y) = \begin{cases} \zeta_0 \xleftarrow{R} \mathcal{U}, \zeta_1 \xleftarrow{R} \mathcal{U}, \omega_x, & \text{if } e == 0 \\ 1 \text{ and set } z \text{ for } \omega_x), & \text{if } e == 1 \wedge (x == \zeta_0 \vee x == \zeta_1) \\ m_a, & \text{if } e == 2 \wedge x == \omega_a \\ \perp, & \text{otherwise} \end{cases} \tag{89}$$

U the sampling universe.

Hybrid Game $\mathcal{H}_0'$ to $\mathcal{H}_1'$ From the ideal game 9f to game 9e, we make the following changes. First we modify the $b \xleftarrow{R} \{0,1\}$ to sample x_0, x_1 instead. Sender generates choices x_0, x_1 and sends them to the chooser. We remove the assignment of b to a to a coin flip between x_0 and x_1. We also sample noise n and secret s the sender returns also $As + n$. Due to the hardness assumption the adversary has negligigle advantage distinguishing between the two games.



(a) Realized Game Naor Pinkas Oblivious Transfer

(b) Intermediate Game Naor Pinkas Oblivious Transfer

(c) Ideal Game Naor Pinkas Oblivious Transfer

(d) Realized Game under the LWE-DH assumption

(e) Intermediate Game under the LWE-DH assumption

(f) Ideal Game under the LWE-DH assumption

Diagram 9: Games 9a to 9c show the original Naor- Pinkas Sender security proof. A Chooser able to acquire both messages can solve the CDH problem. Games 9d to 9f depict the LWE-DH proof for the Sender. H denotes the random oracle.

Hybrid Game $\mathcal{H}_1'$ to $\mathcal{H}_2'$ At this step we remove the ideal functionality. First, instead of querying $T(0, a, 0)$, the chooser samples a secret y and computes $u = yA$ and au. The substitution can be written as $u = \mathcal{DH} \overleftarrow{-} \mathcal{LWE}(\mathbb{I}, y)$. The change is distinguishable with negligible advantage due to the LWE hardness assumption. Next we query the random oracle with two different values. As the sender does not know y any adversary that can compute the inverse of s can break the search LWE problem with non-negligible probability. Note we assert the random oracle in this construction tolerates up to small noise (up to $q/4$) for convenience.

Rederiving Naor Pinkas Oblivious Transfer Proof of security

Hybrid Game $\mathcal{H}_0'$ ***to*** $\mathcal{H}_1'$ The transformation from the original game transition is straightforward. As DH-LWE does not hold we apply the $\mathcal{DH} \overrightarrow{-} \mathcal{LWE} \rightarrow \overrightarrow{\mathcal{CDH}}$ transformation. Observe on a second pass we need to remove the noise sampling n added, as it is not relevant anymore and becomes dead code. Applying $h : \mathbb{Z}_q^n \twoheadrightarrow \mathbb{Z}_p$ preserves the distributions due to lemmas 3 2.

Hybrid Game $\mathcal{H}_1'$ ***to*** $\mathcal{H}_2'$ Note we modify the transition to exponentiate to y^{-1} instead and continue as above.

