Electronic Colloquium on Computational Complexity, Report No. 53 (2007)

Efficient Non-interactive Proof Systems for Bilinear Groups*

Jens Groth† Amit Sahai‡

UCLA, Computer Science Department
4732 Boelter Hall
Los Angeles, CA 90095-1596, USA
{jg,sahai}@cs.ucla.edu

Abstract

Non-interactive zero-knowledge proofs and non-interactive witness-indistinguishable proofs have played a significant role in the theory of cryptography. However, lack of efficiency has prevented them from being used in practice. One of the roots of this inefficiency is that non-interactive zero-knowledge proofs have been constructed for general NP-complete languages such as Circuit Satisfiability, causing an expensive blowup in the size of the statement when reducing it to a circuit. The contribution of this paper is a general methodology for constructing very simple and efficient non-interactive zero-knowledge proofs and non-interactive witness-indistinguishable proofs that work directly for groups with a bilinear map, without needing a reduction to Circuit Satisfiability.

Groups with bilinear maps have enjoyed tremendous success in the field of cryptography in recent years and have been used to construct a plethora of protocols. This paper provides non-interactive witness-indistinguishable proofs and non-interactive zero-knowledge proofs that can be used in connection with these protocols. Our goal is to spread the use of non-interactive cryptographic proofs from mainly theoretical purposes to the large class of practical cryptographic protocols based on bilinear groups.

Keywords: Non-interactive witness-indistinguishability, non-interactive zero-knowledge, common reference string, bilinear groups.

*Work presented and part of work done while participating in Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security, Institute of Pure and Applied Mathematics, UCLA, 2006.

†Supported by NSF ITR/Cybertrust grant No. 0456717.

‡This research was supported in part from grants from the NSF ITR and Cybertrust programs (including grants 0627781, 0456717, and 0205594), a subgrant from SRI as part of the Army Cyber-TA program, an equipment grant from Intel, and an Alfred P. Sloan Foundation Research Fellowship.

ISSN 1433-8092

1 Introduction

Non-interactive zero-knowledge proofs and non-interactive witness-indistinguishable proofs have played a significant role in the theory of cryptography. However, lack of efficiency has prevented them from being used in practice. Our goal is to construct efficient and practical non-interactive zero-knowledge (NIZK) proofs and non-interactive witness-indistinguishable (NIWI) proofs.

Blum, Feldman and Micali [BFM88] introduced NIZK proofs. Their paper and subsequent work, e.g. [FLS99, Dam92, KP98, DDP02], demonstrates that NIZK proofs exist for all of NP. Unfortunately, these NIZK proofs are all very inefficient. While leading to interesting theoretical results, such as the construction of public-key encryption secure against chosen ciphertext attack by Dolev, Dwork and Naor [DDN00], they have therefore not had any impact in practice.

Since we want to construct NIZK proofs that can be used in practice, it is worthwhile to identify the roots of the inefficiency in the above mentioned NIZK proofs. One drawback is that they were designed with a general NP-complete language in mind, e.g. Circuit Satisfiability. In practice, we want to prove statements such as "the ciphertext c encrypts a signature on the message m" or "the three commitments c_a, c_b, c_c contain messages a, b, c so $c = ab$". An NP-reduction of even very simple statements like these gives us big circuits containing thousands of gates and the corresponding NIZK proofs then become very large.

While we want to avoid an expensive NP-reduction, it is still desirable to have a general way to express statements that arise in practice instead of having to construct non-interactive proofs on an ad hoc basis. A useful observation in this context is that many public-key cryptography protocols are based on finite abelian groups. If we can capture statements that express relations between group elements, then we can express statements that come up in practice such as "the commitments c_a, c_b, c_c contain messages so $c = ab$" or "the plaintext of c is a signature on m", as long as those commitment, encryption, and signature schemes work over the same finite group. In the paper, we will therefore construct NIWI and NIZK proofs for *group-dependent* languages.

The next issue to address is where to find suitable group dependent languages. We will look at statements related to groups with a bilinear map, which have become widely used in the design of cryptographic protocols. Not only have bilinear groups been used to give new constructions of such cryptographic staples as public-key encryption, digital signatures, and key agreement (see [DBS04] and the references therein), but bilinear groups have enabled the first constructions achieving goals that had never been attained before. The most notable of these is the Identity-Based Encryption scheme of Boneh and Franklin [BF03] (see also [Wat05]), and there are many others, such as Attribute-Based Encryption [SW05, GPSW06], Searchable Public-Key Encryption [BCOP04, BSW06, BW06], and One-time Double-Homomorphic Encryption [BGN05]. For an incomplete list of papers (currently over 200) on the application of bilinear groups in cryptography, see [Bar06].

1.1 Our Contribution

In this work, we develop a general set of highly efficient techniques for proving statements involving bilinear groups. The generality of our work extends in two directions. First, we formulate our constructions in terms of modules over commutative rings with an associated bilinear map. This framework captures all known bilinear groups with cryptographic significance – for both supersingular and ordinary elliptic curves, for groups of both prime and composite order. Second, we consider all mathematical operations that could take place in the context of a bilinear group – exponentiation, addition or multiplication of exponents, multiplication of group elements and use of the bilinear map. We also allow both group elements and exponents to be "unknowns" in the statements to be proven.

With our level of generality, for example it would be easy to write down a short statement, using the operations above, that encodes "c is an encryption of the value committed to in d under the product of the

two keys committed to in a and b" where the encryptions and commitments being referred to are existing cryptographic constructions based on bilinear groups. Logical operations like AND and OR are also easy to encode into our framework using standard techniques in arithmetization.

The proof systems we build are *non-interactive*. This allows them to be used in contexts where interaction is undesirable or impossible. We first build highly efficient witness-indistinguishable proof systems, which are of independent interest. We then show how to transform these into zero-knowledge proof systems. We also provide a detailed examination of the efficiency of our constructions in various settings (depending on what type of bilinear group is used).

The security of constructions arising from our framework can be based on *any* of a variety of computational assumptions about bilinear groups (3 of which we discuss in detail here). Thus, our techniques do not rely on any one assumption in particular.

Informal statement of our results. We consider equations over variables from G_1, G_2 and $\mathbb{Z}_{\mathbf{n}}$ as described in Figure 1. We construct efficient witness-indistinguishable proofs for the simultaneous satisfiability of a set of such equations. The witness-indistinguishable proofs have perfect completeness and there are two computationally indistinguishable types of common reference strings giving respectively perfect soundness and perfect witness indistinguishability. We refer to Section 2 for precise definitions.

We also consider the question of non-interactive zero-knowledge. We say a set of equations is *tractable* if it is possible to compute a satisfiability witness in the easier setting where we allow the exponent variables $\phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L$ to take different values in each equation. We offer a technique to transform a set of equations into an equivalent tractable set of equations. Tractable equations have efficient non-interactive zero-knowledge proofs with perfect completeness and two types of computationally indistinguishable common reference strings giving respectively perfect soundness and perfect zero-knowledge simulation.

Instantiation 1: Subgroup decision. Throughout the paper, we will give a general description of our techniques. We will also offer three instantiations that illustrate the use of our techniques. The first instantiation is based on the composite order groups introduced by Boneh, Goh and Nissim [BGN05]. Let G, G_T be cyclic groups of order $\mathbf{n} = \mathbf{pq}$, where $\mathbf{p}, \mathbf{q}$ are primes. Let g be a generator of G. Let $e : G \times G \to G_T$ be a non-degenerate bilinear map, i.e., $e(g, g)$ generates G_T and for all a, b we have $e(g^a, g^b) = e(g, g)^{ab}$. [BGN05] gives an example of a way to set up such groups such that all operations are efficiently computable and membership of G, G_T can be decided efficiently.

We can write $G = G_{\mathbf{p}} \times G_{\mathbf{q}}$, where $G_{\mathbf{p}}, G_{\mathbf{q}}$ are the subgroups of order $\mathbf{p}$ and $\mathbf{q}$ respectively. The subgroup decision problem is to distinguish a random element from G from a random element from $G_{\mathbf{q}}$. In this paper, we will demonstrate that assuming the hardness of the subgroup decision problem there exists a witness-indistinguishable proof for satisfiability of a set of equations from Figure 1 in the subgroup $G_{\mathbf{p}}$ and the order $\mathbf{p}$ subgroup of G_T.

Instantiation 2: XDH and SXDH. Let G_1, G_2, G_T be groups of prime order $\mathbf{p}$ with a non-degenerate bilinear map $e : G_1 \times G_2 \to G_T$. The external Diffie-Hellman (XDH) assumption is that the decisional Diffie-Hellman (DDH) problem is hard in one of the groups G_1 or G_2 [Sco02, BBS04, BGdMM05, GR04, Ver04]. The Symmetric XDH assumption is that the DDH problem is hard in both G_1 and G_2. We will construct a witness-indistinguishable proof for these groups under the SXDH assumption. We will also observe that given only the XDH assumption, we can still give NIWI proofs for some interesting special cases.

Instantiation 3: DLIN. Let G, G_T be groups of prime order $\mathbf{p}$ with a non-degenerate bilinear map $e : G \times G \to G_T$. The decisional linear assumption (DLIN) introduced by Boneh, Boyen and Shacham [BBS04] states that given three random generators f, h, g and f^r, h^s, g^t, it is hard to distinguish the case $t = r + s$

Variables: $x_1, \ldots, x_M \in G_1$, $y_1, \ldots, y_N \in G_2$, $\phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L \in \mathbb{Z}_{\mathbf{n}}$.

Pairing product equation:

$$\prod_{q=1}^{Q} e(a_q \prod_{m=1}^{M} x_m^{\alpha_{qm}}, b_q \prod_{n=1}^{N} y_n^{\beta_{qn}}) = T \ ,$$

for constants $a_q \in G_1, b_q \in G_2, T \in G_T, \alpha_{qm}, \beta_{qn} \in \mathbb{Z}_{\mathbf{n}}$.

Multi-exponentiation in G_1:

$$\prod_{\ell=1}^{L} a_\ell^{\theta_\ell} \cdot \prod_{m=1}^{M} x_m^{\sum_{\ell=1}^{L} \alpha_{m\ell}\theta_\ell + \beta_m} \ = \ t_1,$$

for constants $a_\ell, t_1 \in G_1$ and $\alpha_{m\ell}, \beta_m \in \mathbb{Z}_{\mathbf{n}}$.

Multi-exponentiation in G_2:

$$\prod_{k=1}^{K} b_k^{\phi_k} \cdot \prod_{n=1}^{N} y_n^{\sum_{k=1}^{K} \alpha_{nk}\phi_k + \beta_n} \ = \ t_2,$$

for constants $b_k, t_2 \in G_2$ and $\alpha_{nk}, \beta_n \in \mathbb{Z}_{\mathbf{n}}$.

General arithmetic gate:

$$\sum_{k=1}^{K} \alpha_k \phi_k \ + \ \sum_{\ell=1}^{L} \beta_\ell \theta_\ell \ + \ \sum_{k=1}^{K} \sum_{\ell=1}^{L} \gamma_{k\ell} \phi_k \theta_\ell \ = \ \tau,$$

for constants $\alpha_k, \beta_\ell, \gamma_{k\ell}, \tau \in \mathbb{Z}_{\mathbf{n}}$.

Figure 1: Equations over groups with bilinear map.

from t random. They offer an example of such a group based on elliptic curves, where the DLIN problem is assumed hard. Assuming the hardness of the DLIN problem, we will suggest a witness-indistinguishable proof for satisfiability of a set of equations from Figure 1.

The instantiations illustrate the variety of ways bilinear groups can be constructed. We can choose prime order groups or composite order groups, we can have $G_1 = G_2$ and $G_1 \neq G_2$, and we can make various cryptographic assumptions. All three security assumptions have been used in the cryptographic literature to build interesting protocols.

For all three instantiations, the techniques presented here yield very efficient witness-indistinguishable proofs. In particular, the cost in proof size of each extra equation is constant and independent of the number of variables in the equation. The size of the proofs, can be computed by adding the cost, measured in group elements from G_1 or G_2, of each variable and each equation listed in Figure 2. We refer to Section 9 for more detailed tables.

1.2 Related Work

As we mentioned before, early work on NIZK proofs demonstrated that all NP-languages have non-interactive proofs, however, did not yield efficient proofs. One cause for these proofs being inefficient in practice was the need for an expensive NP-reduction to e.g. Circuit Satisfiability. Another cause of inefficiency was the reliance on the so-called hidden bits model, which even for small circuits is inefficient.

	Subgroup decision	SXDH	DLIN
Variable in G_1 or G_2	1	2	3
Variable in $\mathbb{Z}_{\mathbf{n}}$ or $\mathbb{Z}_{\mathbf{p}}$	1	2	3
Paring product equation	1	8	9
Multi-exponentiation in G_1 or G_2	1	6	9
General arithmetic gate	1	4	6

Figure 2: Number of group elements each variable or equation costs.

Groth, Ostrovsky, and Sahai [GOS06b, GOS06a] investigated NIZK proofs for Circuit Satisfiability using bilinear groups. This addressed the second cause of inefficiency since their techniques give efficient proofs for Circuit Satisfiability, but to use their proofs one must still make an NP-reduction to Circuit Satisfiability thus limiting the applications. We stress that while [GOS06b, GOS06a] used bilinear groups, their application was to build proof systems for circuit satisfiability. Here, we devise entirely new techniques to deal with general statements *about* bilinear groups, without having to reduce to an NP-complete language.

Addressing the issue of avoiding an expensive NP-reduction we have works by Boyen and Waters [BW06, BW07] that suggest efficient NIWI proofs for statements related to group signatures. These proofs are based on bilinear groups of composite order and rely on the subgroup decision assumption.

Groth [Gro06] was the first to suggest a general group-dependent language and NIZK proofs for statements in this language. He investigated a restricted kind of pairing product equation in which only group elements can be variables. He also looked only at the special case of prime order groups G, G_T with a bilinear map $e : G \times G \rightarrow G_T$ and, based on the decisional linear assumption [BBS04], constructed NIZK proofs for such restricted pairing product equations. However, even for very small statements, the very different and much more complicated techniques of Groth yield proofs consisting of thousands of group elements (whereas ours would be in the tens)[1]. Our techniques are much easier to understand, significantly more general, and vastly more efficient.

We summarize our comparison with other works on NIZK proofs in Figure 3.

	Inefficient	Efficient
Circuit Satisfiability	E.g. [KP98]	[GOS06b, GOS06a]
Pairing Product Equations	[Gro06] (restricted case)	This work

Figure 3: Classification of NIZK proofs according to usefulness.

We note that there have been many earlier works (starting with [GMR89]) dealing with efficient *interactive* zero-knowledge protocols for a number of algebraic relations. Here, we focus on *non-interactive* proofs. We also note that even for interactive zero-knowledge proofs, no set of techniques was known for dealing with general algebraic assertions arising in bilinear groups, as we do here.

1.3 New Techniques

[GOS06b, GOS06a, Gro06] start by constructing non-interactive proofs for simple statements and then combine many of them to get more powerful proofs. The main building block in [GOS06b], for instance, is a proof that a given commitment contains either 0 or 1, which has little expressive power on its own. Our

[1] Furthermore, even when limited to the restricted types of statements considered by [Gro06], there are examples of families of statements for which there is an *arbitrary polynomial gap* between the efficiency of the proof systems of [Gro06] and ours. Thus, our construction not only dominates that of [Gro06] in terms of typical use, but also in asymptotic terms.

approach is the opposite: we directly construct proofs for very expressive languages; as such, our techniques are very different from previous work.

