Switching Lemma for Bilinear Tests and Constant-size NIZK Proofs for Linear Subspaces

Charanjit S. Jutla[1] and Arnab Roy[2]

[1] IBM T. J. Watson Research Center, Yorktown Heights, NY 10598, USA
[2] Fujitsu Laboratories of America, Sunnyvale, CA 94085, USA

Abstract. We state a switching lemma for tests on adversarial responses involving bilinear pairings in hard groups, where the tester can effectively switch the randomness used in the test from being given to the adversary at the outset to being chosen after the adversary commits its response. The switching lemma can be based on any k-linear hardness assumptions on one of the groups. In particular, this enables convenient information theoretic arguments in the construction of sequence of games proving security of cryptographic schemes, mimicking proofs and constructions in the random oracle model.
As an immediate application, we show that the computationally-sound quasi-adaptive NIZK proofs for linear subspaces that were recently introduced [JR13b] can be further shortened to *constant*-size proofs, independent of the number of witnesses and equations. In particular, under the XDH assumption, a length n vector of group elements can be proven to belong to a subspace of rank t with a quasi-adaptive NIZK proof consisting of just a single group element. Similar quasi-adaptive aggregation of proofs is also shown for Groth-Sahai NIZK proofs of linear multi-scalar multiplication equations, as well as linear pairing-product equations (equations without any quadratic terms).

Keywords: NIZK, bilinear pairings, quasi-adaptive, Groth-Sahai, Random Oracle, IBE, CCA2.

1 Introduction

Testing pairing equations in bilinear groups is a fundamental component of numerous cryptographic schemes spanning public key encryption schemes, signatures, zero knowledge proofs and so on. We state and prove a *switching lemma* for testing pairing equations in bilinear groups, where an adversary is given some random group elements from one of the groups, and the pairing test (of equality and/or inequality) is performed on adversary's output and the same random group elements. We show that the tester can replace the random group elements in the test with a new set of fresh random group elements, effectively mimicking the behavior of a random oracle. This switching lemma can be based on any k-linear hardness assumptions on one of the groups. This not only enables convenient information theoretic arguments in the construction of sequence of

games proving security of cryptographic schemes, but also allows more efficient protocols reminiscent of the Fiat-Shamir paradigm using random oracles [FS86].

Fiat-Shamir paradigm is best illustrated by the conversion of 3-round sigma protocol [Dam] for proof of knowledge (PoK) of discrete logarithms to a random oracle based NIZK. Consider an example where the prover is trying to prove possession of the discrete logarithm x of a public value g^x. In the first round the prover commits to a random value r by sending g^r. In response, the verifier generates a fresh random value c and sends to the prover. The prover then responds with $r + cx$. This constitutes an honest verifier zero-knowledge PoK. In transforming this to a NIZK, a public random oracle H is used and the prover just transmits $(g^r, r + H(g^r, g^x) \cdot x)$. Essentially the random oracle induces the effect of a 'fresh' randomness that can be used for verification and is not under any effective control of the prover. In this paper we create an analogous effect in the standard model using the hardness of k-linear problems (such as DDH and DLIN) in bilinear groups. We show that even if the random testing values are public and hence known to the prover, during verification one can switch to freshly generated testing values with negligible change in the probability of success of the verification.

As an immediate application, we show that the computationally-sound quasi-adaptive NIZK (QA-NIZK) proofs for linear subspaces that we recently introduced in [JR13b] can be further shortened to *constant*-size proofs, independent of the number of variables and equations. In [JR13b], it was shown that for languages that are linear subspaces of vector spaces of the bilinear groups, one can obtain more efficient computationally-sound NIZK proofs compared to [GS08] in a slightly different *quasi-adaptive* setting, which suffices for many cryptographic applications. In the quasi-adaptive setting, a class of parametrized languages $\{L_\rho\}$ is considered, parametrized by ρ, and the CRS generator is allowed to generate the CRS based on the language parameter ρ. However, the CRS simulator in the zero-knowledge setting is required to be a single efficient algorithm that works for the whole parametrized class or probability distributions of languages, by taking the parameter as input. This property was referred to as *uniform simulation*.

The main idea underlying the construction in [JR13b] can be summarized as follows. Consider the language L_ρ (over a cyclic group $\mathbb{G}$ of order q, in additive notation) defined as

$$L_\rho = \left\{ \langle \boldsymbol{l}_1, \boldsymbol{l}_2, \boldsymbol{l}_3 \rangle \in \mathbb{G}^3 \mid \exists x_1, x_2 \in \mathbb{Z}_q : \ \boldsymbol{l}_1 = x_1 \cdot \mathbf{g},\ \boldsymbol{l}_2 = x_2 \cdot \mathbf{f},\ \boldsymbol{l}_3 = (x_1 + x_2) \cdot \mathbf{h} \right\}$$

where $\rho \stackrel{\text{def}}{=} (\mathbf{g}, \mathbf{f}, \mathbf{h})$ is the parameter defining the language. Suppose that the CRS can be set to be a basis for the null-space $L_\rho^\perp$ of the language L_ρ. Then, just pairing a potential language candidate with $L_\rho^\perp$ and testing for all-zero suffices to prove that the candidate is in L_ρ, as the null-space of $L_\rho^\perp$ is just L_ρ. However, efficiently computing null-spaces in hard bilinear groups is itself hard. Thus, an efficient CRS simulator cannot generate $L_\rho^\perp$. However, it was shown that it suffices to give as CRS a (hiding) commitment that is computationally indistinguishable from a binding commitment to $L_\rho^\perp$.

Our contributions. Utilizing the switching lemma, for n equations in t variables, our computationally-sound quasi-adaptive NIZK proofs for linear subspaces require only k group elements under the k-linear decisional assumption [HK07,Sha07]. Thus, under the XDH[3] assumption for bilinear groups, our proofs require only *one* group element. In contrast, the Groth-Sahai system requires $(n + 2t)$ group elements and our previous system required $(n - t)$ group elements. Similarly, under the decisional linear assumption (DLIN), our proofs require only 2 group elements, whereas the Groth-Sahai system requires $(2n+3t)$ group elements and our previous system required $(2n-2t)$ group elements. These parameters are summarized in Table 1. While our CRS size grows linearly with n, the number of pairing operations is competitive and could be significantly less compared to earlier schemes for appropriate n and t.