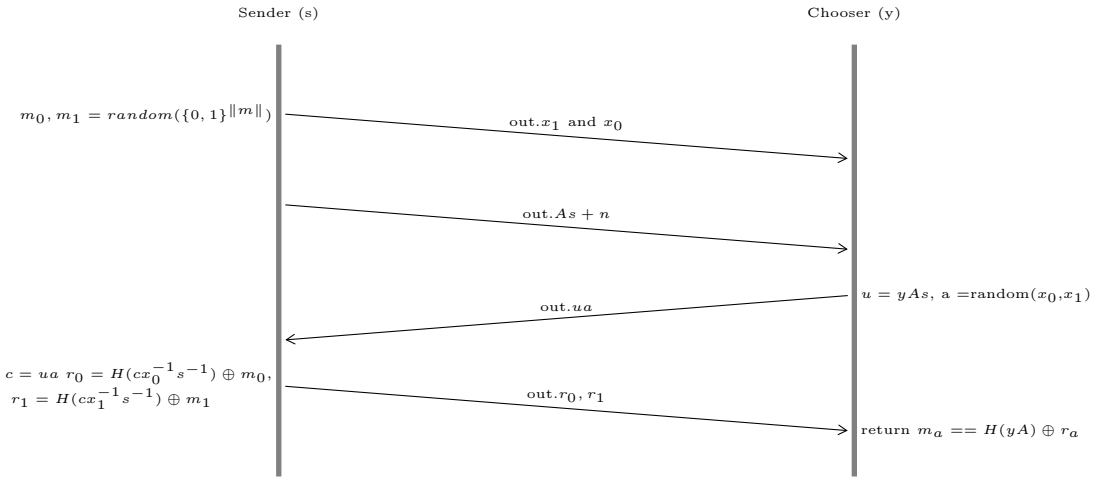


Diagram 10: Original 1-2 Oblivious Transfer under the DH-LWE assumption

Protocol Diagrams The reader can now see the original Naor Pinkas 1-2 Oblivious Transfer in diagram 11 and an oblivious transfer under the DH-LWE assumption in diagram 10.