The way we construct our efficient yet powerful NIWI proofs is by viewing the groups G_1, G_2, G_T as submodules of appropriately chosen modules M_1, M_2, M_T. Furthermore, from the bilinear map $e : G_1 \times G_2 \to G_T$, we can construct a bilinear map $E : M_1 \times M_2 \to M_T$. We introduce a number of new techniques for building NIWI proofs in this setting. The primary advantage of the modular setting is that it permits characterizing witness-indistinguishability in a very simple way. Moreover, witness-indistinguishability relies on high-level properties of modules over a commutative ring so our approach becomes very general and covers a wide range of different types of bilinear groups.

1.4 Applications

There are many applications of our NIWI proofs and NIZK proofs. Subsequent to this work, Chandran, Groth and Sahai [CGS07] construct ring-signatures of sublinear size using the NIWI proofs in the first instantiation, which is based on the subgroup decision problem. Groth and Lu [GL07] use the NIWI and NIZK proofs from instantiations 1 and 3 to construct non-interactive proofs for the correctness of a shuffle. We note that the proofs of Boyen and Waters [BW06, BW07] used to construct group signatures can be seen as examples of the NIWI proofs in instantiation 1. Also, by attaching NIZK proofs to semantically secure public-key encryption in any instantiation we get an efficient non-interactive verifiable cryptosystem. Boneh [Bon06] has suggested using this for optimistic fair exchange [Mic03], where two parties use a trusted but lazy third party to guarantee fairness.

2 Non-interactive Witness-Indistinguishable Proofs

Let R be an efficiently computable ternary relation. For triplets $(\sigma, x, w) \in R$ we call x the statement and w the witness. Given some σ we let L be the language consisting of statements in R. For a relation that ignores σ this is of course the standard definition of an NP-language.

A non-interactive proof system for a relation R consists of a three probabilistic polynomial time algorithms: a CRS generation algorithm K, a prover P and a verifier V. The CRS generation algorithm produces a common reference string σ. The prover takes as input (σ, x, w) and produces a proof π. The verifier takes as input (σ, x, π) and outputs 1 if the proof is acceptable and 0 if rejecting the proof. We call (K, P, V) a non-interactive proof system for R if it has the completeness and soundness properties described below.

PERFECT COMPLETENESS. For all adversaries $\mathcal{A}$ we have

$$\Pr\left[\sigma \leftarrow K(1^k); (x, w) \leftarrow \mathcal{A}(\sigma); \pi \leftarrow P(\sigma, x, w) : V(\sigma, x, \pi) = 1 \text{ if } (\sigma, x, w) \in R\right] = 1.$$

PERFECT SOUNDNESS. For all adversaries $\mathcal{A}$ we have

$$\Pr\left[\sigma \leftarrow K(1^k); (x, \pi) \leftarrow \mathcal{A}(\sigma) : V(\sigma, x, \pi) = 0 \text{ if } x \notin L\right] = 1.$$

COMPOSABLE WITNESS INDISTINGUISHABILITY. In this paper, we will use a strong definition of witness indistinguishability. We introduce a reference string simulator S that generates a simulated CRS. We require that the adversary cannot distinguish a real CRS from a simulated CRS. Then we require that on a simulated CRS, it is *perfectly* indistinguishable, which witness the prover used.

In other words, for all non-uniform polynomial time adversaries $\mathcal{A}$ we have

$$\Pr[\sigma \leftarrow K(1^k) : \mathcal{A}(\sigma) = 1] \approx \Pr[\sigma \leftarrow S(1^k) : \mathcal{A}(\sigma) = 1]$$

and

$$\begin{aligned} & \Pr\Big[\sigma \leftarrow S(1^k); (x, w_0, w_1) \leftarrow \mathcal{A}(\sigma); \pi \leftarrow P(\sigma, x, w_0) : \mathcal{A}(\pi) = 1\Big] \\ = \; & \Pr\Big[\sigma \leftarrow S(1^k); (x, w_0, w_1) \leftarrow \mathcal{A}(\sigma); \pi \leftarrow P(\sigma, x, w_1) : \mathcal{A}(\pi) = 1\Big], \end{aligned}$$

where we require $(\sigma, x, w_0), (\sigma, x, w_1) \in R$.

COMPOSABLE ZERO-KNOWLEDGE. Composable zero-knowledge [Gro06] is a strengthening of the usual notion of non-interactive zero-knowledge. First, we require that an adversary cannot distinguish a real CRS from a simulated CRS. Second, we require that the adversary, *even when it gets access to the secret simulation key* τ, cannot distinguish real proofs on a simulated CRS from simulated proofs.

In other words, there exists a polynomial time simulator (S_1, S_2) so for all non-uniform polynomial time adversaries $\mathcal{A}$ we have

$$\Pr\Big[\sigma \leftarrow K(1^k) : \mathcal{A}(\sigma) = 1\Big] \approx \Pr\Big[(\sigma, \tau) \leftarrow S_1(1^k) : \mathcal{A}(\sigma) = 1\Big],$$

and

$$\begin{aligned} & \Pr\Big[(\sigma, \tau) \leftarrow S_1(1^k); (x, w) \leftarrow \mathcal{A}(\sigma, \tau); \pi \leftarrow P(\sigma, x, w) : \mathcal{A}(\pi) = 1 \text{ and } (x, w) \in R\Big] \\ = \; & \Pr\Big[(\sigma, \tau) \leftarrow S_1(1^k); (x, w) \leftarrow \mathcal{A}(\sigma, \tau); \pi \leftarrow S_2(\sigma, \tau, x) : \mathcal{A}(\pi) = 1 \text{ and } (x, w) \in R\Big]. \end{aligned}$$

3 Commitment from Modules

Let $(R, +, \cdot, 0, 1)$ be a commutative ring. Recall, that an R-module is an abelian group $(M, \cdot, 1)$ such that for all $r, s \in R$ and $u, v \in M$ we have[2]

$$u^{r+s} = u^r u^s \qquad \text{and} \qquad (uv)^r = u^r v^r.$$

Let $u_1, \ldots, u_I$ be elements in an R-module M. Consider an element $x \in M$. We may commit to x by choosing $r_1, \ldots, r_I \leftarrow R$ at random and letting the commitment be

$$c := x \prod_{i=1}^{I} u_i^{r_i}.$$

Define U to be the submodule generated by $u_1, \ldots, u_I$. In case $x \in U$, the message x is perfectly hidden. On the other hand, c uniquely determines x in the factor group M/U, so if $u_1, \ldots, u_I$ do not generate M, then c contains non-trivial information about x.

Peeking a little ahead, we will be interested in modules, where it is hard to tell whether $M = U$. The common reference string for our NIWI proofs will contain a set of u_i's. If they generate M, we will get perfect witness indistinguishability. On the other hand, if they do not generate M, we will get perfect soundness.

Instead of committing to messages from M, we may be interested in committing to a ring element $\phi \in R$. Consider therefore a setup, where have $u \in M$ and $u_1, \ldots, u_I$. We can commit to ϕ by selecting $r_1, \ldots, r_I$ at random and computing the commitment

$$c := u^{\phi} \prod_{i=1}^{I} u_i^{r_i}.$$

[2]Note that our modules will correspond to the groups underlying our cryptographic constructions. In order to maintain cryptographic tradition, we therefore write modules with multiplicative notation. This breaks mathematics tradition in which modules are written with additive notation. Such differences in notation are common in the cryptographic literature.

In case, $u \in U$ this perfectly hides the message. On the other hand, since $c \in M/U$ determines a unique value $u^\phi \in M/U$, the commitment contains non-trivial information about ϕ if $u \notin U$.

As we shall see below, our treatment of commitments using the language of modules generalizes several previous works dealing with commitments over bilinear groups, including [BGN05, GOS06b, GOS06a, Gro06, Wat06].

Instantiation 1: Subgroup decision. Based on the subgroup decision assumption, we can set up a commitment scheme as follows. We have an element $h \in G$ and commit to $x \in G$ by picking $r \leftarrow \mathbb{Z}_{\mathbf{n}}$ at random and computing the commitment $c := xh^r$. In case, h has order $\mathbf{n}$ this commitment is perfectly hiding. On the other hand, if h has order $\mathbf{q}$, then $c \in G/G_{\mathbf{q}}$ determines $x \in G_{\mathbf{p}}$ uniquely. Actually, given the factorization of $\mathbf{n}$ we can also decrypt the commitment as $x = c^{\mathbf{q}(\mathbf{q}^{-1} \bmod \mathbf{p})} \in G_{\mathbf{p}}$.

If we want to commit to ring elements, we let g be a generator of G. A commitment $c = g^\phi h^r$ is perfectly hiding in case h has order $\mathbf{n}$. In case h has order $\mathbf{q}$, the commitment uniquely determines $\phi \bmod \mathbf{p}$. The latter setup was used in [BGN05] to construct a cryptosystem that is both additively homomorphic and also has a one-time multiplication map.

Instantiation 2: XDH and SXDH. Consider a cyclic group G of prime order $\mathbf{p}$, where the DDH problem is hard. By entry-wise multiplication we get an abelian group G^2, which is a module over $\mathbb{Z}_{\mathbf{p}}$. Let $(g,h),(u,v)$ be two elements in G^2. We can commit to $(1,x) \in G^2$ as $c := (g,h)^r(u,v)^t(1,x) = (g^r u^t, h^r v^r x)$. If there exists $s \in \mathbb{Z}_{\mathbf{p}}$ so $(u,v) = (g,h)^s$, then the commitment corresponds to ElGamal encryption of x, i.e., $c = (g^{r+st}, h^{r+st}x)$. On the other hand, if (g,h) and (u,v) are linearly independent, then c is a perfectly hiding commitment to x. Distinguishing between (g,h) and (u,v) being linearly independent or not corresponds to the DDH problem.

To commit to a ring element, we use the following approach. We have a setup with elements (g,h) and (u,v). Under the DDH assumption, we cannot tell whether these elements are linearly independent or not. We commit to $\phi \in \mathbb{Z}_{\mathbf{p}}$, by choosing r at random and setting $c := (g,h)^\phi(u,v)^r$. In case, $(g,h),(u,v)$ are linearly independent this determines $\phi \in \mathbb{Z}_{\mathbf{p}}$ uniquely, but if $(g,h) = (u,v)^s$ for some $s \in \mathbb{Z}_{\mathbf{p}}$, then we have a perfectly hiding Pedersen commitment to ϕ.

Instantiation 3: DLIN. Let f,h,g be three random generators of G so $f = g^\alpha, h = g^\beta$. The DLIN assumption states that it is hard to tell whether three elements $(u,v,w) = (f^{r_u}, h^{s_v}, g^{t_w})$ have the property that $t_w = r_u + s_v$. We will look at the $\mathbb{Z}_{\mathbf{p}}$-module G^3 formed by entry-wise multiplication. Consider three elements $(f,1,g),(1,h,g),(u,v,w)$ in G^3. To commit to a message (x_1,x_2,x_3) we compute $c := (x_1,x_2,x_3)(f,1,g)^r(1,h,g)^s(u,v,w)^t$ for random $r,s,t \in \mathbb{Z}_{\mathbf{p}}$. In case, $(f,1,g),(1,g,h),(u,v,w)$ are linearly independent they generate all of G^3 and thus we have a perfectly hiding commitment. On the other hand, in case $(u,v,w) = (f^{r_u}, h^{s_v}, g^{r_u+s_v})$ for some $r_u, s_v \in \mathbb{Z}_{\mathbf{p}}$, we have that $c_1^{-1/\alpha} c_2^{-1/\beta} c_3 = x_1^{-1/\alpha} x_2^{-1/\beta} x_3$ is uniquely determined. In particular, if we commit to $(1,1,x)$, then we can with knowledge of α,β extract x from the commitment. This commitment scheme coincides with the scheme of [Wat06]. We note that the different, and less efficient, commitment scheme of [Gro06] can be similarly described in our language of modules, as well.

To commit to a message $\phi \in \mathbb{Z}_{\mathbf{p}}$ we also consider a setup with three elements $(f,1,g),(1,h,g),(u,v,w)$. We commit to ϕ by choosing r,s at random and computing $c := (f,1,g)^r(1,h,g)^s(u,v,w)^\phi$. In case (u,v,w) can be written as $(f^{r_u}, h^{s_v}, g^{r_u+s_v})$ this is a perfectly hiding commitment scheme. But if $(f,1,g),(1,h,g),(u,v,w)$ are linearly independent, the commitment scheme determines $\phi \in \mathbb{Z}_{\mathbf{p}}$ uniquely. This coincides with the scheme of [GOS06a].

4 Setup

Let M_1, M_2, M_T be R-modules. Let furthermore, $E : M_1 \times M_2 \to M_T$ be a bilinear map, i.e., for all $r, s \in R$ and $u, u' \in M_1, v, v' \in M_2$ we have

$$E(u^r u', v) = E(u, v)^r E(u', v) \qquad \text{and} \qquad E(u, v^s v') = E(u, v)^s E(u, v').$$

In the paper, we will always assume a setup with R-modules M_1, M_2, M_T and bilinear map $E : M_1 \times M_2 \to M_T$. Let $u_1, \ldots, u_I$ be elements in M_1 and $v_1, \ldots, v_J$ be elements in M_2. Let U be the submodule of M_1 generated by $u_1, \ldots, u_I$ and V be the submodule of M_2 generated by $v_1, \ldots, v_J$.

There are IJ not necessarily distinct elements $E(u_i, v_j)$ in M_T. They give rise to an R-linear map

$$\mu : R^{IJ} \to M_T \qquad (\rho_{11}, \ldots, \rho_{IJ}) \mapsto \prod_{i=1}^{I} \prod_{j=1}^{J} E(u_i, v_j)^{\rho_{ij}}.$$

Trivially, $(0, \ldots, 0)$ always belongs to the kernel of E, however, there may or may not be more vectors in the kernel. Let $\eta_1, \ldots, \eta_H \in R^{IJ}$ be H vectors in R^{IJ} that generate the kernel of μ. In other words, given any vector $\rho = (\rho_{11}, \ldots, \rho_{IJ})$ so

$$\prod_{i=1}^{I} \prod_{j=1}^{J} E(u_i, v_j)^{\rho_{ij}} = 1,$$

there exists $t_1, \ldots, t_H \in R$ so it can be written as

$$\rho = \sum_{h=1}^{H} t_h \eta_h \qquad \text{that is} \qquad (\rho_{11}, \ldots, \rho_{IJ}) = (\sum_{h=1}^{H} t_h \eta_{h11}, \ldots, \sum_{h=1}^{H} t_h \eta_{hIJ}).$$

Looking ahead, the CRS for the NIWI proofs we are about to suggest will contain $u_1, \ldots, u_I \in M_1$ and $v_1, \ldots, v_J \in M_2$, as well as $\eta_1, \ldots, \eta_H$. Depending on how we generate the CRS we will get either perfect soundness or perfect witness indistinguishability. In the perfect witness indistinguishability case, we will require that $\eta_1, \ldots, \eta_H$ generate the kernel of the map μ. For perfect soundness, we do not make such a requirement, however, notice that common reference string for perfect soundness and simulated common reference strings for perfect witness indistinguishability must be computationally indistinguishable, so in the perfect soundness case we also have $\mu(\eta_h) = 1$ for all $\eta_1, \ldots, \eta_H$.