Note that Schnorr proofs of multiple equations in the random oracle model can also be combined into a proof consisting of only two group elements (by taking random linear combinations employing the random oracle), but it still requires commitments to all the variables. Thus, our proofs are even shorter than Schnorr proofs. On the other hand, Schnorr proofs are proof of knowledge (as opposed to ours or Groth-Sahai), and can be somewhat faster to verify as they only use exponentiation instead of pairings. We also show that proofs of multiple

Table 1. Comparison with Groth-Sahai, Jutla-Roy (2013) and Schnorr-NIZKs for Linear Subspaces. Parameter t is the number of unknowns and n is the dimension of the vector space, i.e. the number of equations. *See text for recent independent work.*

	XDH			DLIN		
	Proof	CRS	#Pairings	Proof	CRS	#Pairings
Groth-Sahai	$n + 2t$	4	$2n(t + 2)$	$2n + 3t$	9	$3n(t + 3)$
Jutla-Roy '13	$n - t$	$2t(n - t) + 2$	$(n - t)(t + 2)$	$2n - 2t$	$4t(n - t) + 3$	$2(n - t)(t + 2)$
Schnorr (RO)	$t + 2$	–	–	–	–	–
This paper	1	$n + t + 1$	$n + 1$	2	$2(n + t + 2)$	$2(n + 2)$

linear scalar-multiplication equations, as well as multiple *linear* pairing product equations (i.e. without any quadratic terms) can be aggregated into a single proof in the Groth-Sahai system. This can lead to significant shortening of proofs of multiple linear pairing product equations. The comparisons are tabulated in Table 2. We remark that this is in contrast to the batching of Groth-Sahai proof verification [BFI+10], where the proofs were not aggregated, but multiple pairing equations were batched together during the verification step. We can use similar batching techniques to improve the verification step; therefore, we skip taking these optimizations into consideration. A recent work [LPJY14] has also obtained constant-size QA-NIZK proofs under DLIN (but not under XDH). While our proofs are marginally shorter (2 against 3 in DLIN), they additionally show constant-size unbounded simulation-sound QA-NIZK proofs.

[3] XDH is the assumption that DDH is hard in one of the pairing groups. Also note that DDH is same as the k-linear assumption for $k = 1$.

Table 2. Comparison with (1) Groth-Sahai for n number of linear Scalar Multiplication Equations: $\vec{y} \cdot \vec{\mathbf{a}}_j + \vec{b}_j \cdot \vec{\mathbf{x}} = \mathbf{u}_j$, with $j \in [1, n]$, $\vec{y} \in {\mathbb{Z}_q}^s, \vec{\mathbf{x}} \in \mathbb{G}^t$ and $\mathbf{u}_j \in \mathbb{G}$. and (2) Groth-Sahai for n number of linear Pairing Product Equations: $e(\vec{\mathbf{y}}, \vec{\mathbf{a}}_j) + e(\vec{\mathbf{b}}_j, \vec{\mathbf{x}}) = \mathbf{u}_j$, with $j \in [1, n]$, $\vec{\mathbf{y}} \in \mathbb{G}^s$, $\vec{\mathbf{x}} \in \mathbb{G}^t$ and $\mathbf{u}_j \in \mathbb{G}_T$.

	DLIN Linear Multi-Scalar and Linear Pairing-Product		
	Proof	CRS	#Pairings
Groth-Sahai	$3(s+t)+9n$	9	$9n(s+t+3)+n$
This paper	$3(s+t)+18$	$9+4n$	$18(s+t+3)+n$

While the cryptographic literature is replete with applications using NIZK proofs of algebraic languages over bilinear groups, and many examples were given in [JR13b] involving NIZK proofs of linear subspaces, we focus on two particular cases where aggregation of proofs of linear subspaces lead to interesting results. We consider a construction of [CCS09] to convert key-dependent message (KDM) CPA secure encryption scheme [BHHO08] into a KDM-CCA2 secure scheme which involved proving $O(N)$ linear equations, where N is the security parameter. With our aggregation of proofs, the size of this proof (in the quasi-adaptive setting) is reduced to just 2 group elements (under the DLIN assumption) from the earlier $O(N)$ sized quasi-adaptive proofs and Groth-Sahai proofs. It is also easy to see that the quasi-adaptive setting for proving the NIZK suffices, as is the case for most applications. As another application we reduce the size of the publicly-verifiable CCA2-IBE scheme obtained in [JR13b] by another group element to just five group elements plus a tag. This makes it shorter than the highly-optimized CCA2-IBE scheme obtained using the [CHK04] paradigm from hierarchical-IBE (HIBE) and in addition is publicly-verifiable.

Organization of the paper. We begin the rest of the paper with the switching lemma for bilinear tests in hard groups in Section 2. We recall the quasi-adaptive NIZK definitions in Section 3 and develop constant-size quasi-adaptive NIZKs for linear subspaces in Section 4. In Section 5, we apply our switching lemma to aggregate Groth-Sahai NIZKs. Finally, we provide application examples in Section 6. We defer detailed proofs, formal descriptions and a summary of standard hardness assumptions that we use to the full paper [JR13a].

2 Switching Lemma for Bilinear Tests in Hard Groups

Notations. Consider bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with pairing e to a target group $\mathbb{G}_T$, all of prime order q, and random generators $\mathbf{g}_1 \in \mathbb{G}_1$ and $\mathbf{g}_2 \in \mathbb{G}_2$. Let $\mathbf{0}_1, \mathbf{0}_2$ and $\mathbf{0}_T$ be the identity elements in the three groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ respectively. We will use additive notation for group operations, with $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ viewed as $\mathbb{Z}_q$-vector spaces. The scalar product by $\mathbb{Z}_q$ elements naturally extends to vectors and matrices of group elements. The pairing operation also naturally extends to vectors of elements (by summation) and correspondingly to matrices of elements. Column vectors will be denoted by an arrow over the letter, e.g. $\vec{\mathrm{r}}$

for (column) vector of $\mathbb{Z}_q$ elements, and $\vec{\mathbf{d}}$ as (column) vector of group elements. Thus, $e(\vec{\mathbf{f}}^\top, \vec{\mathbf{h}}) = \sum_i e(\mathbf{f}_i, \mathbf{h}_i)$.

Switching Lemma Usage Example. We demonstrate the usage of the Switching Lemma by way of a toy example. Suppose we are given three elements $\mathbf{g}, \mathbf{f}(= a \cdot \mathbf{g}), \mathbf{h}(= b \cdot \mathbf{g})$ in the group $\mathbb{G}_1$ and we need a proof system, not necessarily ZK, for tuples of the form $(x \cdot \mathbf{g}, x \cdot \mathbf{f}, x \cdot \mathbf{h})$. Towards that end, suppose the following CRS is published: $((ar_1 + br_2) \cdot \mathbf{g}_2, -r_1 \cdot \mathbf{g}_2, -r_2 \cdot \mathbf{g}_2)$. So the pairing test $e(x \cdot \mathbf{g}, (ar_1 + br_2) \cdot \mathbf{g}_2) + e(x \cdot \mathbf{f}, -r_1 \cdot \mathbf{g}_2) + e(x \cdot \mathbf{h}, -r_2 \cdot \mathbf{g}_2) = \mathbf{0}_T$, satisfies completeness, i.e., it holds for valid tuples.

However, how do we know that it is sound? A look at the pairing equation shows that there is a fair degree of freedom to satisfy it, without being a valid tuple. So we definitely have to resort to a computational hardness assumption to argue soundness. This is where we invoke the switching lemma, which is based on a hardness assumption. Thus even though we publish a CRS that uses r_1, r_2, during verification we can switch them with fresh r'_1, r'_2 chosen randomly and independently.