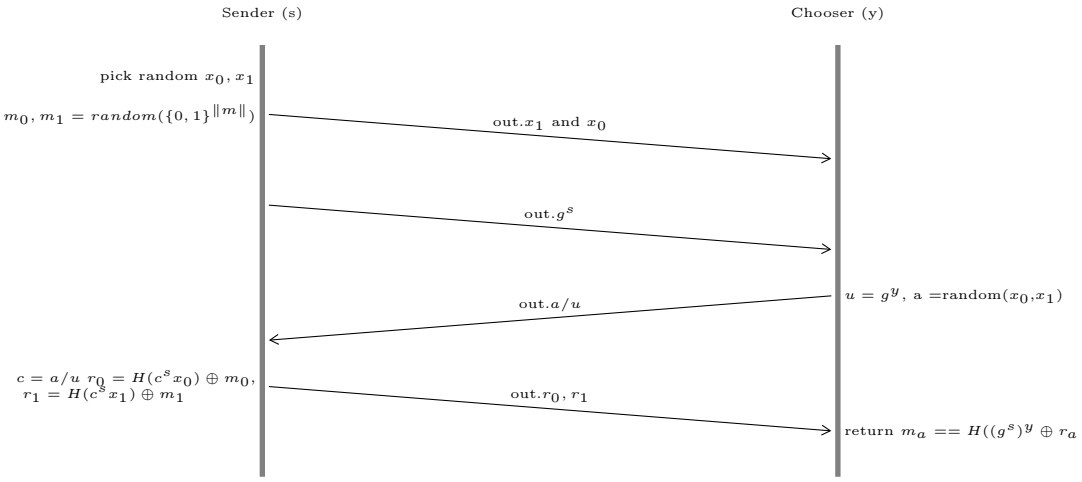


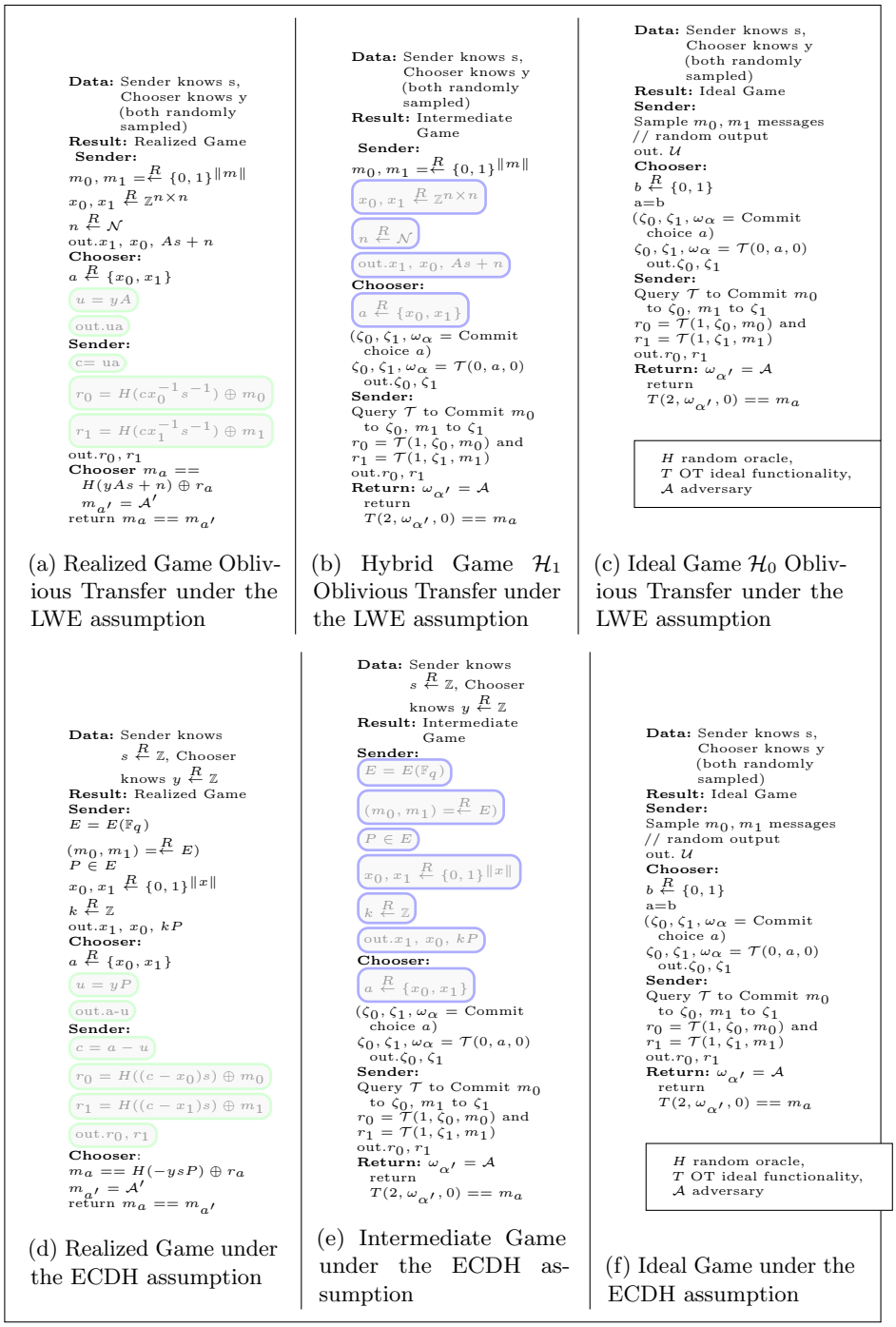
Diagram 11: Reconstructed Naor Pinkas Oblivious Transfer under the CDH hardness assumption

C.3 Constructing Oblivious Transfer under the ECDH hardness assumption

Reconstructing Game Transitions for computational ECDH hardness assumption

Hybrid Game $\mathcal{H}_0'$ ***to*** $\mathcal{H}_1'$ Similarly, we apply the $\mathcal{DH} \xrightarrow{-} \mathcal{LWE} \rightarrow \mathcal{C}\overrightarrow{\mathcal{DH}}$ transformation from proposition C1. The distribution $\{x_0, x_1\}$ remains uniform after applying $h : \mathbb{Z}_q^n \twoheadrightarrow E(F_q)$. Observe again on a second pass we need to remove the noise sampling n added, as it is not relevant anymore and becomes dead code.

Hybrid Game $\mathcal{H}_1'$ ***to*** $\mathcal{H}_2'$ The transformation over game transition $\mathcal{H}_1 \rightarrow \mathcal{H}_2$ follows in a similar manner.



(a) Realized Game Oblivious Transfer under the LWE assumption

(b) Hybrid Game $\mathcal{H}_1$ Oblivious Transfer under the LWE assumption

(c) Ideal Game $\mathcal{H}_0$ Oblivious Transfer under the LWE assumption

(d) Realized Game under the ECDH assumption

(e) Intermediate Game under the ECDH assumption

(f) Ideal Game under the ECDH assumption

Diagram 12: Games 12d to 12f show new security proof under ECDH. Games 12a to 12c depict the LWE-DH proof for the Sender. H denotes the random oracle.