The symmetric setting. In the next section, we will offer NIWI proofs based on this kind of setup. In some cases, we will have $M = M_1 = M_2$, which may yield some efficiency improvements. We may use the same set of vectors, i.e., instead of working with $u_1, \ldots, u_I$ and $v_1, \ldots, v_J$ we may simplify to the case where we just have $u_1, \ldots, u_I \in M$. Similarly, for commitments to exponents we use $u = v$. Finally, E may be symmetric, i.e., for all $u, v \in M$ we have $E(u, v) = E(v, u)$. We call this the *symmetric setting*.

Instantiation 1: Subgroup decision. Recall in this setting we have two cyclic groups G, G_T of order $\mathbf{n} = \mathbf{pq}$ and a bilinear map $e : G \times G \to G_T$. The subgroup decision assumption says that we cannot distinguish whether an element h has order $\mathbf{q}$ or order $\mathbf{n}$. We will use h of order $\mathbf{q}$ to get perfect soundness, while we will use h of order $\mathbf{n}$ to get perfect witness indistinguishability. Since e is non-degenerate, $e(h, h)$ generates G_T when h has order $\mathbf{n}$. This means the map $\mu : \mathbb{Z}_{\mathbf{n}} \to G_T$ given by $\rho \mapsto e(h, h)^\rho$ has trivial kernel 0.

Instantiation 2: XDH and SXDH. Here we have three prime order groups with a bilinear map $e : G_1 \times G_2 \to G_T$. As described in the previous section, we get $\mathbb{Z}_{\mathbf{p}}$ modules $M_1 = G_1^2, M_2 = G_2^2$. Entry-wise multiplication also makes $M_T = G_T^4$ a $\mathbb{Z}_{\mathbf{p}}$-module. There is a bilinear map given by

$$E_4 : G_1^2 \times G_2^2 \to G_T^4 \qquad (\begin{pmatrix} a \\ b \end{pmatrix}, (x, y)) \mapsto \begin{pmatrix} e(a,x) & e(a,y) \\ e(b,x) & e(b,y) \end{pmatrix}.$$

It is easy to see that

$$E_4(\begin{pmatrix} 1 \\ g_1 \end{pmatrix}, (1, g_2)) \quad , \quad E_4(\begin{pmatrix} 1 \\ g_1 \end{pmatrix}, (g_2, 1)) \quad , \quad E_4(\begin{pmatrix} g_1 \\ 1 \end{pmatrix}, (1, g_2)) \quad , \quad E_4(\begin{pmatrix} g_1 \\ 1 \end{pmatrix}, (g_2, 1))$$

form a basis for G_T^4 since $e(g_1, g_2)$ generates G_T. By the bilinear properties of E_4 we therefore have that

$$E_4(u_1, v_1) \quad , \quad E_4(u_1, v_2) \quad , \quad E_4(u_2, v_1) \quad , \quad E_4(u_2, v_2)$$

form a basis for G_T^4, whenever u_1, u_2 are linearly independent in G_1^2 and v_1, v_2 are linearly independent in G_2^2. Therefore, when they are linearly independent the map

$$\mu_4 : \mathbb{Z}_{\mathbf{p}}^4 \to G_T^4 \qquad (\rho_{11}, \rho_{12}, \rho_{21}, \rho_{22}) \mapsto \prod_{i=1}^{2} \prod_{j=1}^{2} E_4(u_i, v_j)^{\rho_{ij}}$$

has trivial kernel $(0, 0, 0, 0)$.

Instantiation 3: DLIN. In this setting we have a bilinear map $e : G \times G \to G_T$. With entry-wise multiplication, we get the $\mathbb{Z}_{\mathbf{p}}$-modules $M_1 = M_2 = G^3$. In the main body of the paper, we will use the module $M_T = G_T^6$ given by entry-wise multiplication. In special cases, the module G_T^9 will be more useful, see Section 8.

We will use the symmetric bilinear map $E_6 : G^3 \times G^3 \to G_T^6$ given by

$$(\begin{pmatrix} a \\ b \\ c \end{pmatrix}, (x, y, z)) \mapsto \begin{pmatrix} e(a,x) & e(a,y)e(b,x) & e(a,z)e(c,x) \\ & e(b,y) & e(b,z)e(c,y) \\ & & e(c,z) \end{pmatrix}.$$

The corresponding map

$$\mu_6 : \mathbb{Z}_{\mathbf{p}}^9 \to G_T^6 \qquad (\rho_{11}, \ldots, \rho_{33}) \mapsto \prod_{i=1}^{3} \prod_{j=1}^{3} E(u_i, u_j)^{\rho_{ij}}$$

has a non-trivial kernel. If u_1, u_2, u_3 form a basis for G^3, the three identities $E_6(u_i, u_j)E_6(u_j, u_i)^{-1} = 1$ yield a basis for the kernel of μ_6. This basis consists of the vectors

$$\eta_1 = (0, 1, 0, -1, 0, 0, 0, 0, 0) \ , \ \eta_2 = (0, 0, 1, 0, 0, 0, -1, 0, 0) \ \text{ and } \ \eta_3 = (0, 0, 0, 0, 0, 1, 0, -1, 0).$$

For any linearly independent u_1, u_2, u_3 we have that

$$E_6(u_1, u_1) \ , \ E_6(u_1, u_2) \ , \ E_6(u_1, u_3) \ , \ E_6(u_2, u_2) \ , \ E_6(u_2, u_3) \ , \ E_6(u_3, u_3)$$

form a basis for G_T^6.

5 Pairing Product Equations

In this section, we will assume that we have already committed to the variables. We will offer a method to construct non-interactive proofs for the committed values satisfying a pairing product equation. Our method yields proofs with perfect completeness, perfect soundness and on a simulated common reference string with perfectly hiding commitments it gives us proofs with perfect witness-indistinguishability.

A simple pairing product equation. We have commitments $c_1, \ldots, c_Q \in M_1$ and $d_1, \ldots, d_Q \in M_2$. We will look at the satisfiability of the following simple pairing product equation over variables $x_1, \ldots, x_Q \in M_1, y_1, \ldots, y_Q \in M_2$ and $r_{qi}, s_{qj} \in R$.

$$\prod_{q=1}^{Q} E(x_q, y_q) = T \qquad \text{and} \qquad c_q = x_q \prod_{i=1}^{I} u_i^{r_{qi}} \ , \ d_q = y_q \prod_{j=1}^{J} v_j^{s_{qj}},$$

where T is a constant in M_T.

Suppose, we have x_q, y_q, r_{qi}, s_{qi} so the equations described above hold. For arbitrary $t_{ij}, t_h \in R$ we have the following equality, which is central to this paper:

$$\begin{aligned}
\prod_{q=1}^{Q} E(c_q, d_q) \cdot T^{-1} &= \prod_{q=1}^{Q} E(x_q \prod_{i=1}^{I} u_i^{r_{qi}}, y_q \prod_{j=1}^{J} v_j^{s_{qj}}) \cdot T^{-1} \\
&= \prod_{q=1}^{Q} E(x_q, y_q) \cdot T^{-1} \cdot \prod_{q=1}^{Q} \prod_{i=1}^{I} E(u_i^{r_{qi}}, y_q \prod_{j=1}^{J} v_j^{s_{qj}}) \cdot \prod_{q=1}^{Q} \prod_{j=1}^{J} E(x_q, v_j^{s_{qj}}) \\
&= 1 \cdot \prod_{i=1}^{I} E(u_i, \prod_{q=1}^{Q} d_q^{r_{qi}}) \cdot \prod_{j=1}^{J} E(\prod_{q=1}^{Q} x_q^{s_{qj}}, v_j) \\
&= \prod_{i=1}^{I} E(u_i, \prod_{j=1}^{J} v_j^{t_{ij}} \cdot \prod_{q=1}^{Q} d_q^{r_{qi}}) \cdot \prod_{j=1}^{J} E(\prod_{i=1}^{I} u_i^{-t_{ij}} \cdot \prod_{q=1}^{Q} x_q^{s_{qj}}, v_j) \\
&= \prod_{i=1}^{I} E(u_i, \prod_{j=1}^{J} v_j^{t_{ij}} \cdot \prod_{q=1}^{Q} d_q^{r_{qi}}) \cdot \prod_{j=1}^{J} E(\prod_{i=1}^{I} u_i^{-t_{ij} + \sum_{h=1}^{H} t_h \eta_{hij}} \cdot \prod_{q=1}^{Q} x_q^{s_{qj}}, v_j).
\end{aligned}$$

Write

$$\pi_i := \prod_{j=1}^{J} v_j^{t_{ij}} \cdot \prod_{q=1}^{Q} d_q^{r_{qi}} \qquad \text{and} \qquad \psi_j := \prod_{i=1}^{I} u_i^{\sum_{h=1}^{H} t_h \eta_{hij}} \cdot \prod_{i=1}^{I} u_i^{-t_{ij}} \cdot \prod_{q=1}^{Q} x_q^{s_{qj}},$$

to get the simpler

$$\prod_{q=1}^{Q} E(c_q, d_q) \ = \ T \ \cdot \ \prod_{i=1}^{I} E(u_i, \pi_i) \ \cdot \ \prod_{j=1}^{J} E(\psi_j, v_j). \tag{1}$$

We shall use π_i's and ψ_j's computed in this way as witness-indistinguishable proofs. In those proofs, we will choose the t_{ij}'s and the t_h's at random from R. Perfect completeness of the NIWI proofs will follow from Equation 1. Perfect soundness of our proofs will follow from the fact that for any x_q, y_q such that there exists r_{qi}, s_{qj} so $c_q = x_q \prod_{i=1}^{I} u_i^{r_{qi}}, d_q = \prod_{j=1}^{J} v_j^{s_{qj}}$ valid proofs satisfying Equation (1) imply

$$\prod_{q=1}^{Q} E(x_q, y_q) \cdot T^{-1} \ \in \ \prod_{i=1}^{I} E(u_i, M_2) \cdot \prod_{j=1}^{J} E(M_1, v_j).$$

To prove witness indistinguishability, the following lemma will be useful.

Lemma 1 *Assume we have $u_1, \ldots, u_I \in M_1$ and $v_1, \ldots, v_J \in M_2$ and $\eta_1, \ldots, \eta_H$ generating the kernel of μ. Consider two witnesses x_q, y_q, r_{qi}, s_{qj} and $x'_q, y'_q, r'_{qi}, s'_{qj}$ satisfying the equations. If for all q we have $x_q, x'_q \in U, y_q, y'_q \in V$ and we pick the t_{ij}'s and t_h's at random from R, then the distribution of the resulting proofs π_i, ψ_j's and π'_i, ψ'_j's are identical.*

Proof. Consider a witness, x_q, y_q, r_{qi}, s_{qj} as specified in the lemma. This gives us $\pi_1, \ldots, \pi_I \in V$ and $\psi_1, \ldots, \psi_J \in U$. Since we pick the t_{ij}'s at random, the π_i's are distributed uniformly at random in V. Consider any fixed tuple $(\pi_1, \ldots, \pi_I)$ of elements from V. The corresponding ψ_j's in U satisfy $\prod_{j=1}^{J} E(\psi_j, v_j) = \prod_{q=1}^{Q} E(c_q, d_q) \cdot T^{-1} \prod_{i=1}^{I} E(u_i, \pi_i)^{-1}$. Since $\eta_1, \ldots, \eta_H$ generate the kernel of μ, by picking the t_h's at random in the construction of the ψ_j's, we get random ψ_j's from U such that $\prod_{j=1}^{J} E(\psi_j, v_j) = \prod_{q=1}^{Q} E(c_q, d_q) \cdot T^{-1} \prod_{i=1}^{I} E(u_i, \pi_i)^{-1}$. We conclude that with the witness x_q, y_q, r_{qi}, s_{qj} we get a uniform random sample of π_i, ψ_j under the restriction that $\prod_{q=1}^{Q} E(c_q, d_q) = T \cdot \prod_{i=1}^{I} E(u_i, \pi_i) \cdot \prod_{j=1}^{J} E(\psi_j, v_j)$. By a similar argument the other witness, $x'_q, y'_q, r'_{qi}, s'_{qj}$ gives exactly the same distribution on π'_i, ψ'_j. □

The symmetric setting. In the symmetric setting, where $M = M_1 = M_2$ and we use the same generators $u_1, \ldots, u_I$ for both modules and E is symmetric, we can simplify the expression by collapsing the proofs. We have

$$\prod_{q=1}^{Q} E(c_q, d_q) \cdot T^{-1} = \prod_{i=1}^{I} E(u_i, \pi_i) \cdot \prod_{j=1}^{I} E(\psi_j, u_j) = \prod_{i=1}^{I} E(u_i, \pi_i \psi_i).$$

This may lead to protocols with higher efficiency.

General pairing product equations. In the general case, we are interested in variables $x_1, \ldots, x_M \in M_1, y_1, \ldots y_N \in M_2$ and $r_{mi}, s_{nj} \in R$ so

$$\prod_{q=1}^{Q} E(a_q \prod_{m=1}^{M} x_m^{\alpha_{qm}}, b_q \prod_{n=1}^{N} y_n^{\beta_{qn}}) = T \quad , \quad c_m = x_m \prod_{i=1}^{I} u_i^{r_{mi}} \ , \ d_n = y_n \prod_{j=1}^{J} v_j^{s_{nj}},$$

for constants $c_m, a_q \in M_1, d_n, b_q \in M_2, T \in M_T, \alpha_{qm}, \beta_{qn} \in R$.

The commitments are homomorphic, we have

$$a_q \prod_{m=1}^{M} c_m^{\alpha_{qm}} = a_q \prod_{m=1}^{M} (x_m \prod_{i=1}^{I} u_i^{r_{mi}})^{\alpha_{qm}} = a_q \prod_{m=1}^{M} x_m^{\alpha_{qm}} \cdot \prod_{i=1}^{I} u_i^{\sum_{m=1}^{M} \alpha_{qm} r_{mi}}.$$

This means, anybody can compute commitments to $a_q \prod_{m=1}^{M} x_m^{\alpha_{qm}}$. In a similar fashion, anybody can compute commitments to $b_q \prod_{n=1}^{N} y_n^{\beta_{qn}}$. The general case of pairing product equations, can therefore be reduced to the simpler case we have looked at in this section.

Instantiation 1: Subgroup decision. We are now ready to present our first witness-indistinguishable proof. The common reference string will be $(\mathbf{n}, G, G_T, e, h)$, where h has order $\mathbf{q}$. On a simulation reference string, we use h of order $\mathbf{n}$. When h has order $\mathbf{n}$, the kernel of μ is trivial, so on neither type of reference string do we need to concern ourselves with generators for the kernel.

The statement consists of commitments $c_1, d_1, \ldots, c_Q, d_Q \in G$ and $T \in G_T$, and we claim that c_q, d_q are commitments to $x_q, y_q \in G_{\mathbf{p}}$ so $\prod_{q=1}^{Q} e(x_q, y_q) = T_{\mathbf{p}}$, where $T_{\mathbf{p}} = T^{\mathbf{q}(\mathbf{q}^{-1} \bmod \mathbf{p})}$, i.e., T restricted to the order $\mathbf{p}$ subgroup of G_T.

Suppose we have a witness, $x_q, y_q \in G, r_q, s_q \in \mathbb{Z}_{\mathbf{n}}$ so

$$\prod_{q=1}^{Q} e(x_q, y_q) = T \quad , \quad c_q = x_q h^{r_q} \quad , \quad d_q = y_q h^{s_q}.$$

Since we are in the symmetric setting we can construct a proof $\pi := \prod_{q=1}^{Q} x_q^{s_q} d_q^{r_q}$ so

$$\prod_{q=1}^{Q} E(c_q, d_q) = E(h, \pi).$$

This will be our witness-indistinguishable proof.