This means if a candidate tuple $(\boldsymbol{l}_1, \boldsymbol{l}_2, \boldsymbol{l}_3)$ satisfies the original test with a certain probability, then it also satisfies the switched test: $e(\boldsymbol{l}_1, (ar'_1 + br'_2) \cdot \mathbf{g}_2) + e(\boldsymbol{l}_2, -r'_1 \cdot \mathbf{g}_2) + e(\boldsymbol{l}_3, -r'_2 \cdot \mathbf{g}_2) = \mathbf{0}_T$ with almost the same probability. Rearranging, we get: $r'_1 \cdot e(a \cdot \boldsymbol{l}_1 - \boldsymbol{l}_2, \mathbf{g}_2) + r'_2 \cdot e(b \cdot \boldsymbol{l}_1 - \boldsymbol{l}_3, \mathbf{g}_2) = \mathbf{0}_T$. Now, observe that the r'_1, r'_2 were chosen *after* the tuple was given. So with high probability, both of $e(a \cdot \boldsymbol{l}_1 - \boldsymbol{l}_2, \mathbf{g}_2)$ and $e(b \cdot \boldsymbol{l}_1 - \boldsymbol{l}_3, \mathbf{g}_2)$ must be $\mathbf{0}_T$. Therefore, $\boldsymbol{l}_2 = a \cdot \boldsymbol{l}_1$ and $\boldsymbol{l}_3 = b \cdot \boldsymbol{l}_1$, thus proving soundness.

Another way to look at this is that we produced a single CRS by random linear combination of CRS'es to prove the individual languages $\{(x \cdot \mathbf{g}, x \cdot \mathbf{f}) \mid x \in \mathbb{Z}_q\}$ and $\{(x \cdot \mathbf{g}, x \cdot \mathbf{h}) \mid x \in \mathbb{Z}_q\}$. Since the combined CRS is given to the adversary, we cannot resort to information-theoretic arguments to separate the individual equations. However with the switching lemma in play, the separation follows.

Switching Lemma Intuition. First consider the asymmetric bilinear group setting, where DDH holds in each individual group, and there is no easy isomorphism from $\mathbb{G}_1$ to $\mathbb{G}_2$ and vice-versa. If an Adversary $\mathcal{A}$ is given two random group elements, say $\mathbf{r}_1, \mathbf{r}_2$, from $\mathbb{G}_2$, then one would like to claim that it is highly improbable for $\mathcal{A}$ to produce non-zero $\mathbf{f}_1, \mathbf{f}_2$ in $\mathbb{G}_1$ such that $e(\mathbf{f}_1, \mathbf{r}_1) + e(\mathbf{f}_2, \mathbf{r}_2) = \mathbf{0}_T$. First, note that if the groups were symmetric, then this is easy to achieve by setting $\mathbf{f}_1 = \mathbf{r}_2$ and $\mathbf{f}_2 = -\mathbf{r}_1$. But, since we are in the asymmetric setting, the improbability is proven under DDH holding for $\mathbb{G}_2$ as follows: We will show that an adversary $\mathcal{A}$ that can produce a non-zero $\mathbf{f}_1, \mathbf{f}_2$ satisfying the above pairing equation can be used to produce an adversary B that can break DDH. So, given a DDH challenge, $\mathbf{g}_2, x \cdot \mathbf{g}_2, y \cdot \mathbf{g}_2$ and $\mathbf{h}$ which is either $xy \cdot \mathbf{g}_2$ or $z \cdot \mathbf{g}_2$, adversary B passes $\mathbf{g}_2, x \cdot \mathbf{g}_2$ to $\mathcal{A}$ (note they are random and independent). Since $\mathcal{A}$ produces non-zero $\mathbf{f}_1, \mathbf{f}_2$ such that $e(\mathbf{f}_1, \mathbf{g}_2) + e(\mathbf{f}_2, x \cdot \mathbf{g}_2) = \mathbf{0}_T$, it follows that $\mathbf{f}_1 = -x \cdot \mathbf{f}_2$. Then comparing $e(\mathbf{f}_1, y \cdot \mathbf{g}_2)$ with $-e(\mathbf{f}_2, \mathbf{h})$ allows B to distinguish the two versions of $\mathbf{h}$.

Surprisingly, a similar claim holds when the adversary $\mathcal{A}$ is given an arbitrary long, say length n vector $\vec{\mathbf{r}}$ of random group elements from $\mathbb{G}_2$, and $\mathcal{A}$ is required to produce a length n vector $\vec{\mathbf{f}}$ (from $\mathbb{G}_1$) such that $e(\vec{\mathbf{f}}^{\top}, \vec{\mathbf{r}}) = \mathbf{0}_T$. This is proven using a hybrid argument, and for that purpose it is useful to restate the above claim of improbability as a switching lemma: *Given $\mathbf{r}_1, \mathbf{r}_2$, if an adversary has probability Δ success in producing non-zero $\mathbf{f}_1, \mathbf{f}_2$ such that $e(\mathbf{f}_1, \mathbf{r}_1) + e(\mathbf{f}_2, \mathbf{r}_2) = \mathbf{0}_T$, then the probability of $e(\mathbf{f}_1, \mathbf{r}'_1) + e(\mathbf{f}_2, \mathbf{r}'_2) = \mathbf{0}_T$ holding is also negligibly close to Δ, where $\mathbf{r}'_1, \mathbf{r}'_2$ are chosen after $\mathcal{A}$ commits $\mathbf{f}_1, \mathbf{f}_2$.*

Moving on to the symmetric bilinear groups, and assuming that the k-linear (commonly called DLIN for 2-linear) assumption holds for the groups, one can show that if $\mathcal{A}$ is now given k independent pairs of random group elements, then it is highly improbable for $\mathcal{A}$ to produce non-zero $\mathbf{f}_1, \mathbf{f}_2$ such that the above pairing test holds for all k pairs (with the same $\mathbf{f}_1, \mathbf{f}_2$). Again, a switching lemma variant is more useful for proving the general lemma for n-vectors. Further, the reduction to the k-linear assumption is achieved by embedding the k-linear challenge in a single pairing test which is a random linear combination of the k pairing tests.

We now state the switching lemma in its full generality and later remark on interesting special cases.

Lemma 1 (Switching Lemma). *Let $\mathcal{D}$ be an arbitrary efficiently samplable distribution over $n \times m$ matrices from $\mathbb{Z}_q$. For any PPT adversary $\mathcal{A}$ producing a vector of n elements from group $\mathbb{G}_1$, let $\Delta_{\mathcal{A}}$ be the following probability*

$$\Pr\left[\begin{array}{c} \mathbf{R} \xleftarrow{\$} \mathbb{G}_2^{m\times k},\ \mathsf{C}^{n\times m} \leftarrow \mathcal{D},\ \vec{\mathbf{f}}^{n\times 1} \leftarrow \mathcal{A}(\mathbf{g}_1, \mathbf{g}_2, \mathbf{R}, \mathsf{C}) : \\ \vec{\mathbf{f}} \neq \vec{\mathbf{0}}_1^{n\times 1} \ \textbf{and}\ \ e\left(\vec{\mathbf{f}}^{\top}, \mathsf{C}\cdot\mathbf{R}\right) = \vec{\mathbf{0}}_T^{1\times k} \end{array}\right]$$

Then, under the k-linear assumption for group $\mathbb{G}_2$, the following probability is negligibly close to $\Delta_{\mathcal{A}}$.

$$\Pr\left[\begin{array}{c} \mathbf{R} \xleftarrow{\$} \mathbb{G}_2^{m\times k},\ \mathsf{C}^{n\times m} \leftarrow \mathcal{D},\ \vec{\mathbf{f}}^{n\times 1} \leftarrow \mathcal{A}(\mathbf{g}_1, \mathbf{g}_2, \mathbf{R}, \mathsf{C}),\ \mathbf{R}' \xleftarrow{\$} \mathbb{G}_2^{m\times k} : \\ \vec{\mathbf{f}} \neq \vec{\mathbf{0}}_1^{n\times 1} \ \textbf{and}\ \ e\left(\vec{\mathbf{f}}^{\top}, \mathsf{C}\cdot\mathbf{R}'\right) = \vec{\mathbf{0}}_T^{1\times k} \end{array}\right]$$

The absolute value of the difference in the probabilities is bounded by $m \cdot \mathrm{ADV}(klin)$.