D Chameleon Encryption in the LWE

D.1 Construction

The construction, similar to original, is as follows:

- $\mathrm{Gen}(1^\lambda, n) \mapsto (t, k)$:
  $(a_{i,j} \xleftarrow{R} \mathbb{Z}_p,\ i \in 1, \ldots, n,\ j \in \{0,1\})$
  1. $t = \begin{pmatrix} a_{1,0}, \ldots, a_{n,0} \\ a_{1,1}, \ldots, a_{n,1} \end{pmatrix},\ k = \left(A, \begin{pmatrix} Aa_{1,0} + n, \ldots, Aa_{n,0} + n \\ Aa_{1,1} + n, \ldots, Aa_{n,1} + n \end{pmatrix}\right)$
  2. out (t, k)
- $H(k, x; r) \mapsto h$:
  1. Parse k as above, $r \xleftarrow{R} \mathbb{Z}_p^n$
  2. $h = A'r + \sum\limits_{j \in \{1,\ldots,n\}} Aa_{j,x_j} + n$
  3. out h
- $H^{-1}(t, (x, r), x') \mapsto r'$:
  1. Parse t
  2. $r' = r + A'^{-1}A \sum\limits_{j \in \{1,\ldots,n\}} a_{j,x_j} - a_{j,x'_j} \mod p$
  3. out r'
- $\mathrm{Enc}(k, (h, i, b), m) \mapsto \mathrm{ct}$:
  1. Parse $k,\ \rho \xleftarrow{R} \mathbb{Z}_p^n$
  2. $c = \rho A + n,\ c' = \rho h$
  3. $\forall y \in \{0,1\},\ j \in \{1, \ldots, n\} \backslash \{i\} :\ c_{j,y} = \rho A a_{i.y} + n$
  4. $c_{i,0} = c_{i,1} = \perp$
  5. $e = m \oplus \mathrm{HardCore}^3(\rho A a_{i,b} + n)$
  6. out $ct = \left(e, c, c', \begin{pmatrix} c_{1,0}, \ldots, c_{n,0} \\ c_{1,1}, \ldots, c_{n,1} \end{pmatrix}\right)$
- $\mathrm{Dec}(k, (x, r), ct) \mapsto m$:
  1. Parse ct as above
  2. out $e \oplus \mathrm{HardCore}\left(c'\left(cA^{-1}A'r + \sum\limits_{j \in \{1,\ldots\} \backslash \{i\}} c_{j,x_j}\right)^{-1}\right)$

Diagram 13: Chameleon primitive under the LWE

where $n \in \mathbb{Z}^n$ is noise resampled per invocation, x_j the j-th bit of x. A^{-1} must be such that $A^{-1}(\text{noise})$ is a small quantity.

D.2 Uniformity

Similar to the original argument, for all arguments $k,\ x$, we have that $H(k, x; r) = A'r + \sum\limits_{j \in \{1,\ldots,n\}} Aa_{j,x_j} + n$ is statistically close to the uniform distribution by assumption – r is sampled uniformly.

D.3 Trapdoor Collision

Suppose $x \neq x', r, k, t$ and $r' = r + A'^{-1}A \sum_{j\in\{1,\ldots,n\}} a_{j,x_j} - a_{j,x'_j} \mod p$. We need to show that $H(k, x'; r') - H(k, x; r) ==$ noise:

$$H(k, x'; r') = A'r' + \sum_{j\in\{1,\ldots,n\}} Aa_{j,x'_j} + n \tag{90}$$

$$= A'r + A'A'^{-1}A \sum_{j\in\{1,\ldots,n\}} a_{j,x_j} - a_{j,x'_j} + \sum Aa_{j,x'_j} + n \tag{91}$$

$$= A'r + A\left(\sum_{j\in\{1,\ldots,n\}} ((a_{j,x_j} - a_{j,x'_j}) + a_{j,x'_j}) + \Delta n\right) \tag{92}$$

$$= H(k, x; r) + n' \tag{93}$$

Observe the original collision proof can now also derived if we apply the surjective homomorphism described in lemma 5. Similarly for the uniformity condition (applying lemma 2).