Lemma 2 *The non-interactive proof system has perfect completeness, perfect soundness and composable witness indistinguishability. The size of the proof is 1 element from G.*

Proof. Perfect completeness follows from Equation (1). The hardness of the subgroup decision problem implies that it is hard to distinguish a common reference string with h of order $\mathbf{q}$ from a simulated common reference string with h of order $\mathbf{n}$. From Lemma 1 we get perfect witness indistinguishability when h has order $\mathbf{n}$.

It remains to prove that in case h has order $\mathbf{q}$, we get perfect soundness. Define $\lambda \in \mathbb{Z}_{\mathbf{n}}$ to be the number so $\lambda = 1 \bmod \mathbf{p}, \lambda = 0 \bmod \mathbf{q}$. Observe, c_q^{λ} defines a unique $x_q \in G_{\mathbf{p}}$ so $c_q = x_q h^{r_q}$ for some $r_q \in \mathbb{Z}_{\mathbf{n}}$. Similarly, d_q defines a unique $y_q \in G_{\mathbf{p}}$ so $d_q = y_q h^{s_q}$. We have

$$\prod_{q=1}^{Q} e(x_q, y_q) \cdot T^{-1} \in e(h, G),$$

so if we let $T_{\mathbf{p}} = T^{\lambda}$ then we can conclude $\prod_{q=1}^{Q} e(x_q, y_q) = T_{\mathbf{p}}$ in $G_{\mathbf{p}}$. □

It is worth noting that if we know the factorization of $\mathbf{n}$, then we can extract $x_q, y_q \in G_{\mathbf{p}}$ from the commitments, so the scheme is a perfect proof of knowledge.

Instantiation 2: XDH and SXDH. We will construct a NIWI proof for the existence of committed $x_1, \ldots, x_Q \in G_1, y_1, \ldots, y_Q \in G_2$ so $\prod_{q=1}^{Q} e(x_q, y_q) = T$ for a constant $T \in G_T$. The common reference string will contain a description of the groups we are working over and four vectors $u_1, u_2 \in G_1^2, v_1, v_2 \in G_2^2$, such that $u_1 = u_2^r, v_1 = v_2^s$ for some $r, s \in \mathbb{Z}_{\mathbf{p}}$. This means u_1, u_2 are linearly dependent and span a 1-dimensional subspace of G_1^2, and v_1, v_2 are linearly dependent and span a 1-dimensional subspace of G_2^2. We also require that these vectors are linearly independent of $(1, g_1) \in G_1^2, (1, g_2) \in G_2^2$, where g_1 generates G_1 and g_2 generates G_2.

The commitments to the x_q's will be of the form $c_q = (1, x_q) u_1^{r_{q1}} u_2^{r_{q2}}$ and the commitments to the y_q's will be of the form $d_q = (1, y_q) v_1^{s_{q1}} v_2^{s_{q2}}$, for random $r_{q1}, r_{q2}, s_{q1}, s_{q2} \in \mathbb{Z}_{\mathbf{p}}$. We construct the proofs as

$$\pi_1 := v_1^{t_{11}} v_2^{t_{12}} \prod_{q=1}^{Q} d_q^{r_{q1}} \ , \ \pi_2 := v_1^{t_{21}} v_2^{t_{22}} \prod_{q=1}^{Q} d_q^{r_{q2}} \ , \ \psi_1 := u_1^{-t_{11}} u_2^{-t_{21}} \prod_{q=1}^{Q} x_q^{s_{q1}} \ , \ \psi_2 := u_1^{-t_{12}} u_2^{-t_{22}} \prod_{q=1}^{Q} (1, x_q)^{s_{q2}},$$

for randomly chosen $t_{ij} \leftarrow \mathbb{Z}_{\mathbf{p}}$. The proofs satisfy

$$\prod_{q=1}^{Q} E(c_q, d_q) = \begin{pmatrix} 1 & 1 \\ 1 & T \end{pmatrix} E(u_1, \pi_1) E(u_2, \pi_2) E(\psi_1, v_1) E(\psi_2, v_2),^{3}$$

[3] Please, keep in mind that we use entry-wise multiplication, matrix multiplication is not even defined here.

this is what the verifier checks.

Lemma 3 *The scheme described above has perfect completeness, perfect soundness and composable witness indistinguishability. The size of the proof is 4 elements from G_1 and 4 elements from G_2.*

Proof. Perfect completeness follows from Equation (1) and the fact that all operations are efficiently computable. By the SXDH assumption, we cannot distinguish the common reference string from a simulated reference string, where u_1 and u_2 are linearly independent, and v_1 and v_2 are linearly independent. When both these pairs are linearly independent, we have $U = G_1^2$ and $V = G_2^2$, and therefore $(1, x_q) \in U$ and $(1, y_q) \in V$. Lemma 1 then gives us perfect witness indistinguishability.

It remains to prove that we have perfect soundness on a real common reference string. Since u_1, u_2 span a 1-dimensional vector space, which does not contain $(1, g_1)$ each c_q has a unique x_q so $c_q = (1, x_q)u_1^{r_{q1}}u_2^{r_{q2}}$. Similarly, each d_q defines a unique y_q so d_q is a commitment to $(1, y_q)$. A valid proof implies

$$\prod_{q=1}^{Q} E(\begin{pmatrix} 1 \\ x_q \end{pmatrix}, (1, y_q)) \begin{pmatrix} 1 & 1 \\ 1 & T^{-1} \end{pmatrix} \in E(u_1, G_2^2)E(u_2, G_2^2)E(G_1^2, v_1)E(G_1^2, v_2).$$

Let us consider the possible values the bilinear map can take when used on the vectors u_1, u_2, v_1, v_2. Since u_1 and u_2 are set up so they're linearly dependent we have $E(u_1, G_2^2)E(u_2, G_2^2) = E(u_2, G_2^2)$, and similarly since v_1 and v_2 are linearly dependent we have $E(G_1^2, v_1)E(G_1^2, v_2) = E(G_1^2, v_2)$. Let us now consider what the vectors in these two sets look like. Write $u_2 = (g_1, g_1^\alpha)$ and $v_2 = (g_2, g_2^\beta)$ for $\alpha, \beta \in \mathbb{Z}_{\mathbf{p}}$. For any vector $(x, y) \in G_2^2$ we have

$$E(u_2, (x, y)) = E(\begin{pmatrix} g_1 \\ g_1^\alpha \end{pmatrix}, (x, y)) = \begin{pmatrix} e(g_1, x) & e(g_1, y) \\ e(g_1, x)^\alpha & e(g_1, y)^\alpha \end{pmatrix}.$$

Similarly, for any $(a, b) \in G_1^2$ we have

$$E(\begin{pmatrix} a \\ b \end{pmatrix}, v_2) = E(\begin{pmatrix} a \\ b \end{pmatrix}, (g_2, g_2^\beta)) = \begin{pmatrix} e(a, g_2) & e(a, g_2)^\beta \\ e(b, g_2) & e(b, g_2)^\beta \end{pmatrix}.$$

The existence of proofs $\pi_1, \pi_2, \psi_1, \psi_2$ implies the existence of a, b, x, y so

$$\begin{pmatrix} 1 & 1 \\ 1 & \prod_{q=1}^{Q} e(x_q, y_q) \cdot T^{-1} \end{pmatrix} = \begin{pmatrix} e(g_1, x)e(a, g_2) & e(g_1, y)e(a, g_2)^\beta \\ e(g_1, x)^\alpha e(b, g_2) & e(g_1, y)^\alpha e(b, g_2)^\beta) \end{pmatrix}.$$

This means $e(g_1, x) = e(a, g_2)^{-1}$. Inserting this in entry $(1, 2)$ gives us $y = x^\beta$. While inserting it in entry $(2, 1)$ shows that $b = a^\alpha$. Inserting these three observations in entry $(2, 2)$ we conclude

$$\prod_{q=1}^{Q} e(x_q, y_q) = Te(g_1, y)^\alpha e(b, g_2)^\beta = T(e(g_1, x)e(a, g_2))^{\alpha\beta} = T.$$

□

If we know the appropriate discrete logarithms, then we can decrypt the ElGamal ciphertext c_q, d_q and extract x_q, y_q. In other words, we have a perfect proof of knowledge.

Instantiation 3: DLIN. Let us return to the symmetric setting using the DLIN assumption. We set up the common reference string with three vectors $u_1 = (f, 1, g), u_2 = (1, h, g), u_3 = (u, v, w)$ such that they form a 2-dimensional subspace of G^3 and f, h, g all are generators of G. We require that $(1, 1, g) \notin U$. Each commitment c_q, d_q therefore uniquely defines x_q, y_q so $c_q = (1, 1, x_q)\prod_{i=1}^{3} u_i^{r_{qi}}, d_q = (1, 1, y_q)\prod_{j=1}^{J} u_j^{s_{qj}}$.

We are interested in the statement $\prod_{q=1}^{Q} e(x_q, y_q) = T$. Following Equation 1 in the symmetric setting, we let the proof consist of π_1, π_2, π_3 given by

$$\pi_i = \prod_{j=1}^{3} u_j^{\sum_{h=1}^{3} t_h \eta_{hij}} \cdot \prod_{q=1}^{Q} (1, 1, x_q)^{s_{qi}} d_q^{r_{qi}}.$$

The verifier checks that

$$\prod_{q=1}^{Q} E_6(c_q, d_q) = \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & T \end{pmatrix} \prod_{i=1}^{3} E_6(u_i, \pi_i).$$

Lemma 4 *The proof has perfect completeness, perfect soundness and composable witness indistinguishability. The proof consists of 9 elements from G.*

Proof. Perfect completeness follows from Equation (1) and the fact that we can compute all operations efficiently. By the DLIN assumption the common reference string is indistinguishable from a common reference string with u_1, u_2, u_3 being linearly independent. In the latter setting, we have $U = G^3$ and therefore all $(1, 1, x_q), (1, 1, y_q) \in U$. By Lemma 1 we therefore have perfect witness indistinguishability on this kind of reference string.

It remains to prove perfect soundness. Since $(1, 1, g) \notin U$, each commitment c_q, d_q specifies unique messages $(1, 1, x_q), (1, 1, y_q)$. Since $(1, 1, g)$ is linearly independent of u_1, u_2 we have

$$\prod_{q=1}^{Q} E_6(\begin{pmatrix} 1 \\ 1 \\ x_q \end{pmatrix}, (1, 1, y_q)) \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & T \end{pmatrix}^{-1} \in E_6(u_1, G^3) E_6(u_2, G^3)$$

implies $\prod_{q=1}^{Q} e(x_q, y_q) = T$. □

Given the relevant discrete logarithms of f, h with respect to g it is possible to decrypt the commitments c_q and d_q to get out the plaintexts x_q, y_q. We therefore have a perfect proof of knowledge.

6 General Arithmetic Gates

The common reference string contains, $u, u_1, \ldots, u_I \in M_1$ and $v, v_1, \ldots, v_J \in M_2$ as well as IJ vectors $\eta_1, \ldots, \eta_H$. The common reference string should be indistinguishable from a simulated reference string, and on a simulated reference string we require $u \in U, v \in V$ and $\eta_1, \ldots, \eta_H$ generate the kernel of μ.

We will focus on the following simple case first. We have commitments $c_1, \ldots, c_q \in M_1, d_1, \ldots, d_q \in M_2$ and interested in the existence of $\phi_q, r_{qi}, \theta_q, s_{qj}$ so

$$c_q = u^{\phi_q} \prod_{i=1}^{I} u_i^{r_{qi}}\ ,\ d_q = v^{\theta_q} \prod_{j=1}^{J} v_j^{s_{qj}} \quad \text{and} \quad \sum_{q=1}^{Q} \phi_q \theta_q = 0.$$

It follows from Equation 1 that if this is the case, then for arbitrary $t_{ij}, t_h \in R$ we have

$$\prod_{q=1}^{Q} E(c_q, d_q) \ = \ \prod_{i=1}^{I} E(u_i, \pi_i) \ \cdot \ \prod_{j=1}^{J} E(\psi_j, v_j),$$

where

$$\pi_i := \prod_{j=1}^{J} v_j^{t_{ij}} \cdot \prod_{q=1}^{Q} d_q^{r_{qi}} \qquad \text{and} \qquad \psi_j := \prod_{i=1}^{I} u_i^{\sum_{h=1}^{H} t_h \eta_{hij}} \cdot \prod_{i=1}^{I} u_i^{-t_{ij}} \cdot \prod_{q=1}^{Q} u^{\phi_q s_{qj}}.$$

This will give us perfect completeness. Perfect witness-indistinguishability on a simulated reference string, where $u \in U, v \in V$ follows from the following corollary to Lemma 1.

Corollary 5 *If $u \in U$ and $v \in V$ then for any set of $\phi_q, r_{qi}, \theta_q, s_{qj}$ satisfying the equation above, by picking t_{ij}, t_h at random from R we get the same distribution of π_i, ψ_j's.*

To argue perfect soundness, we will use that a valid proof implies

$$E(u,v)^{\sum_{q=1}^{Q} \phi_q \theta_q} \in \prod_{i=1}^{I} E(u_i, M_2) \prod_{j=1}^{J} E(M_1, v_j),$$

for any possible way of writing $c_q = u^{\phi_q} \prod_{i=1}^{I} u_i^{r_{qi}}$ and $d_q = v^{\theta_q} \prod_{j=1}^{J} v_j^{s_{qj}}$.

The symmetric case. In the symmetric case, where E is symmetric and $u = v, I = J, u_1 = v_1, \ldots, u_I = v_j$, we obtain a computational saving by combining the proofs. The verifier checks $\prod_{q=1}^{Q} E(c_q, d_q) = \prod_{i=1}^{I} E(u_i, \pi_i \psi_i)$.

General arithmetic gate. In evaluating a general arithmetic gate, we have commitments $c_1, \ldots, c_K \in M_1, d_1, \ldots, d_L \in M_2$ and constants $\alpha_k, \beta_\ell, \gamma_{k\ell}, \tau \in R$. A witness will be on the form $\phi_k, r_{ki}, \theta_\ell, s_{\ell j} \in R$ so

$$\sum_{k=1}^{K} \alpha_k \phi_k \; + \; \sum_{\ell=1}^{L} \beta_\ell \theta_\ell \; + \; \sum_{k=1}^{K} \sum_{\ell=1}^{L} \gamma_{k\ell} \phi_k \theta_\ell \; = \; \tau, \quad c_k = u^{\phi_k} \prod_{i=1}^{I} u_i^{r_{ki}} \quad , \quad d_\ell = v^{\theta_\ell} \prod_{j=1}^{J} v_j^{s_{\ell j}}.$$

Let us observe that due to the homomorphic properties of the commitment schemes, this case can be reduced to the simpler case that we just handled. Anybody can easily compute trivial commitments in M_2 to the α_k's as v^{α_k}. Similarly, anybody can compute commitments to β_ℓ in M_1 as u^{β_ℓ}. Given a commitment to ϕ_k of the form $c_k = u^{\phi_k} \prod_{i=1}^{I} u_i^{r_{ki}}$, it is for any $\gamma_{k\ell} \in R$ straightforward to compute a commitment to $\gamma_{k\ell}\phi_k$ as $c_k^{\gamma_{k\ell}} = u^{\gamma_{k\ell}\phi_k} \prod_{i=1}^{I} u_i^{\gamma_{k\ell} r_{ki}}$. Finally, $u^{-\tau}$ is a commitment to $-\tau$ and u, v are commitments to 1 in respectively M_1 and M_2. Rewriting the general equation as

$$\sum_{k=1}^{K} \phi_k \cdot \alpha_k \; + \; \sum_{\ell=1}^{L} \beta_\ell \cdot \theta_\ell \; + \; \sum_{k=1}^{K} \sum_{\ell=1}^{L} (\gamma_{k\ell}\phi_k) \cdot \theta_\ell \; + (-\tau) \cdot 1 \; = \; 0,$$

shows that we can make a NIWI proof for the general arithmetic gate using the NIWI proof given earlier.