Remarks. If we assume that the distribution $\mathcal{D}$ overwhelmingly produces full ranked matrices, then observe that the later probability is information theoretically close to 0. Hence we can state:

$$\Pr\left[\begin{array}{c} \mathbf{R} \xleftarrow{\$} \mathbb{G}_2^{m\times k},\ \mathsf{C}^{n\times m} \leftarrow \mathcal{D},\ \vec{\mathbf{f}}^{n\times 1} \leftarrow \mathcal{A}(\mathbf{g}_1, \mathbf{g}_2, \mathbf{R}, \mathsf{C}) : \\ \vec{\mathbf{f}} \neq \vec{\mathbf{0}}_1^{n\times 1} \ \textbf{and}\ \ e\left(\vec{\mathbf{f}}^{\top}, \mathsf{C}\cdot\mathbf{R}\right) = \vec{\mathbf{0}}_T^{1\times k} \end{array}\right] \approx_{k-linear} 0$$

If, however, $\mathcal{D}$ produces singular matrices non-negligibly often, then there is an efficient adversary that can induce the event $\vec{\mathbf{f}} \neq \vec{\mathbf{0}}_1$ **and** $e(\vec{\mathbf{f}}^{\top}, \mathsf{C}\cdot\mathbf{R}) = \vec{\mathbf{0}}_T$.

The switching lemma still stands since the same adversary can induce the event $\vec{\mathbf{f}} \neq \vec{\mathbf{0}}_1$ **and** $e\left(\vec{\mathbf{f}}^{\top}, \mathsf{C} \cdot \mathbf{R}'\right) = \vec{\mathbf{0}}_T$ just as easily.

Although the presence of the C matrix is not strictly essential for the settings that we consider in this paper, we leave it in this form for generalizations to groups where the scalar field or ring is not easily invertible.

Instead of using the k-linear assumption directly, we use a related assumption which we call the *k-lifted linear assumption* and is implied by the k-linear assumption with a perfect reduction (see [JR13a] for a proof).

Definition 1 (k-lifted linear assumption). *For a constant $k \geq 1$, assuming a generation algorithm $\mathcal{G}$ that outputs a tuple $(q, \mathbb{G})$ such that $\mathbb{G}$ is of prime order q, the k-lifted linear assumption asserts that it is computationally infeasible to distinguish between*

$$\textsc{Tuple}_0 = (b_1 \cdot \mathbf{g}, \cdots, b_k \cdot \mathbf{g}, r_1 \cdot \mathbf{g}, \cdots, r_k \cdot \mathbf{g},\ b_1 s_1 \cdot \mathbf{g}, \cdots, b_k s_k \cdot \mathbf{g}, \sigma \cdot \mathbf{g})$$

and

$$\textsc{Tuple}_1 = (b_1 \cdot \mathbf{g}, \cdots, b_k \cdot \mathbf{g}, r_1 \cdot \mathbf{g}, \cdots, r_k \cdot \mathbf{g},\ b_1 s_1 \cdot \mathbf{g}, \cdots, b_k s_k \cdot \mathbf{g}, s_{k+1} \cdot \mathbf{g})$$

where $\mathbf{g}$ is chosen randomly from $\mathbb{G}$, b_i, r_i and s_i are chosen randomly from $\mathbb{Z}_q$, and $\sigma = \sum_{i=1}^{n} r_i s_i$.

Note that the k-linear assumption is a variant of the k-lifted linear assumption with all $r_1, ..., r_k$ equal to one. Now we prove the switching lemma under this weaker assumption.

Proof. (of Lemma 1) When $m \leq k$, the lemma follows information-theoretically (although the proof for $m > k$ also works for this case) by noting that in this case $\mathbf{R}$ will have rank m with high probability. Now we focus on the case that $m > k$. Consider the following inductive hypothesis (over j):

$$\Pr\left[\begin{array}{c} \mathbf{R} \xleftarrow{\$} \mathbb{G}_2^{m \times k},\ \mathsf{C}^{n \times m} \leftarrow \mathcal{D},\ \vec{\mathbf{f}}^{n \times 1} \leftarrow \mathcal{A}(\mathbf{g}_1, \mathbf{g}_2, \mathbf{R}, \mathsf{C}),\ \mathbf{R}' \xleftarrow{\$} \mathbb{G}_2^{m \times k} : \\ \vec{\mathbf{f}} \neq \vec{\mathbf{0}}^{n \times 1} \textbf{ and } e\left(\vec{\mathbf{f}}^{\top}, \mathsf{C} \cdot \mathbf{R}''\right) = \vec{\mathbf{0}}_T^{1 \times k} \end{array}\right]$$

differs from $\Delta_{\mathcal{A}}$ by at most $j \cdot \textsc{adv}(klin)$, where $\mathbf{R}''$ has the first $(m-j)$ rows same as first $(m-j)$ rows of $\mathbf{R}$ and the last j rows same as the last j rows of $\mathbf{R}'$. In the base case, i.e., when $j = 0$, this is same as the hypothesis (antecedent) in the lemma, and when $j = m$, this induction hypothesis is same as the claim (consequent) in the lemma. Thus, we just need to prove the induction step.

For an adversary $\mathcal{A}$, suppose the difference in the two probabilities corresponding to (induction hypothesis for) $j = t$ and $j = t + 1$ be δ. More precisely, denote the probability for adversary $\mathcal{A}$ corresponding to $j = t$ by Δ^t. Thus, we are supposing that $|\Delta^t - \Delta^{t+1}| \geq \delta$. Using $\mathcal{A}$ as a black box we wlll demonstrate an adversary $\mathcal{S}$ that will have advantage at least (negligibly close to) δ to break the k-lifted linear assumption.

So, let a *k-lifted linear* challenger produce: $(b_1 \cdot \mathbf{g}_2, \cdots, b_k \cdot \mathbf{g}_2, r_1 \cdot \mathbf{g}_2, ..., r_k \cdot \mathbf{g}_2,$ $b_1 s_1 \cdot \mathbf{g}_2, ..., b_k s_k \cdot \mathbf{g}_2, \boldsymbol{\chi})$ in the group $\mathbb{G}_2$, where $\boldsymbol{\chi}$ is either $(\sum_{i=1}^{n} r_i s_i) \cdot \mathbf{g}_2$ or

random. Note that b_i, r_i and s_i are chosen randomly and independently by the challenger.