D.4 Correctness

Suppose $x \in \{0,1\}^n,\ r$, index $i \in \{1, \ldots, n\}$ and message $m \in \{0,1\}^n$. Generate (k, t), h and ct by invoking Gen, H and Enc respectively with the appropriate afforementioned arguments. It holds:

$$\left(c' - \left(cr + \sum_{j\in\{1,\ldots,n\}\setminus\{i\}} c_{j,x_j}\right)\right) = \rho h - \left(cA^{-1}A'r + \sum_{j\in\{1,\ldots\}\setminus\{i\}} c_{j,x_j}\right)$$

$$= \rho(A'r + \sum_{j\in\{1,\ldots,n\}} Aa_{j,x_j} + n) - \left(cA^{-1}A'r + \sum_{j\in\{1,\ldots,n\}\setminus\{i\}} c_{j,x_j}\right)$$

$$= \rho(A'r + n + \sum_{j\in\{1,\ldots,n\}} Aa_{j,x_j} + n) - \left((\rho A + n)A^{-1}A'r + \sum_{j\in\{1,\ldots,n\}\setminus\{i\}} c_{j,x_j}\right)$$

$$= Aa_{i,x_i} + \Delta n$$

Thus it holds that $\mathrm{Dec}(k, (x, r), \mathsf{ct}) = m$.

D.5 Security

Proof of security works the same as in [11]. Here, however we present a game-based proof (diagrams 14-17) and present how to derive a proof for the corresponding CDH primitive. Assume PPT adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$. We define the ideal game in diagram 14.

1. $(k,t) \xleftarrow{R} \text{Gen}(1^\lambda, n)$
2. $(x, r, i \in \{1,\dots,n\}, \text{st}) = \mathcal{A}_0$
3. $b \xleftarrow{R} \{0,1\}$
4. $\zeta = H(k, x; r)$
5. $\text{ct} = \text{Enc}(k, (\zeta, i, 1 - x_i), b)$
6. $b' = \mathcal{A}_1(k, \text{ct}, (x, r), \text{st})$
7. out $\begin{cases} 1, & b == b' \\ 0, & \text{otherwise} \end{cases}$

Diagram 14: Ideal $\text{IND}^{\text{CE}}_{\mathcal{A}}$ Game

Ideal to $\mathcal{H}_1$ ***Hybrid Game*** : We introduce the Gen algorithm to substitute its ideal equivalent. If $\mathcal{A}$ could distinguish between the two games, in particular between the old and the new k with non-negligible probabibility then it can break LWE. Thus the game transition is composed by applying $\mathcal{DH} \xleftarrow{-} \mathcal{LWE}$to each element of k tuple to get:

$$\begin{pmatrix} Aa_{1,0} + n, \dots, Aa_{n,0} + n \\ Aa_{1,1} + n, \dots, Aa_{n,1} + n \end{pmatrix} \tag{94}$$

$\mathcal{H}_1$ ***to*** $\mathcal{H}_2$ ***Hybrid Game*** : The inverse game transition is constructed directly by applying $\mathcal{DL} \xrightarrow{} \mathcal{WE}$. Hence, the two games are computationally indistinguishable by assertion.

$\mathcal{H}_3$ ***to*** $\mathcal{H}_2$ ***Hybrid Game*** : We work from game $\mathcal{H}_3$ to game $\mathcal{H}_2$ for convenience. We break the game transition into three substeps. First we apply $\mathcal{DL} \xrightarrow{} \mathcal{WE}$ to step (b) and (c) of Enc. Next step we apply the same transformation to step (d) ($\rho A a_{i,b} + n \simeq_c \rho \mathcal{U}_{i,b} + n \simeq_c \mathcal{U}$). As a final step we take two cases: if $i \neq i^*$ or $x \neq x_i$ then the two games are indistinguishable. Otherwise, the return distribution is indistinguishable from HardCore, and thus if $\mathcal{A}$ could distinguish the games in this event it could compute the hardcore bit.

For the sake of brevity we are going to only focus on the differences between games in diagrams 14, 15, 16,17.

D.6 Deriving the original CDH Chameleon Encryption primitive

We can't apply directly theorem 71, as there is no natural map between the two hardness assumptions. We can still however rederive all game transitions by applying lemma 3. In particular, proposition C1 guarantees we can substitute the application of the DH-LWE assumption with CDH (effectively via $\mathcal{CD} \xrightarrow{} \mathcal{H} \circ$