Instantiation 1: Subgroup decision. The common reference string now contains two group elements g, h, with g playing the role of u and h playing the role of u_1. The element g is a generator, while h has order $\mathbf{q}$. We will suggest a NIWI proof for the statement that $c_1, \ldots, c_Q, d_1, \ldots, d_Q$ are commitments to $\phi_1, \ldots, \phi_Q, \theta_1, \ldots, \theta_Q \in \mathbb{Z}_{\mathbf{p}}$ so $\sum_{q=1}^{Q} \phi_q \theta_q = 0 \bmod \mathbf{p}$. Since h has order $\mathbf{q}$, these commitments define $\phi_q, \theta_q \in \mathbb{Z}_{\mathbf{p}}$ uniquely.

Given a witness $\phi_1, \ldots, \phi_Q, \theta_1, \ldots, \theta_Q \in \mathbb{Z}_{\mathbf{n}}$ and $r_q, s_q \in \mathbb{Z}_{\mathbf{n}}$ so

$$c_q = g^{\phi_q} h^{r_q} \quad , \quad d_q = g^{\theta_q} h^{s_q} \quad , \quad \sum_{q=1}^{Q} \phi_q \theta_q = 0 \bmod \mathbf{n},$$

we simply carry out the NIWI proof from the previous section with $x_q = g^{\phi_q}, y_q = g^{\theta_q}$. We have the following corollary to Lemma 2.

Lemma 6 *The NIWI proof has perfect completeness, perfect soundness and composable witness indistinguishability. The size of the proof is 1 group element from G.*

Instantiation 2: XDH and SXDH. The common reference string will contain two linearly independent vectors $u, u_1 \in G_1^2$ and two linearly independent vectors $v, v_1 \in G_2^2$, whereas in the simulation we choose $u \in U$ and $v \in V$. Given a witness $\phi_q, r_q, \theta_q, s_q \in \mathbb{Z}_{\mathbf{p}}$ so $\sum_{q=1}^{Q} \phi_q \theta_q = 0 \bmod \mathbf{p}$, $c_q = u^{\phi_q} u_1^{r_q}$, $d_q = v^{\theta_q} v_1^{s_q}$, we make proofs

$$\pi := v_1^t \cdot \prod_{q=1}^{Q} d_q^{r_q} \qquad \text{and} \qquad \psi := u_1^{-t} \cdot \prod_{q=1}^{Q} u^{\phi_q s_q},$$

for a randomly selected $t \leftarrow \mathbb{Z}_{\mathbf{p}}$. The verifier accepts if

$$\prod_{q=1}^{Q} E_4(c_q, d_q) = E_4(u_1, \pi) E_4(\psi, v_1).$$

Lemma 7 *The proof has perfect completeness, perfect soundness and composable witness indistinguishability assuming the SXDH problem is hard. It consists of 2 elements from G_1 and 2 elements from G_2.*

Proof. Perfect completeness follows by inspection. By the SXDH assumption a common reference string as described above is indistinguishable from a simulated reference string where $u = u_1^r$ and $v = v_1^s$ for some $r, s \in \mathbb{Z}_{\mathbf{p}}$. In this latter case, we have $u \in U$ and $v \in V$, so by Corollary 5 we have perfect witness indistinguishability on this kind of common reference string.

It remains to argue perfect soundness, when u, u_1 and v, v_1 are linearly independent. Note, in this case the commitments are perfectly binding to ϕ_q, θ_q. We have

$$E_4(u, v)^{\sum_{q=1}^{Q} \phi_q, \theta_q} \in E_4(u_1, G_2^2) \cdot E_4(G_1^2, v_1).$$

By the linear independence of the vectors u, u_1 and v, v_1, $E_4(u, v), E_4(u_1, v), E_4(u, v_1), E_4(u_1, v_1)$ is a basis for G_T^4. This implies $E_4(u, v)^{\sum_{q=1}^{Q} \phi_q \theta_q} = 1$, so $\sum_{q=1}^{Q} \phi_q \theta_q = 0 \bmod \mathbf{p}$. □

Instantiation 3: DLIN. We set up the common reference string, so it has three elements $u_1 = (f, 1, g), u_2 = (1, h, g)$, and u which is linearly independent of u_1, u_2. The simulated reference string, will contain $u \in U$. Since E_6 is symmetric we have $E_6(u_1, u_2) = E_6(u_2, u_1)$. The vector $\eta = (0, 1, -1, 0)$ is a basis for the kernel of μ.

Given commitments c_q, d_q we are interested in the existence of $\phi_q, r_{qi}, \theta_q, s_{qi} \in \mathbb{Z}_{\mathbf{p}}$ so

$$\sum_{q=1}^{Q} \phi_q \theta_q = 0 \quad , \quad c_q = u^{\phi_q} u_1^{r_{q1}} u_2^{r_{q2}} \quad , \quad d_q = u^{\theta_q} u_1^{s_{q1}} u_2^{s_{q2}}.$$

From a satisfying witness $\phi_q r_{q1}, r_{q2}, \theta_q, s_{q1}, s_{q2}$ we can create a proof

$$\pi_1 := u_2^t \prod_{q=1}^{Q} d_q^{r_{q1}} u^{\phi_q s_{q1}} \qquad , \qquad \pi_2 := u_1^{-t} \prod_{q=1}^{Q} d_q^{r_{q2}} u^{\phi_q s_{q2}},$$

for randomly chosen $t \leftarrow \mathbb{Z}_{\mathbf{p}}$. The verifier accepts if and only if

$$\prod_{q=1}^{Q} E_6(c_q, d_q) = E_6(u_1, \pi_1) E_6(u_2, \pi_2).$$

Lemma 8 *The proof has perfect completeness, perfect soundness and composable witness indistinguishability. The proof consists of 6 elements from G.*

Proof. Completeness follows from Equation 1. By the DLIN assumption, we cannot distinguish the common reference string from a simulated reference string where $u \in U$. With the latter type of common reference string we have perfect witness indistinguishability according to Corollary 5.

It remains to prove perfect soundness. We have

$$E_6(u,u)^{\sum_{q=1}^{Q}\phi_q\theta_q} \in E_6(u_1,G^3)E_6(u_2,G^3).$$

Since u is linearly independent of u_1, u_2 this means $\sum_{q=1}^{Q}\phi_q\theta_q = 0 \bmod \mathbf{p}$. □

7 Multi-exponentiation

We will without loss of generality consider the task of making a multi-exponentiation of elements in M_1. The case of multi-exponentiation in M_2 is of course similar.

The common reference string will contain, $u_1,\ldots,u_I \in M_1$ and $v, v_1,\ldots,v_J \in M_2$ as well as $\eta_1,\ldots,\eta_H$. On a simulated reference string, we will have $v \in V$ and $\eta_1,\ldots,\eta_H$ generating the kernel of μ.

We will first look at a simple case, and treat the general multi-exponentiation case later. The input consists of commitments $c_1,\ldots,c_Q \in M_1$ and $d_1,\ldots,d_Q \in M_2$. We are interested in the existence of a witness $x_q \in M_1, r_{qi}, \theta_q, s_{qj} \in R$ so

$$c_q = x_q \prod_{i=1}^{I} u_i^{r_{qi}} \quad , \quad d_q = v^{\theta_q} \prod_{j=1}^{J} v_j^{s_{qj}} \quad \text{and} \quad \prod_{q=1}^{Q} x_q^{\theta_q} = t_1,$$

for a constant $t_1 \in M_1$.

Given a satisfying witness $x_q, r_{qi}, \theta_q, s_{qj}$, we get from Equation 1 that for arbitrary $t_{ij}, t_h \in R$

$$\prod_{q=1}^{Q} E(c_q,d_q) \cdot E(t_1,v)^{-1} = \prod_{i=1}^{I} E(u_i,\pi_i) \cdot \prod_{j=1}^{J} E(\psi_j,v_j), \tag{2}$$

where

$$\pi_i := \prod_{j=1}^{J} v_j^{t_{ij}} \cdot \prod_{q=1}^{Q} d_q^{r_{qi}} \qquad \text{and} \qquad \psi_j := \prod_{i=1}^{I} u_i^{\sum_{h=1}^{H} t_h\eta_{hij}} \cdot \prod_{i=1}^{I} u_i^{-t_{ij}} \cdot \prod_{q=1}^{Q} x_q^{s_{qj}}.$$

Perfect completeness follows from this. To argue perfect witness-indistinguishability on a simulated common reference string we have the following corollary to Lemma 1.

Lemma 9 *If $v \in V$ and $\eta_1,\ldots,\eta_H$ generate the kernel of μ, then for any witness $x_q, r_{qi}, \theta_q, s_{qj}$ so $x_1,\ldots,x_Q \in U$ we get the same distribution of proofs π_i, ψ_j.*

Perfect soundness will follow from the fact that a valid proof implies

$$E(\prod_{q=1}^{Q} x_q^{\theta_q} t_1^{-1}, v) \in \prod_{i=1}^{I} E(u_i, M_2) \cdot \prod_{j=1}^{J} E(M_1, v_j)$$

for any way of writing $c_q = x_q \prod_{i=1}^{I} u_i^{r_{qi}}, d_q = v^{\theta_q} \prod_{j=1}^{J} v_j^{s_{qj}}$.

The symmetric case. We may have $M_1 = M_2$ and E symmetric. In case there is overlap between $u_1, \ldots, u_I$ and $v_1, \ldots, v_J$ we may save computation by combining the relevant proofs. We refer to the instantiations for a concrete treatment of this issue.

General multi-exponentiation relationship in M_1. In the general multi-exponentiation case, we are interested in the existence of $x_m \in M_1, \theta_\ell, r_{mi}, s_{\ell j} \in R$ so

$$c_m = x_m \prod_{i=1}^{I} u_i^{r_{mi}} \quad , \quad d_\ell = v^{\theta_\ell} \prod_{j=1}^{J} v_j^{s_{\ell j}} \quad \text{and} \quad \prod_{\ell=1}^{L} a_\ell^{\theta_\ell} \cdot \prod_{m=1}^{M} x_m^{\sum_{\ell=1}^{L} \alpha_{m\ell}\theta_\ell + \beta_m} = t_1,$$

for constants $c_m \in M_1, a_\ell, d_\ell, t_2 \in M_2, \alpha_{m\ell}, \beta_m \in R$. In other words, $c_1, \ldots, c_M$ are commitments to variables $x_1, \ldots, x_M$ and $d_1, \ldots, d_L$ are commitments to variables $\theta_1, \ldots, \theta_L$ so the equation is satisfied.

By the homomorphic properties of the commitment scheme,

$$v^{\beta_m} \prod_{\ell=1}^{L} d_\ell^{\alpha_{m\ell}} = v^{\sum_{\ell=1}^{L} \alpha_{m\ell}\theta_\ell + \beta_m} \prod_{j=1}^{J} v_j^{\sum_{\ell=1}^{L} \alpha_{m\ell} s_{\ell j}}$$

is a commitment to $\sum_{\ell=1}^{L} \alpha_{m\ell}\theta_\ell + \beta_m$. Furthermore, a_ℓ can be seen as a commitment to a_ℓ with randomness $s_{\ell j} = 0$. We now have commitments in M_2 to $\theta_1, \ldots, \theta_L, \sum_{\ell=1}^{L} \alpha_{1\ell}\theta_\ell + \beta_1, \ldots, \sum_{\ell=1}^{L} \alpha_{m\ell}\theta_\ell + \beta_M$ and commitments in M_1 to $a_1, \ldots, a_L, x_1, \ldots, x_M$. We have reduced the general multi-exponentiation case, to the special case we treated above.

Instantiation 1: Subgroup decision. The common reference string contains g, h, where h has order $\mathbf{q}$. Given a witness $x_q \in G, r_q, \theta_q, s_q \in \mathbb{Z}_{\mathbf{n}}$ so

$$c_q = x_q h^{r_q} \quad , \quad d_q = g^{\theta_q} h^{s_q} \quad \text{and} \quad \prod_{q=1}^{Q} x_q^{\theta_q} = t,$$

we compute a proof of the form

$$\psi := \prod_{q=1}^{Q} d_q^{r_q} x_q^{s_q}.$$

The verifier accepts if and only if

$$\prod_{q=1}^{Q} e(c_q, d_q) = e(t, g) e(\psi, h).$$

We have the following corollary to Lemma 2.

Lemma 10 *The proof has perfect completeness, perfect soundness and assuming the subgroup decision problem is hard it has composable witness indistinguishability. The size is 1 group element.*

Instantiation 2: XDH and SXDH. The common reference string will contain $u_1, u_2 \in G_1^2$ so $(1, g_1) \notin U$ and $v, v_1 \in G_2^2$ so $v \notin V$. Given a witness $x_q \in G_1, r_{q1}, r_{q2}, \theta_q, s_q \in \mathbb{Z}_{\mathbf{p}}$ so

$$c_q = (1, x_q) u_1^{r_{q1}} u_2^{r_{q2}} \quad , \quad d_q = v^{\theta_q} v_1^{s_q} \quad \text{and} \quad \prod_{q=1}^{Q} x_q^{\theta_q} = t_1,$$

we construct a NIWI proof as

$$\pi_1 := v^{t_{11}} \prod_{q=1}^{Q} d_q^{r_{q1}} \quad , \quad \pi_2 := v^{t_{21}} \prod_{q=1}^{Q} d_q^{r_{q2}} \quad , \quad \psi := u_1^{-t_{11}} u_2^{-t_{21}} \prod_{q=1}^{Q} (1, x_q)^{s_q},$$

for randomly chosen $t_{11}, t_{21} \leftarrow \mathbb{Z}_{\mathbf{p}}$. The verifier accepts if and only if

$$\prod_{q=1}^{Q} E_4(c_q, d_q) = E_4((1, t_1), v) E_4(u_1, \pi_1) E_4(u_2, \pi_2) E_4(\psi, v_1).$$

Lemma 11 *The proof has perfect completeness, perfect soundness, and assuming the SXDH problem is hard it has composable witness indistinguishability. A proof consists of 2 elements from G_1 and 4 elements from G_2.*

Proof. Perfect completeness on both real and simulated common reference strings follows from Equation 2. Perfect witness-indistinguishability follows from Lemma 9. To argue perfect soundness, note that the commitments c_q and d_q define x_q and θ_q uniquely. We have

$$E_4(\prod_{q=1}^{Q} (1, x_q)^{\theta_q} \cdot (1, t_1^{-1}), v) \in E_4(u_1, G_2^2) \cdot E_4(G_1^2, v_1),$$

since u_1, u_2 are linearly dependent. The linear inpendence of $(1, g)$ and u_1, and the linear independence of v and v_1 implies that $E_4((1, g), v), E_4(u_1, v), E_4((1, g), v_1), E_4(u_1, v_1)$ is a basis for G_T^4. This implies $\prod_{q=1}^{Q} x_q^{\theta_q} = t_1$. □