Let vectors $\vec{\mathbf{r}}$ and $\vec{\mathsf{s}}$ be defined component-wise as $(\vec{\mathbf{r}})_i = r_i \cdot \mathbf{g}_2$ and $(\vec{\mathsf{s}})_i = s_i$, respectively. Define the k by k matrix B as the diagonal matrix with the i-th diagonal element set to b_i. Further, let $\mathbf{B} = \mathsf{B} \cdot \mathbf{g}_2$.

$\mathcal{S}$ samples $\mathsf{C}^{n \times m} \leftarrow \mathcal{D}$, and chooses $\mathbf{g}_1$ at random. It next samples an $(m - t - 1)$ by k matrix R_1 at random from $\mathbb{Z}_q$ (i.e. all elements of the matrix chosen randomly and independently from $\mathbb{Z}_q$). It sets $\mathbf{R}_1 = \mathsf{R}_1 \cdot \mathbf{B}$. It further samples a t by k matrix $\mathbf{R}_2$ at random from $\mathbb{G}_2$ (i.e. all elements chosen randomly and independently from $\mathbb{G}_2$). Finally $\mathcal{S}$ sets $\mathbf{R}$ to be the rows of $\mathbf{R}_1$, the row $\vec{\mathbf{r}}^\top$ and the rows of $\mathbf{R}_2$ combined (in that order) to form an m by k matrix. Observe that all of $\mathbf{R}$'s entries are independently random. The adversary $\mathcal{A}$ is then given $\mathbf{g}_1$, $\mathbf{g}_2$, $\mathbf{R}$ and C. The adversary $\mathcal{A}$ in response produces $\vec{\mathbf{f}}$. Now, $\mathcal{S}$ first checks that $\vec{\mathbf{f}}$ is non-zero. It then chooses another t by k matrix R_2 at random from $\mathbb{Z}_q$ and sets $\mathbf{R}_2 = \mathsf{R}_2 \cdot \mathbf{B}$. Noting that $\mathcal{S}$ has access to $\mathsf{B} \cdot \vec{\mathsf{s}} \cdot \mathbf{g}_2$, $\mathcal{S}$ (efficiently) performs the following bilinear test

$$e\left(\vec{\mathbf{f}}^\top, \mathsf{C} \cdot \begin{bmatrix} \mathsf{R}_1 \cdot \mathsf{B} \cdot \vec{\mathsf{s}} \cdot \mathbf{g}_2 \\ \boldsymbol{\chi} \\ \mathsf{R}_2 \cdot \mathsf{B} \cdot \vec{\mathsf{s}} \cdot \mathbf{g}_2 \end{bmatrix}\right) \stackrel{?}{=} \mathbf{0}_T \tag{1}$$

$\mathcal{S}$ outputs 1 if the test succeeds, and otherwise outpus 0.

Note that the above experiment has two games, one corresponding to real k-lifted linear challenge $\textsc{Tuple}_0$ choice, and one corresponding to fake k-lifted linear $\textsc{Tuple}_1$ challenge choice. We will call these games $\mathbf{G}_0$ (the real game) and $\mathbf{G}_0{}'$ (the fake game). Our aim is to show that the probability of $\mathcal{S}$ outputting 1 in the real game $\mathbf{G}_0$ differs from the probability of its outputting 1 in the fake game $\mathbf{G}_0{}'$ by (negligibly close to) δ. To prove this, we first modify the above two games. In the modified games $\mathbf{G}_1$ and $\mathbf{G}_1{}'$, $\mathcal{S}$ itself chooses the k-lifted linear challenges according to the same distribution as in $\mathbf{G}_0$ and $\mathbf{G}_0{}'$. However, it defers the choice of $\vec{\mathsf{s}}$ to after $\mathcal{A}$ has responded (noting that $\mathcal{A}$ is not given anything related to $\vec{\mathsf{s}}$). After $\mathcal{A}$ responds, $\mathcal{S}$ chooses $\vec{\mathsf{s}}$ at random, and also sets $\boldsymbol{\chi}$ as $\vec{\mathbf{r}}^\top \cdot \vec{\mathsf{s}}$ in $\mathbf{G}_1$ and as $\vec{\mathbf{r}}'^\top \cdot \vec{\mathsf{s}}$ in $\mathbf{G}_1{}'$, where $\vec{\mathbf{r}}'$ is another random k-tuple independent of $\vec{\mathbf{r}}$. Adversary $\mathcal{S}$ then performs the same test (1) as above, and outputs 1 if the test succeeds, and otherwise it outputs 0. Since the distributions in games $\mathbf{G}_1$ and $\mathbf{G}_1{}'$ are identical to the distributions in $\mathbf{G}_0$ and $\mathbf{G}_0{}'$ (resp.), the probabilities of $\mathcal{S}$ outputting 1 remains the same in the respective games.

Now, note that in the (real) game $\mathbf{G}_1$ the above test (1) is equivalent to testing

$$e\left(\vec{\mathbf{f}}^\top, \mathsf{C} \cdot \begin{bmatrix} \mathbf{R}_1 \\ \vec{\mathbf{r}}^\top \\ \mathbf{R}_2 \end{bmatrix} \cdot \vec{\mathsf{s}}\right) \stackrel{?}{=} \mathbf{0}_T \tag{2}$$

and in the (fake) game $\mathbf{G}_1{}'$ the test (1) is equivalent to testing (2) but with $\vec{\mathbf{r}}$ replaced by $\vec{\mathbf{r}}'$. Now define games $\mathbf{G}_2$ and $\mathbf{G}_2{}'$ which are identical to games $\mathbf{G}_1$

and $\mathbf{G}_1{}'$ (resp.) except that instead of (1) the final test performed by $\mathcal{S}$ in $\mathbf{G}_2$ is

$$e\left(\vec{\mathbf{f}}^{\top}, \mathsf{C} \cdot \begin{bmatrix} \mathbf{R}_1 \\ \vec{\mathbf{r}}^{\top} \\ \mathbf{R}_2 \end{bmatrix}\right) \stackrel{?}{=} \vec{\mathbf{0}}_T^{1\times k} \tag{3}$$

and the final test performed by $\mathcal{S}$ in $\mathbf{G}_2{}'$ is same but with $\vec{\mathbf{r}}$ replaced by $\vec{\mathbf{r}}'$. Going through the details of games $\mathbf{G}_2$ and $\mathbf{G}_2{}'$, it is clear that probability of $\mathcal{S}$ outputting 1 in $\mathbf{G}_2$ ($\mathbf{G}_2{}'$) is exactly Δ^t (resp. Δ^{t+1}). Moreover, since the distributions in $\mathbf{G}_1$ and $\mathbf{G}_2$ are identical, Δ^t is also the probability of (3) holding in $\mathbf{G}_1$. Thus, the probability of (2) holding in $\mathbf{G}_1$ is at least Δ^t, and no more except for the probability of (3) not holding and yet (2) holding. Since in game $\mathbf{G}_1$, $\vec{\mathbf{s}}$ is chosen after $\mathcal{A}$ responds, this additional probability is at most the probability (over random choice of $\vec{\mathbf{s}}$) of (2) holding for any fixed choice of rest of the coins in the game for which (3) does not hold. This probability is at most $1/q$. It follows that the probability of $\mathcal{S}$ outputting 1 in $\mathbf{G}_1$ (and hence in $\mathbf{G}_0$) differs from Δ^t by at most $1/q$. A similar argument shows that the probability of $\mathcal{S}$ outputting 1 in $\mathbf{G}_1{}'$ (and hence in game $\mathbf{G}_0{}'$) differs from Δ^{t+1} by at most $1/q$. Since, by hypothesis $|\Delta^{t+1} - \Delta^t| \geq \delta$, this completes the proof.