1. $(k,t) \xleftarrow{R} \mathrm{Gen}(1^\lambda, n)\{$
   (a) $t = \begin{pmatrix} a_{1,0}, \ldots, a_{n,0} \\ a_{1,1}, \ldots, a_{n,1} \end{pmatrix}$, $k = \left(A, \begin{pmatrix} Aa_{1,0}+n, \ldots, Aa_{n,0}+n \\ Aa_{1,1}+n, \ldots, Aa_{n,1}+n \end{pmatrix}\right)$
   (b) out (t,k)
   $\}$
2. $(x, r, i \in \{1,\ldots,n\}, \mathrm{st}) = \mathcal{A}_0$
3. $b \xleftarrow{R} \{0,1\}$
4. $\zeta = H(k, x; r)$
5. $\mathrm{ct} = \mathrm{Enc}(k, (\zeta, i, 1-x_i), b)$
6. $b' = \mathcal{A}_1(k, \mathrm{ct}, (x,r), \mathrm{st})$
7. out $\begin{cases} 1, & b == b' \\ 0, & \text{otherwise} \end{cases}$

Diagram 15: $\mathcal{H}_1$ $\mathrm{IND}^{\mathrm{CE}}_{\mathcal{A}}$ Game

$\vdots$

2. $(x, r, i \in \{1,\ldots,n\}, \mathrm{st}) = \mathcal{A}_0$
3. $b \xleftarrow{R} \{0,1\}$
4. $\zeta = H(k, x; r)\{$
   (a) Parse k as above, $r \xleftarrow{R} \mathbb{Z}_p^n$
   (b) $h = A'r + \sum_{j \in \{1,\ldots,n\}} Aa_{j,x_j} + n$
   (c) out h
   $\}$
5. $\mathrm{ct} = \mathrm{Enc}(k, (\zeta, i, 1-x_i), b)$
6. $b' = \mathcal{A}_1(k, \mathrm{ct}, (x,r), \mathrm{st})$
7. out $\begin{cases} 1, & b == b' \\ 0, & \text{otherwise} \end{cases}$

Diagram 16: $\mathcal{H}_2$ $\mathrm{IND}^{\mathrm{CE}}_{\mathcal{A}}$ Game

$\mathcal{DH} \overleftarrow{-} \mathcal{LWE}$) and subsequently apply lemma 3. Observe also that the new black-box HardCore construction will have a distribution with negligible distance to the original HardCore distribution. Hence $\mathcal{H}_3^{\mathrm{CDH}}$ and $\mathcal{H}_2^{\mathrm{CDH}}$ are indistinguishable.

The proof of correctness is a direct result of applying $\mathcal{C}\overrightarrow{\mathcal{DH}} \circ h \circ \mathcal{DH} \overleftarrow{-} \mathcal{LWE}$, which returns a indistinguishable distribution – with $h : \mathbb{Z}_q^n \twoheadrightarrow \mathbb{Z}_p$. Uniformity is implied by lemma 2 (or lemma 3).

$$\vdots$$

5. $\mathrm{ct} = \mathrm{Enc}(k, (\zeta, i, 1 - x_i), b)\{$
   (a) Parse k, $\rho \xleftarrow{R} \mathbb{Z}_p^n$
   (b) $c = \rho A + n$, $c' = \rho\zeta$
   (c) $\forall y \in \{0,1\}$, $j \in \{1, \ldots, n\} \backslash \{i\} :$ $c_{j,y} = \rho A a_{i.y} + n$
   (d) $c_{i,0} = c_{i,1} = \perp$
   (e) $e = m \oplus \mathrm{HardCore}(\rho A a_{i,b} + n)$
   (f) out $ct = \left(e, c, c', \begin{pmatrix} c_{1,0}, \ldots, c_{n,0} \\ c_{1,1}, \ldots, c_{n,1} \end{pmatrix}\right)$
   $\}$
6. $b' = \mathcal{A}_1(k, \mathrm{ct}, (x, r), \mathrm{st})$
7. out $\begin{cases} 1, & b == b' \\ 0, & \text{otherwise} \end{cases}$

Diagram 17: $\mathcal{H}_3$ $\mathrm{IND}_{\mathcal{A}}^{\mathrm{CE}}$ Game

E Garbled Circuit Constructions

In [11] Döttling and Garg provide a selectively secure IBE scheme. They bypass the algebraic restriction of [63] compressing exponential number of keys via construcing a decryption tree based on garbled circuits [64]. The construction utilizes the chameleon encryption primitive of the previous section.