Instantiation 3: DLIN. The common reference string contains vectors $u_1 = v_1 = (f, 1, g), u_2 = v_2 = (1, h, g)$ and u_3, v so $u_3 = u_1^r u_2^s$ for some $r, s \in \mathbb{Z}_{\mathbf{p}}$ while $v \notin V$. We have that $\eta = (0, 1, -1, 0, 0, 0)$ corresponding to the identity $E_6(u_1, v_2) = E_6(u_2, v_1)$ generates the kernel of μ. Given a witness $x_q \in G, r_{q1}, r_{q2}, r_{q3}, \theta_q, s_{q1}, s_{q2} \in \mathbb{Z}_{\mathbf{p}}$ so

$$c_q = (1, 1, x_q) \prod_{i=1}^{3} u_i^{r_{qi}} \quad , \quad d_q = v^{\theta_q} \prod_{j=1}^{2} v_j^{s_{qj}} \quad \text{and} \quad \prod_{q=1}^{Q} x_q^{\theta_q} = t,$$

we construct a proof as

$$\pi_1 := u_2^{t_{12}} u_3^{t_{13}} \prod_{q=1}^{Q} d_q^{r_{q1}} (1, 1, x_q)^{s_{q1}}, \pi_2 := u_1^{-t_{12}} u_3^{t_{23}} \prod_{q=1}^{Q} d_q^{r_{q2}} (1, 1, x_q)^{s_{q2}}, \pi_3 := u_1^{-t_{13}} u_2^{t_{23}} \prod_{q=1}^{Q} d_q^{r_{q3}},$$

for randomly chosen $t_{12}, t_{13}, t_{23} \leftarrow \mathbb{Z}_{\mathbf{p}}$. The verifier checks that

$$\prod_{q=1}^{Q} E_6(c_q, d_q) = E_6((1, 1, t_1), v) E_6(u_1, \pi_1) E_6(u_2, \pi_2) E_6(u_3, \pi_3).$$

Lemma 12 *The proof has perfect completeness, perfect soundness and assuming the DLIN problem is hard it has composable witness indistinguishability. The proof consists of 9 group elements.*

Proof. Perfect completeness follows from Equation (2). Perfect witness-indistinguishability on a simulation reference string follows from Lemma 9. To argue perfect soundness observe that the commitments c_q and d_q define x_q and θ_q uniquely. Since u_3 is linearly dependent on u_1, u_2 we have $E_6(\prod_{q=1}^{Q}(1,1,x_q)^{\theta_q} \cdot (1,1,t)^{-1}, v) \in E_6((f,1,g),G^3)E_6((1,h,g),G^3)$. Write $v = (1,1,g)^{\delta}u_1^{\delta_1}u_2^{\delta_2}$, then we have

$$\begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & e(\prod_{q=1}^{Q} x_q^{\theta_q} \cdot t^{-1}, g) \end{pmatrix} \in E_6(\begin{pmatrix} f \\ 1 \\ g \end{pmatrix}, G^3)E_6(\begin{pmatrix} 1 \\ h \\ g \end{pmatrix}, G^3).$$

This implies $\prod_{q=1}^{Q} x_q^{\theta_q} = t$ as required. □

8 The One-Sided Case

We have given NIWI proofs for the general case, where we have commitments in both M_1 and M_2. If all the commitments in one of the modules are trivial, i.e., we just have constants in either M_1 or M_2 it may be possible to give simpler NIWI proofs. In this section, we will offer simpler NIWI proofs for the one-sided case.

We remark that the NIWI proofs based on the subgroup decision problem are already so efficient that there is no saving to be made by considering the one-sided case. We therefore only consider the instantiations based on the DLIN assumption and the SXDH assumption. Moreover, in the one-sided case we only need the DDH assumption to hold in one of the groups. We can therefore restrict ourselves to the XDH assumption.

8.1 Pairing Product Equations

In case all the commitments in M_1 or M_2 are trivial we may simplify our NIWI proofs. Without loss of generality, let us look at the case where all the commitments in M_2 are trivial, i.e., we have public elements $b_1, \ldots, b_Q$. Given satisfying x_q, r_{qi} we have for arbitrary $t_h \in R$,

$$\begin{aligned} \prod_{q=1}^{Q} E(c_q, b_q) \cdot T^{-1} &= \prod_{q=1}^{Q} E(x_q \prod_{i=1}^{I} u_i^{r_{qi}}, b_q) \cdot T^{-1} \\ &= \prod_{q=1}^{Q} E(x_q, b_q) \cdot T^{-1} \cdot \prod_{q=1}^{Q}\prod_{i=1}^{I} E(u_i^{r_{qi}}, b_q) \\ &= 1 \cdot \prod_{i=1}^{I} E(u_i, \prod_{q=1}^{Q} b_q^{r_{qi}}) \\ &= \prod_{i=1}^{I} E(u_i, \prod_{j=1}^{J} v_j^{\sum_h t_h \eta_{hij}} \cdot \prod_{q=1}^{Q} b_q^{r_{qi}}) \\ &= \prod_{i=1}^{I} E(u_i, \pi_i), \end{aligned} \tag{3}$$

where $\pi_i := \prod_{j=1}^{J} v_j^{\sum_h t_h \eta_{hij}} \cdot \prod_{q=1}^{Q} b_q^{r_{qi}}$.

Perfect completeness will follow from this equation. The following lemma will give us perfect witness indistinguishability on a simulated common reference string.

Lemma 13 *Assume we have $u_1, \ldots, u_I \in M_1$ and $v_1, \ldots, v_J \in M_2$ and $\eta_1, \ldots, \eta_H$ generates the kernel of μ. In the special case described above, all witnesses with $x_1, \ldots, x_Q \in U$ and constants $b_1, \ldots, b_Q \in V$ yield the same distribution of proofs π_i if we choose the t_h's at random from R.*

Proof. Since $c_q \in U, b_q \in V$ and $\eta_1, \ldots, \eta_H$ generates the kernel of μ, we get a uniform distribution of the proofs π_i that satisfy the equation by choosing the t_h's at random from R. □

Perfect soundness will follow from the implication of a valid proof that

$$\prod_{q=1}^{Q} E(x_q, b_q) \cdot T^{-1} \in \prod_{i=1}^{I} E(u_i, M_2),$$

whenever we can write $c_q = x_q \prod_{q=1}^{Q} u_i^{r_{qi}}$.

Instantiation 2: XDH and SXDH. The XDH assumption states that in one of the groups the DDH problem is hard. Assume without loss of generality that in group G_1 the DDH problem is hard. This suffices to construct a witness-indistinguishable proof for the special case where $d_1, \ldots, d_Q$ are commitments with trivial randomness, i.e., on the form $(1, b_1), \ldots, (1, b_Q)$. The common reference string contains descriptions of the group and u_1, u_2 that form a 1-dimensional subspace of G_1^2. Now there is a NIWI proof consisting of 2 elements in G_2 for the commitments $c_1, \ldots, c_Q$ containing $(1, x_1), \ldots, (1, x_Q)$ so $\prod_{q=1}^{Q} e(x_q, b_q) = T$.

The prover has witness $x_q \in G_1$ and $r_{qi} \in \mathbb{Z}_{\mathbf{p}}$ so $c_q = (1, x_q) u_1^{r_{q1}} u_2^{r_{q2}}$ and $\prod_{q=1}^{Q} e(x_q, b_q) = 1$. The proof consists of $\pi_1 := \prod_{q=1}^{Q} (1, b_q)^{r_{q1}}$ and $\pi_2 := \prod_{q=1}^{Q} (1, b_q)^{r_{q2}}$. The verifier checks that $\prod_{q=1}^{Q} E_4(c_q, d_q) = \begin{pmatrix} 1 & 1 \\ 1 & T \end{pmatrix} \prod_{i=1}^{2} E_4(u_i, \pi_i)$.

Lemma 14 *The NIWI proof for the one-sided case has perfect completeness, perfect soundness and composable witness indistinguishability assuming the DDH problem is hard in G_1. The proof consists of 2 group elements in G_2.*

Proof. Perfect completeness follows from Equation 3. A simulation string contains u_1, u_2 that are linearly independent. By the DDH assumption in G_1, it is indistinguishable from a common reference string, where u_1 and u_2 are linearly dependent. On a simulation string, u_1 and u_2 form a basis for G_1^2 and therefore $(1, x_q) \in U$. By Lemma 13 we get perfect witness indistinguishability.

To prove soundness, we use the fact that $E_4(u_1, G_2^2) = E_4(u_2, G_2^2)$. The proof therefore shows

$$\prod_{q=1}^{Q} E_4((1, x_q), (1, b_q)) \begin{pmatrix} 1 & 1 \\ 1 & T^{-1} \end{pmatrix} \in E_4(u_1, G_2^2).$$

Since $(1, g_1)$ is linearly independent of u_1 this implies $\prod_{q=1}^{Q} e(x_q, b_q) = T$. □

Instantiation 3: DLIN. It turns out that in the one-sided case, we get simpler proofs by using the bilinear map E_9 defined below instead of E_6. The map E_9 is not symmetric, however, we observe that in the one-sided case symmetry will not be needed. We use the module $M_T = G_T^9$ and the bilinear map $E_9 : G^3 \times G^3 \to G_T^9$ given by

$$\left(\begin{pmatrix} a \\ b \\ c \end{pmatrix}, (x, y, z) \right) \mapsto \begin{pmatrix} e(a,x) & e(a,y) & e(a,z) \\ e(b,x) & e(b,y) & e(b,z) \\ e(c,x) & e(c,y) & e(c,z) \end{pmatrix}.$$

If we have linearly independent elements $u_1, u_2, u_3 \in G^3$, then the map $\mu_9 : \mathbb{Z}_{\mathbf{p}}^9 \to G_T^9$ has trivial kernel and the nine different combinations $E_9(u_i, u_j)$ form a basis of G_T^9.

We will consider the simplified case, where the d_q's are trivial commitments, i.e., $d_q = (1, 1, b_q)$ for public b_q. We still have $c_q \in G^3$ and $T \in G_T$ and want to prove the existence of x_q, r_{qi} so

$$\prod_{q=1}^{Q} e(x_q, b_q) = T \quad , \quad c_q = x_q \prod_{i=1}^{3} u_i^{r_{qi}},$$

where u_1, u_2, u_3 are set up as in the previous example. It turns out that in the one-side case, it is more convenient for us to use the map E_9 instead of E_6, so we will do that. As a consequence, the map μ_9 has trivial kernel, which will make our protocol simpler.

A real common reference string will have $u_3 = u_1^r u_2^s$ for some r, s, such that c_q is a perfectly binding commitment to x_q. On the other hand, a simulated common reference string will have u_1, u_2, u_3 linearly independent, so the commitment is perfectly hiding. The proof is

$$\pi_1 := \prod_{q=1}^{Q} d_q^{r_{q1}} \qquad , \qquad \pi_2 := \prod_{q=1}^{Q} d_q^{r_{q2}} \qquad , \qquad \pi_3 := \prod_{q=1}^{Q} d_q^{r_{q3}}.$$

The verifier checks,

$$\prod_{q=1}^{Q} E_9(c_q, d_q) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & T \end{pmatrix} \prod_{i=1}^{3} E_9(u_i, \pi_i).$$

Please note, since $d_q = (1, 1, b_q)$, the proof only consists of 3 group elements.

Lemma 15 *The proof has perfect completeness, perfect soundness and composable witness indistinguishability assuming the DLIN problem is hard. The proof consists of 3 group elements.*

Proof. Perfect completeness, no matter whether it is a real common reference string or a simulated reference string, follows from Equation 3. By the DLIN assumption, common reference strings and simulated reference strings are indistinguishable. On a simulated reference string, u_1, u_2, u_3 are linearly independent, so $U = G^3$. Therefore, by Lemma 13 we have perfect witness indistinguishability.

It remains to consider perfect soundness on a common reference string, where u_3 is linearly dependent on $u_1 = (f, 1, g), u_2 = (1, h, g)$. From the verification, we get c_q are commitments to unique x_q so

$$\prod_{q=1}^{Q} E_9(\begin{pmatrix} 1 \\ 1 \\ x_q \end{pmatrix}, (1, 1, b_q)) \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & T \end{pmatrix}^{-1} \in E_9(u_1, G^3) E_9(u_2, G^3).$$

This implies the existence of $a, b, c, x, y, z \in G$ so

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & \prod_{q=1}^{Q} e(x_q, b_q) \cdot T^{-1} \end{pmatrix} = E_9(u_1, (a, b, c)) E_9(u_2, (x, y, z)).$$

Since $(1, 1, g)$ is linearly independent of u_1, u_2 we have $\prod_{q=1}^{Q} e(x_q, b_q) = T$. □

8.2 General Arithmetic Gates: Linear Relations

An interesting special case, is the situation where we have commitments $c_1, \ldots, c_K$ and are interested in equations over variables $\phi_k, r_{ki} \in R$ of the form

$$c_k = u^{\phi_k} \prod_{i=1}^{I} u_i^{r_{ki}} \qquad \text{and} \qquad \sum_{k=1}^{K} \phi_k \beta_k = \tau,$$

for constants $\beta_k, \tau \in R$. Given variables $\phi_k, r_{ki} \in R$ satisfying the equation, we have for arbitrary $t_h \in R$

$$\prod_{k=1}^{K} E(c_k, v^{\beta_k}) \cdot E(u,v)^{-\tau} = \prod_{i=1}^{I} E(u_i, \pi_i) \quad \text{where} \quad \pi_i := v^{\sum_{k=1}^{K} \beta_k r_{ki}} \cdot \prod_{j=1}^{J} v_j^{\sum_{h=1}^{H} t_h \eta_{hij}}.$$

We get the following corollary to Lemma 13.