3 Quasi-Adaptive NIZK Proofs

We recall here the definitions from [JR13b] and provide a summary. Instead of considering NIZK proofs for a (witness-) relation R, the authors consider Quasi-Adaptive NIZK proofs for a probability distribution $\mathcal{D}$ on a collection of (witness-) relations $\mathcal{R} = \{R_\rho\}$. The quasi-adaptiveness allows for the common reference string (CRS) to be set based on R_ρ after the latter has been chosen according to $\mathcal{D}$. However the simulator generating the CRS (in the simulation world) is required to be a single probabilistic polynomial time algorithm that works for the whole collection of relations $\mathcal{R}$.

To be more precise, they consider ensemble $\{\mathcal{D}_\lambda\}$ of distributions on collection of relations $\mathcal{R}_\lambda$, where each $\mathcal{D}_\lambda$ specifies a probability distribution on $\mathcal{R}_\lambda = \{R_{\lambda,\rho}\}$. When λ is clear from context it can be dropped. Since in the quasi-adaptive setting the CRS could depend on the relation, an associated *parameter language* $\mathcal{L}_{\text{par}}$ is considered such that a member of this language is enough to characterize a particular relation, and this language member is provided to the CRS generator.

A tuple of algorithms $(\mathsf{K}_0, \mathsf{K}_1, \mathsf{P}, \mathsf{V})$ is called a *QA-NIZK* proof system for witness-relations $\mathcal{R}_\lambda = \{R_\rho\}$ with parameters sampled from a distribution $\mathcal{D}$ over associated parameter language $\mathcal{L}_{\text{par}}$, if there exists a probabilistic polynomial time simulator $(\mathsf{S}_1, \mathsf{S}_2)$, such that for all non-uniform PPT adversaries $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ we have:

Quasi-Adaptive Completeness:

$$\Pr[\lambda \leftarrow \mathsf{K}_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; \psi \leftarrow \mathsf{K}_1(\lambda, \rho); (x, w) \leftarrow \mathcal{A}_1(\lambda, \rho, \psi); \\ \pi \leftarrow \mathsf{P}(\psi, x, w) : \ \mathsf{V}(\psi, x, \pi) = 1 \text{ if } R_\rho(x, w)] = 1$$

Quasi-Adaptive Soundness:

$$\Pr[\lambda \leftarrow \mathsf{K}_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; \psi \leftarrow \mathsf{K}_1(\lambda, \rho); \\ (x, \pi) \leftarrow \mathcal{A}_2(\lambda, \rho, \psi) : \ \mathsf{V}(\psi, x, \pi) = 1 \ \text{ and } \ \neg(\exists w : R_\rho(x, w))] \approx 0$$

Quasi-Adaptive Zero-Knowledge:

$$\Pr[\lambda \leftarrow \mathsf{K}_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; \psi \leftarrow \mathsf{K}_1(\lambda, \rho) : \mathcal{A}_3^{\mathsf{P}(\psi, \cdot, \cdot)}(\lambda, \rho, \psi) = 1] \approx \\ \Pr[\lambda \leftarrow \mathsf{K}_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; (\psi, \tau) \leftarrow \mathsf{S}_1(\lambda, \rho) : \mathcal{A}_3^{\mathsf{S}(\psi, \tau, \cdot, \cdot)}(\lambda, \rho, \psi) = 1],$$

where $\mathsf{S}(\psi, \tau, x, w) = \mathsf{S}_2(\psi, \tau, x)$ for $(x, w) \in R_\rho$ and both oracles (i.e. P and S) output failure if $(x, w) \notin R_\rho$.

Note that ψ is the CRS in the above definitions.

4 Aggregating Quasi-Adaptive Proofs of Linear Subspaces

We summarize the linear-subspace QA-NIZK setting of [JR13b] here and refer the reader to that paper for details.

Linear Subspace Languages. We consider languages that are linear subspaces of vectors of $\mathbb{G}_1$ elements. In other words, the languages we are interested in can be characterized as languages parametrized by $\mathbf{A}$ as below:

$$L_{\mathbf{A}} = \{\vec{\mathsf{x}}^\top \cdot \mathbf{A} \in \mathbb{G}_1^n \mid \vec{\mathsf{x}} \in {\mathbb{Z}_q}^t\}, \text{ where } \mathbf{A} \text{ is a } t \times n \text{ matrix of } \mathbb{G}_1 \text{ elements.}$$

Here $\mathbf{A}$ is an element of the associated *parameter language* $\mathcal{L}_{\text{par}}$, which is all $t \times n$ matrices of $\mathbb{G}_1$ elements. The parameter language $\mathcal{L}_{\text{par}}$ also has a corresponding witness relation $\mathcal{R}_{\text{par}}$, where the witness is a matrix of $\mathbb{Z}_q$ elements : $\mathcal{R}_{\text{par}}(\mathbf{A}, \mathsf{A})$ iff $\mathbf{A} = \mathsf{A} \cdot \mathbf{g}_1$.

Robust and Efficiently Witness-Samplable Distributions. Let the $t \times n$ dimensional matrix $\mathbf{A}$ be chosen according to a distribution $\mathcal{D}$ on $\mathcal{L}_{\text{par}}$. The distribution $\mathcal{D}$ is called *robust* if with probability close to one the left-most t columns of $\mathbf{A}$ are full-ranked. A distribution $\mathcal{D}$ on $\mathcal{L}_{\text{par}}$ is called *efficiently witness-samplable* if there is a probabilistic polynomial time algorithm such that it outputs a pair of matrices $(\mathbf{A}, \mathsf{A})$ that satisfy the relation $\mathcal{R}_{\text{par}}$ (i.e., $\mathcal{R}_{\text{par}}(\mathbf{A}, \mathsf{A})$ holds), and further the resulting distribution of the output $\mathbf{A}$ is same as $\mathcal{D}$. For example, the uniform distribution on $\mathcal{L}_{\text{par}}$ is efficiently witness-samplable, by first picking A at random, and then computing $\mathbf{A}$.

QA-NIZK Construction. We now describe a computationally sound quasi-adaptive NIZK $(\mathsf{K}_0, \mathsf{K}_1, \mathsf{P}, \mathsf{V})$ for linear subspace languages $\{L_{\mathbf{A}}\}$ with parameters sampled from a robust and efficiently witness-samplable distribution $\mathcal{D}$ over the associated parameter language $\mathcal{L}_{\text{par}}$. As a conceptual starting point, we first develop a construction which has k^2 element proofs, demonstrating a single application of the Switching Lemma. Later, we give a k element construction which linearly combines the first construction proofs and uses an additional layer of Switching Lemma application. Our description here is self sufficient and relates to the scheme in [JR13b] in that we linearly combine proofs of multiple elements yielding constant-size proofs.