At this point, note we have taken all of the steps to introduce an IBE protocol in LWE similar to the work of Döttling and Garg [11]. First observe that the proof of correctness and security in [11] of the Garbled Circuit evaluation is abstract and independent of the CDH construction. Thus the main construction and proofs of security and soundness were presented in the previous section. To derive the proof of security in CDH, we need only apply 3 for each hybrid game between different uniform samplings.

(This showcases the power of the compression method despite its inefficiency. It appears that similar constructions using Garbled Circuits can bypass similar algebraic impossibilities.)

We now introduce basic notions for completeness, before stating the main lemmas.

An IBE protocol is a tuple of

- Setup (λ)
- $\mathrm{Extract}(\mathrm{PP}, \mathrm{MK}, \mathrm{id})$
- $\mathrm{Encrypt}(\mathrm{PP}, \mathrm{id}, m)$
- $\mathrm{Decrypt}(\mathrm{PP}, \mathrm{SK}, c)$

for security parameter λ, MK master key, SKsecret key, PP public parameters, id an identity and $m \in \{0,1\}$ a message, c ciphertext. It satisfies the following completeness and security properties.

Completeness : For any security parameter λ and any $\mathrm{id} \in \{0,1\}^n$, message m and for a $\mathrm{SK}_{\mathrm{id}} = \mathrm{Extract}(\mathrm{PP}, \mathrm{MK}, \mathrm{id})$:

$$\mathrm{Decrypt}(\mathrm{PP}, \mathrm{SK}_{\mathrm{id}}, \mathrm{Encrypt}(\mathrm{PP}, \mathrm{id}, m)) = m$$

Security : For any adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ it holds that

$$\mathrm{Adv}_{\mathcal{A}}\left(\mathrm{IND}_{\mathcal{A}}^{\mathrm{IBE}}, [\mathrm{out}.\, b \xleftarrow{R} \{0,1\}]\right) \leq \mathrm{Negl}.(\lambda)$$

as shown in diagram 18.

For each adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ query we have that $\mathrm{id} \neq \mathrm{id}^*$.

1. $(\mathrm{PP}, \mathrm{MK}) = \mathrm{Setup}(1^\lambda)$
2. $(\mathrm{id}^*, m_0, m_1, \mathrm{st}) = \mathcal{A}_0(\mathrm{PP})$, $|m_0| == |m_1|$.
3. $b \xleftarrow{R} \{0,1\}$
4. $\mathrm{ct} = \mathrm{Encrypt}(\mathrm{PP}, \mathrm{id}^*, m_b)$
5. $b' = \mathcal{A}_1(\mathrm{PP}, \mathrm{ct}, st)$
6. out $\begin{cases} 1, & b == b' \\ 0, & \text{otherwise} \end{cases}$

Diagram 18: $\mathrm{IND}_{\mathcal{A}}^{\mathrm{IBE}}$ Game

E.1 Basic Definitions

Definition 25. *A garble circuit [64] is a tuple of algorithms:*

- *Garble:* $\lambda \times C \to \tilde{C} \times e_c$ *with* $e_c = \{X_{i,0}, X_{i,1}\}_{i \in \{1,\ldots,n\}}$
- *Project Encoding:* $x \in \{0,1\}^n \times e_c \mapsto \tilde{x} = \{X_{i,x_i}\}_{i \in \{1,\ldots,n\}}$
- *Evaluate:* $\tilde{x} \times \tilde{C} \to y$

satisfying the following security and correctness properties:

Security: There is a PPT Simulator ***Sim*** *that for any circuit and input* C, x *it holds:*

$$(\tilde{C}, \tilde{x}) \stackrel{c}{\simeq} \mathrm{Sim}(C, C(x)) \tag{95}$$

with $\stackrel{c}{\simeq}$ *denoting computational equivalence.*

Correctness: For any circuit C and input $x \in \{0,1\}^n$ it holds that

$$\Pr[C(x) = \text{Evaluate}(\tilde{C}, (\tilde{x}))] = 1 \tag{96}$$

Note $\tilde{C}, E = \text{Garble}(\lambda, C)$ the garbled circuit and $\tilde{x} \in E$ the encrypted input.

Proposition E1. *The IBE construction of [11] utilizing the chameleon encryption in 13 is selectively secure.*