Lemma 16 *If $u \in U$ and $v \in V$, then no matter the witness ϕ_k, r_{ki}, we get identical distributions of $\pi_1, \ldots, \pi_K$.*

For perfect soundness, we will use that for any way of writing $c_k = u^{\phi_k} \prod_{i=1}^{I} u_i^{r_{qi}}$ a valid proof implies

$$E(u,v)^{\sum_{k=1}^{K} \phi_k \beta_k - \tau} \in \prod_{i=1}^{I} E(u_i, M_2).$$

Instantiation 2: XDH and SXDH. The special case, where we have commitments $c_1, \ldots, c_K$ and constants $\beta_1, \ldots, \beta_K, \tau$ and want to prove $\sum_{k=1}^{K} \phi_k \theta_k = \tau$ is easily solvable. The common reference string will contain u, u_1 that span G_1^2 and we select $v = (1, g_2) \in G_2^2$. Assuming the XDH assumption, with the DDH problem being hard in G_1, we cannot distinguish this kind of reference string from one where $u \in U$. The NIWI proof is $\pi := \prod_{k=1}^{K} v^{\beta_k r_k}$. The size is only 1 group elements from G_2 since $v = (1, g_2)$. The verifier checks that

$$\prod_{k=1}^{K} E_4(c_k, v^{\beta_k}) = E_4(u,v)^{\tau} E_4(u_1, \pi).$$

Lemma 17 *The proof has perfect completeness, perfect soundness and composable witness indistinguishability under the XDH assumption. The proof consists of 1 group element from G_2.*

Proof. Perfect completeness follows from Equation 1. The hardness of the DDH problem in G_1 means that we cannot distinguish common reference strings with u, u_1 linearly independent from simulated reference strings with $u \in U$. Perfect witness indistinguishability on simulated reference strings now follows from the fact that $\pi = (1, x)$ is uniquely determined by the verification, so all witnesses yield the same proof. For perfect soundness, we observe $E_4(u,v)^{\prod_{k=1}^{K} \phi_k \beta_k - \tau} \in E_4(u_1, G_2^2)$ implies $\prod_{k=1}^{K} \phi_k \beta_k = \tau$ since u, u_1 are linearly independent. □

Instantiation 3: DLIN. Consider a common reference string set up in the same way as before. In the linear case, we have commitments c_k and constants $\beta_1, \ldots, \beta_K, \tau$. The witness will be of the form ϕ_k, r_{k1}, r_{k2} so

$$\sum_{k=1}^{K} \phi_k \beta_k = \tau \quad , \quad c_k = u^{\phi_k} u_1^{r_{k1}} u_2^{r_{k2}}.$$

Define $v = (1, 1, g)$. We can compute the proof $\pi_1 := v^{\sum_{k=1}^{K} \beta_k r_{k1}}$ and $\pi_2 := v^{\sum_{k=1}^{K} \beta_k r_{k2}}$. This consists of 2 group elements. The verifier checks

$$\prod_{k=1}^{K} E_9(c_k, v^{\beta_k}) = E_9(u,v)^{\tau} \cdot E_9(u_1, \pi_1) E_9(u_2, \pi_2).$$

Lemma 18 *The proof has perfect completeness, perfect soundness and composable witness indistinguishability under the DLIN assumption. The proof consists of 2 group elements.*

Proof. Perfect completeness follows from Equation 3. By the DLIN assumption, we cannot distinguish whether $u \in U$ or not, so common reference string and simulated reference strings are indistinguishable. There are unique proofs π_1, π_2 satisfying the equation, so no matter which witness we have, we get the same proofs. To prove perfect soundness when $u \notin U$, observe that the commitments define ϕ_k, r_{k1}, r_{k2} uniquely. We have

$$E_9(u,v)^{\phi_k\beta_k-\tau} \in E_9(u_1, G^3)E_9(u_2, G^3).$$

Since u, u_1, u_2 are linearly independent we have $E_9(u,v)^{\sum_{k=1}^{K}\phi_k\beta_k-\tau} = 1$, which implies $\sum_{k=1}^{K}\phi_k\beta_k = \tau$. □

8.3 Multi-exponentiation of Constants

We have elements $a_1, \ldots, a_L \in M_1$ and commitments $d_1, \ldots, d_L \in M_2$ and are interested in the existence of $\theta_\ell, s_{\ell j}$ so

$$d_\ell = v^{\theta_\ell}\prod_{j=1}^{J} v_j^{s_{\ell j}} \qquad \text{and} \qquad \prod_{\ell=1}^{L} a_\ell^{\theta_\ell} = t_1,$$

for a constant $t_1 \in M_1$.

Given $\theta_\ell, s_{\ell j}$ so the equations are satisfied, we get from Equation 3 that for arbitrary $t_{ij}, t_h \in R$

$$\prod_{\ell=1}^{L} E(a_\ell, d_\ell) \cdot E(t_1, v)^{-1} = \prod_{j=1}^{J} E(\psi_j, v_j),$$

where

$$\psi_j = \prod_{i=1}^{I} u_i^{\sum_{h=1}^{H} t_h\eta_{hij}} \cdot \prod_{\ell=1}^{L} a_\ell^{s_{\ell j}}.$$

We have the following corollary to Lemma 13.

Lemma 19 *If $v \in V$, $a_1, \ldots, a_L \in U$ and $\eta_1, \ldots, \eta_H$ generates the kernel of E, then for any witness $\theta_\ell, s_{\ell j}$ we get the same distribution of proofs ψ_j.*

Instantiation 2: XDH and SXDH. In the special case, where we are just looking at a multi-exponentiation of constants, we do not need u_1, u_2. The witness is θ_ℓ, s_ℓ so

$$d_\ell = v^{\theta_\ell}v_1^{s_\ell} \qquad \text{and} \qquad \prod_{\ell=1}^{L} a_\ell^{\theta_\ell} = t.$$

We construct a proof as

$$\psi := \prod_{\ell=1}^{L} a_\ell^{s_\ell}.$$

The verifier accepts if and only if

$$\prod_{\ell=1}^{L} E_4((1, a_\ell), d_\ell) = E_4((1,t), v)E_4(\psi, v_1).$$

Lemma 20 *The proof has perfect completeness, perfect soundness, and assuming the DDH problem is hard in G_2 we have composable witness indistinguishability. The size of the proof is 2 elements from G_1.*

Proof. Perfect completeness follows by inspection. Perfect witness-indistinguishability on a simulated reference string follows from Lemma 13. To argue perfect soundness, notice that v, v_1 being independent implies that d_q defines a unique $\theta_\ell \in \mathbb{Z}_{\mathbf{p}}$. We have $E_4((1, \prod_{\ell=1}^{L} a_\ell^{\theta_\ell} \cdot t^{-1}), v) \in E_4(G_1^2, v_1)$. This is only possible if $\prod_{\ell=1}^{L} a_\ell^{\theta_\ell} = t$. □

Instantiation 3: DLIN. We have a common reference string with u, u_1, u_2 so u is linearly independent of u_1, u_2. the witness is $\theta_\ell, s_{\ell 1}, s_{\ell 2}$ so

$$d_\ell = u^{\theta_\ell} u_1^{\ell s_{\ell 1}} u_2^{\ell 2} \qquad , \qquad \prod_{\ell=1}^{\theta_\ell} = t.$$

The proof is

$$\pi_1 := \prod_{\ell=1}^{L} (1, 1, a_\ell)^{s_{\ell 1}} \qquad , \qquad \pi_2 := \prod_{\ell=1}^{L} (1, 1, a_\ell)^{s_{\ell 2}}.$$

The verifier checks that

$$\prod_{\ell=1}^{L} E_9((1, 1, a_\ell), d_\ell) = E_9((1, 1, t_1), u) E_9(\pi_1, u_1) E_9(\pi_2, u_2).$$

Observe, only the last entries in π_1, π_2 are non-trivial, so the proof consists of 2 group elements.

Lemma 21 *The proof has perfect completeness, perfect soundness and assuming the DLIN problem is hard it has composable witness indistinguishability. The proof consists of 2 group elements.*

Proof. Perfect completeness can be verified directly. Perfect witness-indistinguishability follows from Lemma 13 on simulation reference string where u is linearly dependent on u_1, u_2. To argue perfect soundness, observe that $u, u_1 = (f, 1, g), u_2 = (1, h, g)$ being independent implies that d_ℓ defines θ_ℓ uniquely. We have $E_9(\prod_{\ell=1}^{L} (1, 1, a_\ell)^{\theta_\ell} (1, 1, t)^{-1}, u) \in E_9((f, 1, g), G^3) E_9((1, h, g), G^3)$. Write $u = (1, 1, g)^{\delta} (f, 1, g)^{\delta_1} (1, h, g)^{\delta_2}$ for $\delta \in \mathbb{Z}_{\mathbf{p}}^*$, to see that this implies $\prod_{\ell=1}^{L} a_\ell^{\theta_\ell} = t$. □

9 Witness-indistinguishable Proofs

We will now present the witness-indistinguishable proof for equations over modules. The setup consists of R-modules M_1, M_2, M_T and a bilinear map $E : M_1 \times M_2 \to M_T$. We have a commitment scheme that we can use to commit to elements in M_1 and M_2 given by elements $u_1, \ldots, u_I \in M_1, v_1, \ldots, v_J \in M_2$. We also have elements $u, u'_1, \ldots, u'_{I'} \in M_1, v, v'_1, \ldots, v'_{J'} \in M_2$, which gives us a commitment scheme for the ring elements. For all relevant combinations of these elements, which may or may not have some overlap, we also have generators $\eta_1, \ldots, \eta_H$ for the kernels of the corresponding maps μ.

Consider a set of equations over variables $x_1, \ldots, x_M \in M_1, y_1, \ldots, y_N \in M_2, \phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L \in R$. We have the following witness-indistinguishable protocol that takes as input the common reference string and a witness for simultaneous satisfiability of all equations.

1. Commit to all variables. Pick $r_{mi}, s_{nj}, \rho_{ki}, \sigma_{\ell j} \in R$ at random and set

$$c_m := x_m \prod_{i=1}^{I} u_i^{r_{mi}} \ , \ d_n := y_n \prod_{j=1}^{J} v_j^{s_{nj}} \ , \ c'_k := u^{\phi_k} \prod_{i=1}^{I'} (u'_i)^{\rho_{ki}} \ , \ d'_\ell := v^{\theta_\ell} \prod_{j=1}^{J'} (v'_j)^{\sigma_{\ell j}}.$$

2. For each pairing product equation make a proof as described in Section 5. This costs I elements in M_2 and J elements in M_1 for each pairing product equation.

3. For each multi-exponentiation relationship in M_1 make a proof as described in Section 7. This costs J' elements from M_1 and I elements from M_2.

4. For each multi-exponentiation relationship in M_2 make a proof as described in Section 7. This costs J elements from M_1 and I' elements from M_2.

5. For each general arithmetic gate, make a NIWI proof as described in Section 6. Each proof consists of J' elements from M_1 and I' elements from M_2.

NIWI proofs for bilinear groups. The overarching goal of this paper is to obtain non-interactive witness-indistinguishable proofs for equations over groups with a bilinear map. We now have the following method to construct such proofs.

1. Embed the bilinear groups into appropriately chosen modules with a bilinear map.

2. Express group elements and equations as elements and equations in the modules.

3. Use the witness-indistinguishable proof described above.

Instantiation 1: Subgroup decision. Given an order $\mathbf{p}$ subgroup of the composite order group $(\mathbf{n}, G, G_T, e, g, g_{\mathbf{q}}) \leftarrow \mathcal{G}(1^k)$, we will set up the witness-indistinguishable proof as follows.

CRS generation: Choose $h = g_{\mathbf{q}}^r$ for $r \leftarrow \mathbb{Z}_{\mathbf{n}}^*$. The CRS is $\sigma := (\mathbf{n}, G, G_T, e, g, h)$.

Simulated CRS generation: Choose $h = g^r$ for $r \leftarrow \mathbb{Z}_{\mathbf{n}}^*$. The simulated CRS is $\sigma := (\mathbf{n}, G, G_T, e, g, h)$.

Proof: Given a witness on the form $x_m \in G, \phi_k \in \mathbb{Z}_{\mathbf{n}}$[4], we can pick randomizers r_m, ρ_k and commit to them as $c_m := x_m h^{r_m}$ and $c'_k := g^{\phi_k} h^{\rho_k}$. For each type of equation, we now make a witness-indistinguishable proof as described in the previous sections.

Verification: Check the proof for each equation.

Theorem 22 *The proof has perfect completeness, perfect soundness with respect to the order* $\mathbf{p}$ *subgroups, and assuming the subgroup decision problem is hard it has composable witness indistinguishability. The size of the proof can be found by adding the costs of variables and equations found in Figure 4.*

Proof. Lemmas 2, 6, 10 prove this theorem. □

	Subgroup Decision	DLIN	DLIN one-sided
Variable x_m (equal to y_m)	1	3	3
Variable ϕ_k (equal to θ_k)	1	3	3
Pairing product equation	1	9	3
Multi-exponentiation	1	9	2
General arithmetic gate	1	6	2

Figure 4: Cost of each variable and equation measured in group elements from G.

[4]Since this is the symmetric setting, we do not need to separate the variables into x_m, y_n and ϕ_k, θ_ℓ.

Instantiation 2: XDH and SXDH. Given $(\mathbf{p}, G_1, G_2, G_T, e, g_1, g_2) \leftarrow \mathcal{G}(1^k)$, we will set up the witness-indistinguishable proof as follows.

CRS generation: We choose $x_1, x_2, y_1, y_2, r, s \leftarrow \mathbb{Z}_{\mathbf{p}}^*$ and $t_1, t_2 \leftarrow \mathbb{Z}_{\mathbf{p}}$. We set $u_1 := (g_1, g_1^{x_1}), u_2 := u_1^r$ and $u := u_1^{t_1}(1, g_1)^{y_1}$. We set $v_1 := (g_2, g_2^{x_2}), v_2 := v_1^s$ and $v := v_1^{t_2}(1, g_2)^{y_2}$. This way, we have u_1, u_2 are linearly dependent and independent from $(1, g_1)$, while u, u_1 are linearly independent. Similarly, we have v_1, v_2 being linearly dependent and both independent from $(1, g_2)$, while v, v_1 are linearly independent. Set $\sigma := (\mathbf{p}, G_1, G_2, G_T, e, g_1, g_2, u_1, u_2, u, v_1, v_2, v)$.

Simulated CRS generation: We choose $x_1, x_2, y_1, y_2, r, s \leftarrow \mathbb{Z}_{\mathbf{p}}^*$ and $t_1, t_2 \leftarrow \mathbb{Z}_{\mathbf{p}}$. We set $u_1 := (g_1, g_1^{x_1}), u := u_1^r$ and $u_1 := u_1^{t_1}(1, g_1)^{y_1}$. We set $v_1 := (g_2, g_2^{x_2}), v := v_1^s$ and $v_2 := v_1^{t_2}(1, g_2)^{y_2}$. This way, we have u_1, u_2 are linearly independent, while u, u_1 are linearly dependent. Similarly, we have v_1, v_2 being linearly independent, while v, v_1 are linearly dependent. Set $\sigma := (\mathbf{p}, G_1, G_2, G_T, e, g_1, g_2, u_1, u_2, u, v_1, v_2, v)$

Proof: We have a witness $x_m \in G_1, y_n \in G_2, \phi_k, \theta_\ell \in \mathbb{Z}_{\mathbf{p}}$. We pick randomizers $r_{mi}, s_{nj}, \rho_k, \sigma_\ell \leftarrow \mathbb{Z}_{\mathbf{p}}$ and commit to the witness as $c_k := (1, x_m)u_1^{r_{m1}}u_2^{r_{m2}}, d_k := (1, y_n)v_1^{s_{n1}}v_2^{s_{n2}}, c'_k := u^{\phi_k}u_1^{\rho_k}, d'_k := v^{\theta_\ell}v_1^{\sigma_\ell}$. For each equation, we make a witness indistinguishable proof as described in the previous sections.

Verification: Check the proof for each equation.

Theorem 23 *The proof has perfect completeness, perfect soundness, and assuming the SXDH problem is hard it has composable witness indistinguishability. The size of the proof can be found by adding the costs in Figure 5.*

Proof. Lemmas 3, 7, 11 prove this theorem. □

	SXDH		XDH (one-sided)	
	G_1	G_2	G_1	G_2
Variable x_m	2	0	2	0
Variable y_n	0	2	N/A	N/A
Variable ϕ_k	2	0	2	0
Variable θ_ℓ	0	2	N/A	N/A
Pairing product equation	4	4	0	2
Multi-exponentiation in G_1	2	4	N/A	N/A
Multi-exponentiation in G_2	4	2	0	2
General arithmetic gate	2	2	0	1

Figure 5: Cost of each variable and equation measured in group elements from G_1 and G_2.

Instantiation 3: DLIN. We have a group with a bilinear map $(\mathbf{p}, G, G_T, e, g) \leftarrow \mathcal{G}(1^k)$. We set up the proof as follows.