Algorithm K_1: The algorithm K_1 generates the CRS as follows. Let $\mathbf{A}^{t\times n}$ be the parameter supplied to K_1. Let $s \stackrel{\text{def}}{=} n - t$: this is the number of equations in excess of the unknowns. It generates a matrix $\mathsf{D}^{t\times k^2}$ with all elements chosen randomly from $\mathbb{Z}_q$ and k elements $\{b_v\}_{v\in[1,k]}$ and sk elements $\{r_{iu}\}_{i\in[1,s],u\in[1,k]}$ all chosen randomly from $\mathbb{Z}_q$. Define matrices $\mathsf{R}^{s\times k^2}$ and $\mathsf{B}^{k^2\times k^2}$ component-wise as follows:

$$(\mathsf{R})_{i,k(u-1)+v} = r_{iu}, \text{ with } i \in [1,s], u, v \in [1,k].$$

$$(\mathsf{B})_{ij} = \begin{cases} b_v & \text{if } i = j = k(u-1)+v, \text{ with } u, v \in [1,k] \\ 0 & \text{if } i \neq j, \text{ with } i, j \in [1,k^2] \end{cases}$$

Intuitively, the matrix R is a k times column-wise repetition of the r_{ij}'s, and if we denote $\{b_v\}_{v\in[1,k]}$ by $\vec{b}$, then the diagonal matrix B is just the vector $\vec{b}$ repeated k times along the diagonal (i.e. $\mathsf{B}_{k(u-1)+v,k(u-1)+v}$ is b_v and not b_u).

The common reference string (CRS) has two parts $\mathbf{CRS}_p$ and $\mathbf{CRS}_v$ which are to be used by the prover and the verifier respectively.

$$\mathbf{CRS}_p^{t\times k^2} := \mathbf{A} \cdot \begin{bmatrix} \mathsf{D} \\ \mathsf{R}\ \mathsf{B}^{-1} \end{bmatrix} \qquad \mathbf{CRS}_v^{(n+k^2)\times k^2} = \begin{bmatrix} \mathsf{D}\ \mathsf{B} \\ \mathsf{R} \\ -\mathsf{B} \end{bmatrix} \cdot \mathbf{g}_2$$

Prover P**:** Given candidate $\vec{l}^{1\times n} = \vec{\mathrm{x}}^{\top} \cdot \mathbf{A}$ with witness vector $\vec{\mathrm{x}}^{t\times 1}$, the prover generates the following proof consisting of k^2 elements in $\mathbb{G}_1$: $\vec{\mathbf{p}}^{1\times k^2} := \vec{\mathrm{x}}^{\top} \cdot \mathbf{CRS}_p$

Verifier V**:** Given candidate $\vec{l}^{1\times n}$, and proof $\vec{\mathbf{p}}^{1\times k^2}$, the verifier checks the following (k^2 equations) :

$$e\left(\left[\vec{l}^{1\times n} \middle|\ \vec{\mathbf{p}}^{1\times k^2}\right], \mathbf{CRS}_v\right) \stackrel{?}{=} \vec{\mathbf{0}}_T^{1\times k^2}$$

Theorem 1. *The above algorithms* $(\mathsf{K}_0, \mathsf{K}_1, \mathsf{P}, \mathsf{V})$ *constitute a computationally sound quasi-adaptive NIZK proof system for linear subspace languages* $\{L_{\mathbf{A}}\}$ *with parameters* $\mathbf{A}$ *sampled from a robust and efficiently witness-samplable distribution* $\mathcal{D}$ *over the associated parameter language* $\mathcal{L}_{par}$*, given any group generation algorithm for which the k-linear assumption holds for group* $\mathbb{G}_2$*.*

Proof Intuition. We now give a proof sketch for soundness and defer the full proof, including completeness and zero knowledge, to the full paper [JR13a].

Soundness: We prove soundness by transforming the system over a sequence of games. Consider an adversary $\mathcal{A}$ that *wins* if it can produce a "proof" $\vec{\mathbf{p}}$ for a candidate $\vec{l}$ that is not in $L_{\mathbf{A}}$ and yet the pairing test $e\left(\left[\vec{l}^{1\times n}\middle|\vec{\mathbf{p}}^{1\times k^2}\right], \mathbf{CRS}_v\right) \stackrel{?}{=} \vec{\mathbf{0}}_T^{1\times k^2}$ holds. Game $\mathbf{G}_0$ just replicates the soundness security definition. In Game $\mathbf{G}_1$ the CRS is generated using parameter witness A and its null-space, and this can be done efficiently by the challenger as the parameter distribution is efficiently witness samplable. After this transformation, we show that in the case of a certain event, a verifying proof of a non-language member implies breaking the k-linear assumption in group $\mathbb{G}_2$, while in the case of the event not occurring we can apply the Switching Lemma to bound the probability of the adversary winning.

In Game $\mathbf{G}_1$, the challenger efficiently samples $\mathbf{A}$ according to distribution $\mathcal{D}$, along with witness A (since $\mathcal{D}$ is an efficiently witness samplable distribution). Since A is a $t \times (t+s)$ dimensional rank t matrix, there is a rank s matrix $\begin{bmatrix}\mathsf{W}^{t\times s}\\ \mathrm{I}^{s\times s}\end{bmatrix}$ of dimension $(t+s)\times s$ whose columns form a complete basis for the null-space of A, which means $\mathsf{A}\cdot\begin{bmatrix}\mathsf{W}^{t\times s}\\ \mathrm{I}^{s\times s}\end{bmatrix} = 0^{t\times s}$. In this game, the NIZK CRS is computed as follows: Generate matrix $\mathsf{D}'^{\,t\times k^2}$ with elements randomly chosen from $\mathbb{Z}_q$ and the matrices $\mathsf{R}^{s\times k^2}$ and $\mathsf{B}^{k^2\times k^2}$ as in the real CRS. Implicitly set: $\mathsf{D} = \mathsf{D}' + \mathsf{W}\ \mathsf{R}\ \mathsf{B}^{-1}$. Therefore we have,

$$\mathbf{CRS}_p^{t\times k^2} = \mathbf{A}\cdot\begin{bmatrix}\mathsf{D}\\ \mathsf{R}\ \mathsf{B}^{-1}\end{bmatrix} = \mathbf{A}\cdot\left(\begin{bmatrix}\mathsf{D}'\\ 0^{s\times k^2}\end{bmatrix} + \begin{bmatrix}\mathsf{W}\\ \mathrm{I}^{s\times s}\end{bmatrix}\cdot\mathsf{R}\ \mathsf{B}^{-1}\right) = \mathbf{A}\cdot\begin{bmatrix}\mathsf{D}'\\ 0^{s\times k^2}\end{bmatrix}$$

$$\mathbf{CRS}_v^{(n+k^2)\times k^2} = \begin{bmatrix}\mathsf{D}\ \mathsf{B}\\ \mathsf{R}\\ -\mathsf{B}\end{bmatrix}\cdot\mathbf{g}_2 = \begin{bmatrix}\mathsf{D}'\ \mathsf{B}+\mathsf{W}\ \mathsf{R}\\ \mathsf{R}\\ -\mathsf{B}\end{bmatrix}\cdot\mathbf{g}_2$$