CRS generation: Pick $\alpha, \beta, t \leftarrow \mathbb{Z}_{\mathbf{p}}^*$ and $r_3, s_3, r, s \leftarrow \mathbb{Z}_{\mathbf{p}}$. Set $f := g^\alpha, h := g^\beta$. We set $u_1 := (f, 1, g), u_2 := (1, h, g), u_3 := u_1^{r_3}u_2^{s_3}, u := u_1^r u_2^s (1, 1, g)^t$. This way we have u_1, u_2, u_3 being linearly independent of $(1, 1, g)$ and u. Set $\sigma := (\mathbf{p}, G, G_T, e, g, u_1, u_2, u_3, u)$.

Simulated CRS generation: Pick $\alpha, \beta, t \leftarrow \mathbb{Z}_{\mathbf{p}}^*$ and $r_3, s_3, r, s \leftarrow \mathbb{Z}_{\mathbf{p}}$. Set $f := g^\alpha, h := g^\beta$. We set $u_1 := (f, 1, g), u_2 := (1, h, g), u_3 := u_1^{r_3}u_2^{s_3}(1, 1, g)^t, u := u_1^r u_2^s$. This way we have u_1, u_2, u_3 being linearly independent, and $u \in U$. Set $\sigma := (\mathbf{p}, G, G_T, e, g, u_1, u_2, u_3, u)$.

Proof: We have a witness $x_m \in G, \phi_k \in \mathbb{Z}_{\mathbf{p}}$ satisfying a set of equations. We pick randomizers $r_{m1}, r_{m2}, r_{m3}, \rho_{k1}, \rho_{k2} \leftarrow \mathbb{Z}_{\mathbf{p}*}$ and commit to the witness as $c_k := (1, 1, x_m) \prod_{i=1}^{3} u_i^{r_{mi}}$ and $d_k := u^{\phi_k} \prod_{i=1}^{2} u_i^{\rho_{ki}}$. For each equation, we make a proof as described in the previous sections.

Verification: Verify the proof for each equation.

Theorem 24 *The proof has perfect completeness, perfect soundness and assuming the DLIN problem is hard it has composable witness indistinguishability. The increase in proof size that each variable and equation costs is given in Figure 4.*

Proof. Lemmas 4, 8, 12 prove this theorem. □

For comparison, we also list the cost of the general protocol in Figure 6 both for the general case, where $M_1 \neq M_2$, and the symmetric case where $M_1 = M_2$ and E is symmetric. The figure also contains the price to pay in case the equation is one-sided, in which case savings may be obtained.

	Asymmetric		Symmetric	One-sided	
	M_1	M_2	$M_1 = M_2$	M_1	M_2
Variable x_m	1	0	1	1	0
Variable y_n	0	1	1	N/A	N/A
Variable ϕ_k	1	0	1	1	0
Variable θ_ℓ	0	1	1	N/A	N/A
Pairing product equation	J	I	I	0	I
Multi-exponentiation in M_1	I	J'	I	N/A	N/A
Multi-exponentiation in M_2	I'	J	I	0	I'
General arithmetic gate	J'	I'	I'	0	I'

Figure 6: Cost of each variable and equation measured in elements from M_1 and M_2.

10 Non-interactive Zero-Knowledge Proofs

We have presented some very efficient NIWI proofs for sets of equations over bilinear groups. In this section, we will show that in many cases our techniques can also be used to construct efficient NIZK proofs.

Suppose we have a set of equations over variables $x_1, \ldots, x_M \in G_1, y_1, \ldots, y_N \in G_2, \phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L \in R$ and we want to prove a set of equations are simultaneously satisfiable. An obvious strategy would be to use the witness and make a NIWI proof that the equations are satisfiable. There is also an obvious problem with this strategy, the simulator does not know a witness and therefore it cannot simulate a proof.

It turns out that the strategy is better than it seems at first glance. In the NIWI proof we have described, we make a proof for each single equation by itself and each individual proof is witness-indistinguishable. In the simulation, the commitments are perfectly hiding and therefore we may imagine using trapdoor commitments and opening the commitments to different exponents for each equation and witness-indistinguishable proof. In particular, to commit to an exponent ϕ, we compute $c := u^{\phi} \prod_{i=1}^{I} u_i^{r_i}$. If we know a linear relation $\xi_1, \ldots, \xi_I$ so $u = \prod_{i=1}^{i} u_i^{\xi_i}$, we can open it to any given message ϕ' as $c := u^{\phi'} \prod_{i=1}^{I} u_i^{r_i + \xi_i(\phi - \phi')}$. We define a NIWI proof to be *individual* composable witness-indistinguishable, if it is composable witness-indistinguishable, the simulation reference string sets up perfect hiding commitments to the group elements

and perfect trapdoor commitments for the exponents and each equation gets it own witness-indistinguishable proof.

We call a set S of equations over variables $x_1, \ldots, x_M \in G_1, y_1, \ldots, y_N \in G_2, \phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L \in R$ *tractable* if it is possible to deterministically[5] compute a satisfiability witness for each individual equation, such that all witness use the same $x_1, \ldots, x_M, y_1, \ldots, y_N$, but may vary $\phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L$ freely from equation to equation.

Theorem 25 *For a set of tractable equations over bilinear groups $(\mathbf{n}, G_1, G_2, G_T, e, g_1, g_2)$ with an individual composable witness-indistinguishable proof, there is a composable zero-knowledge simulator.*

Proof. The simulator S_1 creates a simulated reference string and outputs also the trapdoors for the commitment schemes used to commit to the exponents.

The simulator S_2 gets the tractable set of equations and computes a satisfiability witness w such that $x_1, \ldots, x_M, y_1, \ldots, y_M$ are the same in each equation, while $\phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L$ may vary from equation to equation. It commits to $x_1, \ldots, x_M, y_1, \ldots, y_M$, while making trapdoor commitments $c_1, \ldots, c_K, d_1, \ldots, d_L$ to the exponents. For each equation, it opens the trapdoor commitments to get satisfying $x_1, \ldots, x_M, y_1, \ldots, y_N, \phi_1, \ldots, \phi_K, \theta_1, \ldots, \theta_L$ and makes a witness-indistinguishable proof.

We will now prove that on a simulation reference string, we have perfect zero-knowledge. We are given a witness for simultaneous satisfiability of all equations and have to show that on a simulation reference string, it is perfectly indistinguishable whether we create a proof using the witness or we use the simulator to create the proof. Consider the following hybrid experiment, where we run the simulator to generate the commitments but then open all the commitments (using brute force) to the witness and make real witness-indistinguishable proofs for each equation. Since each individual proof is perfectly witness-indistinguishable, this is perfectly indistinguishable from the simulation. On the other hand, since each commitment is perfectly hiding the hybrid experiment is also perfectly indistinguishable from running the real prover on a simulated reference string. □

Corollary 26 *Tractable equations in the subgroup decision, SXDH and DLIN cases described in this paper have composable zero-knowledge proofs with perfect completeness and perfect soundness, computational indistinguishability between real common reference strings and simulated reference strings, and perfect zero-knowledge on simulated reference strings.*

Making sets of equations tractable. There is a technique to make sets of equations tractable. We introduce some extra variables, among them $\phi, \theta \in R$. We will also introduce some extra equations, among them $\phi = 0, \theta = 0$. Note, we can commit to them as $c := 1, d := 1$, so there is no extra cost here.

Let us start with the general arithmetic gate. We can modify it to

$$\phi \cdot 1 + \sum_{k=1}^{K} \alpha_k \phi_k \ + \ \sum_{\ell=1}^{L} \beta_\ell \theta_\ell \ + \ \sum_{k=1}^{K} \sum_{\ell=1}^{L} \gamma_{k\ell} \phi_k \theta_\ell \ = \ \tau,$$

for constants $\alpha_k, \beta_\ell, \gamma_{k\ell}, \tau \in \mathbb{Z}_{\mathbf{n}}$. Since ϕ can be opened to anything, it is now easy to see that we can satisfy any individual general arithmetic gate equation. Since the proof size is independent of the number of variables, this modification costs nothing.

For a multi-exponentiation equation in G_1, we can introduce an extra variable $z \in G_1$ and use

$$\prod_{\ell=1}^{L} a_\ell^{\theta_\ell} \cdot \prod_{m=1}^{M} x_m^{\sum_{\ell=1}^{L} \alpha_{m\ell}\theta_\ell + \beta_m} \cdot t_1^{-1} = z^{\theta},$$

[5] We define tractability in terms of a deterministic witness-computing algorithm because we want it to be possible to check directly whether a set of equations is tractable or not.

for constants $a_\ell, t_1 \in G_1$ and $\alpha_{m\ell}, \beta_m \in \mathbb{Z}_{\mathbf{n}}$. For this equation we can use $\theta = 1$ and just set z to be the product given in the equation, so the equation is now trivially satisfiable. Multi-exponentiation equations in G_2 work similarly.

The most complicated type of equation to make tractable is the pairing product equation. The problem is that it may be hard to compute group elements $a'_1, b'_1, \ldots, a'_\Omega, b'_\Omega$ so $\prod_{\omega=1}^{\Omega} e(a'_\omega, b'_\omega) = T$. However, assume T is on a form such that this is possible, then we can move this part to the other side of the equation. This reduces the problem to the case $T = 1$.

We introduce variables $z_1, \ldots, z_Q$ and rewrite the pairing product equation as

$$\prod_{q=1}^{Q} e(z_q, b_q \prod_{n=1}^{N} y_n^{\beta_{qn}}) = 1 \quad , \quad z_q = (a_q \prod_{m=1}^{M} x_m^{\alpha_{qm}})^{1-\theta},$$

which is solvable by picking $z_1 = \cdots = z_Q = 1$ and $\theta = 1$.

The case of pairing product equations point to a fundamental difference between witness-indistinguishable proofs and zero-knowledge proofs using our techniques. NIWI proofs can handle any target T, whereas zero-knowledge proofs can only handle special types of target T. Second, even if $T = 1$ it seems like in the most general case the cost is linear in Q for pairing product equations, whereas in the NIWI proofs the cost of such an equation is constant.

11 Conclusion and an Open Problem

Our main contribution in this paper is the construction of efficient non-interactive cryptographic proofs for use in bilinear groups. Our proofs can be instantiated with many different types of bilinear groups and the security of our proofs can be based on many different types of intractability assumptions, of which we have given three instantiations: the subgroup decision assumption, the SXDH assumption and the DLIN assumption.

Since we have been interested in bilinear groups we have in our instantiations based the modules on bilinear groups. It is possible that other types of modules with a bilinear map exist, which are not constructed from bilinear groups. The existence of such modules might lead to efficient NIWI and NIZK proofs based on entirely different intractability assumptions. We leave the construction of such modules with a bilinear map as an interesting open problem.

Acknowledgements

We gratefully acknowledge Brent Waters for a number of helpful ideas, comments, and conversations related to this work. In particular, our module-based approach can be seen as formalizing part of the intuition expressed by Waters that the Decisional Linear Assumption, Subgroup Decision Assumption in composite-order groups, and XDH can typically be exchanged for one another. (We were inspired by previously such connections made by [GOS06a, Wat06].) It would be interesting to see if this intuition can be made formal in other settings, such as Traitor Tracing [BSW06] or Searchable Encryption [BW06]. We also thank Dan Boneh for his encouragement and for suggesting using our techniques to get fair exchange.

References

[Bar06] Paulo Barreto. The pairing-based crypto lounge, 2006. Available at `http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html`.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *proceedings of CRYPTO '04, LNCS series, volume 3152*, pages 41–55, 2004.

[BCOP04] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *proceedings of EUROCRYPT '04, LNCS series, volume 3027*, pages 506–522, 2004.

[BF03] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *proceedings of STOC '88*, pages 103–112, 1988.

[BGdMM05] Lucas Ballard, Matthew Green, Breno de Medeiros, and Fabian Monrose. Correlation-resistant storage via keyword-searchable encryption. Cryptology ePrint Archive, Report 2005/417, 2005. Available at `http://eprint.iacr.org/2005/417`.

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-dnf formulas on ciphertexts. In *proceedings of TCC '05, LNCS series, volume 3378*, pages 325–341, 2005.

[Bon06] Dan Boneh. Personal communication, 2006.

[BSW06] Dan Boneh, Amit Sahai, and Brent Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In *proceedings of EUROCRYPT '06, LNCS series, volume 4004*, pages 573–592, 2006.

[BW06] Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In *proceedings of EUROCRYPT '06, LNCS series, volume 4004*, pages 427–444, 2006.

[BW07] Xavier Boyen and Brent Waters. Full-domain subgroup hiding and constant-size group signatures. In *proceedings of PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 1–15, 2007. Available at `http://www.cs.stanford.edu/~xb/pkc07/`.

[CGS07] Nishant Chandran, Jens Groth, and Amit Sahai. Ring signatures of sub-linear size without random oracles. To appear at ICALP 2007, 2007.

[Dam92] Ivan Damgård. Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with proprocessing. In *proceedings of EUROCRYPT '92, LNCS series, volume 658*, pages 341–355, 1992.

[DBS04] Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptographic protocols : A survey. Cryptology ePrint Archive, Report 2004/064, 2004. `http://eprint.iacr.org/`.

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. *SIAM Journal of Computing*, 30(2):391–437, 2000.

[DDP02] Alfredo De Santis, Giovanni Di Crescenzo, and Giuseppe Persiano. Randomness-optimal characterization of two np proof systems. In *proceedings of RANDOM '02, LNCS series, volume 2483*, pages 179–193, 2002.

[FLS99] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple non-interactive zero knowledge proofs under general assumptions. *SIAM Journal of Computing*, 29(1):1–28, 1999.

[GL07] Jens Groth and Steve Lu. Non-interactive proofs for the correctness of a shuffle. Work in progress, 2007.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proofs. *SIAM Journal of Computing*, 18(1):186–208, 1989. First published at STOC 1985.

[GOS06a] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for nizk. In *proceedings of CRYPTO '06, LNCS series, volume 4117*, pages 97–111, 2006.

[GOS06b] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero-knowledge for np. In *proceedings of EUROCRYPT '06, LNCS series, volume 4004*, pages 339–358, 2006.

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM CCS '06*, pages 89–98, 2006.

[GR04] Steven D. Galbraith and Victor Rotger. Easy decision diffie-hellman groups. *London Mathematical Society Journal of Computation and Mathematics*, 7:201–218, 2004.

[Gro06] Jens Groth. Simulation-sound nizk proofs for a practical language and constant size group signatures. In *proceedings of ASIACRYPT '06, LNCS series*, 2006. Full paper available at `http://www.brics.dk/~jg/NIZKGroupSignFull.pdf`.

[KP98] Joe Kilian and Erez Petrank. An efficient noninteractive zero-knowledge proof system for np with general assumptions. *Journal of Cryptology*, 11(1):1–27, 1998.

[Mic03] Silvio Micali. Simple and fast optimistic protocols for fair electronic exchange. In *PODC*, pages 12–19, 2003.

[Sco02] Mike Scott. Authenticated id-based key exchange and remote log-in with simple token and pin number. Cryptology ePrint Archive, Report 2002/164, 2002. Available at `http://eprint.iacr.org/2002/164`.

[SW05] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *proceedings of EUROCRYPT '05, LNCS series, volume 3494*, pages 457–473, 2005.

[Ver04] Eric R. Verheul. Evidence that xtr is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology*, 17(4):277–296, 2004.

[Wat05] Brent Waters. Efficient identity-based encryption without random oracles. In *proceedings of EUROCRYPT '05*, pages 114–127, 2005.

[Wat06] Brent Waters. New techniques for slightly 2-homomorphic encryption, 2006. Manuscript.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/