Suppose that $\mathcal{A}$ wins $\mathbf{G}_1$. Now, let us partition the $\mathbb{Z}_q$ matrix A as $\left[\mathsf{A}_0^{t\times t}\middle|\mathsf{A}_1^{t\times s}\right]$ and the candidate vector $\vec{l}$ as $\left[\vec{l}_0^{1\times t}\middle|\vec{l}_1^{1\times s}\right]$. Note that, since A_0 has rank t, the elements of $\vec{l}_0$ are 'free' elements and $\vec{l}_0$ can be extended to a unique n element vector $\vec{l}\,'$, which is a member of $L_{\mathbf{A}}$. This member vector $\vec{l}\,'$ can be computed as $\vec{l}\,'^{1\times n} := \left[\vec{l}_0\middle|-\vec{l}_0\cdot\mathsf{W}\right]$, where $\mathsf{W} = -\mathsf{A}_0^{-1}\mathsf{A}_1$. The proof of $\vec{l}\,'$ is computed as $\vec{\mathbf{p}}'^{1\times k^2} := \vec{l}_0\cdot\mathsf{D}'$. Since $\mathcal{A}$ wins $\mathbf{G}_1$, then $(\vec{l},\vec{\mathbf{p}})$ passes the verification test, and further by design $(\vec{l}',\vec{\mathbf{p}}')$ passes the verification test. Thus, we obtain: $(\vec{l}_1' - \vec{l}_1)\cdot\mathsf{R} = (\vec{\mathbf{p}}' - \vec{\mathbf{p}})\cdot\mathsf{B}$, where $\vec{l}_1'^{1\times s} = -\vec{l}_0\cdot\mathsf{W}$. This gives us a set of equalities,

for all $u \in [1,k]$:

$$\sum_{i=1}^{s}(\boldsymbol{l}'_{1i}-\boldsymbol{l}_{1i})\cdot r_{iu} = (\mathbf{p}'_{k(u-1)+1}-\mathbf{p}_{k(u-1)+1})\cdot b_1 = \cdots = (\mathbf{p}'_{k(u-1)+k}-\mathbf{p}_{k(u-1)+k})\cdot b_k \tag{4}$$

Note that since $\vec{\boldsymbol{l}}$ is not in the language, there exists an $i \in [1,s]$, such that $\vec{\boldsymbol{l}}'_{1i} - \vec{\boldsymbol{l}}_{1i} \neq 0$. Now consider the event E defined as follows:

$$\text{Event } E \equiv \text{ For some } u \in [1,k] : \sum_{i=1}^{s}(\boldsymbol{l}'_{1i} - \boldsymbol{l}_{1i}) \cdot r_{iu} \neq \mathbf{0}_1 \tag{5}$$

Our strategy now is to show that the probability of $\mathcal{A}$ winning in both the events E and $\neg E$ is negligible. Under the event $\neg E$, we apply the Switching Lemma to switch the r_{iu}'s to a fresh set of random values r'_{iu}'s while verifying. After that, we argue information theoretically that the probability of winning the switched game is negligible. Under the event E, we show that one can build a k-linear challenge adversary using $\mathcal{A}$, such that if $\mathcal{A}$ wins then this new adversary can efficiently compute the (least) u in Event E, and using the multiple equalities in Equation 4 it can break the k-linear challenge. □

We now show that the proof system described above with k^2 group elements can be further shortened to just k group elements. The main idea is to observe that Equation 4 is again several sets of equations, and we can carefully set up the system so that the prover only shows random linear combinations of Equation 4. Then resorting to Switching Lemma we conclude that the individual equations must be true. We now describe this optimized Quasi-Adaptive NIZK proof system in detail.

QA-NIZK construction with k elements. In this construction the **Algorithm** K_1 generates the CRS as follows. It generates a matrix $\mathsf{D}^{t\times k}$ with all elements chosen randomly from $\mathbb{Z}_q$ and k elements $\{b_v\}_{v\in[1,k]}$ and k^3 elements $\{t_{uvw}\}_{u,v,w\in[1,k]}$ and sk elements $\{r_{iu}\}_{i\in[1,s],u\in[1,k]}$ all chosen randomly from $\mathbb{Z}_q$. Define matrices $\mathsf{R}^{s\times k}$ and $\mathsf{B}^{k\times k}$ component-wise as follows:

$$(\mathsf{R})_{iw} = \sum_{u=1}^{k}\sum_{v=1}^{k} r_{iu}t_{uvw}, \text{ with } i \in [1,s], w \in [1,k].$$

$$(\mathsf{B})_{vw} = \sum_{u=1}^{k} b_v t_{uvw}, \text{ with } v, w \in [1,k].$$

The construction of $\mathbf{CRS}_p$ and $\mathbf{CRS}_v$ remain algebraically the same, although now they use lesser elements. The prover and verifier also retain the same algebraic form. The set of equalities for this construction corresponding to the equation $(\vec{\boldsymbol{l}}'_1 - \vec{\boldsymbol{l}}_1) \cdot \mathsf{R} = (\vec{\mathbf{p}}' - \vec{\mathbf{p}}) \cdot \mathsf{B}$, is for all $w \in [1,k]$:

$$\sum_{i=1}^{s}\left[(\boldsymbol{l}'_{1i} - \boldsymbol{l}_{1i}) \cdot \left(\sum_{u=1}^{k}\sum_{v=1}^{k} r_{iu}t_{uvw}\right)\right] - \sum_{v=1}^{k}\left[(\mathbf{p}'_v - \mathbf{p}_v) \cdot \left(\sum_{u=1}^{k} b_v t_{uvw}\right)\right] = \mathbf{0}_1 \tag{6}$$

Rearranging, we get for all $w \in [1,k]$:

$$\sum_{u=1}^{k}\sum_{v=1}^{k}\left[t_{uvw}\left(\sum_{i=1}^{s}\left[(\boldsymbol{l}'_{1i}-\boldsymbol{l}_{1i})\cdot r_{iu}\right]-(\mathbf{p}'_v-\mathbf{p}_v)\cdot b_v\right)\right]=\mathbf{0}_1 \tag{7}$$

Now, using the Switching Lemma and after applying information theoretic arguments, we transition to a game where the adversary wins if it wins the original game and the following event occurs:

$$\text{For all } u\in[1,k]:\sum_{i=1}^{s}(\boldsymbol{l}'_{1i}-\boldsymbol{l}_{1i})\cdot r_{iu}=(\mathbf{p}'_1-\mathbf{p}_1)\cdot b_1=\cdots=(\mathbf{p}'_k-\mathbf{p}_k)\cdot b_k \tag{8}$$

After this point, the proof is analogous to the previous QA-NIZK construction. Detailed proof is given in [JR13a]. We also give a more optimized construction in [JR13a] which uses less randomness and enjoys a better security reduction.

5 Aggregating Groth-Sahai Proofs

We show that proofs of multiple linear scalar-multiplication equations, as well as multiple *linear* pairing product equations can be aggregated into a single proof in the Groth-Sahai system. We will focus on describing the aggregation for the scalar-multiplication equations, as the results for the linear pairing product equations are obtained in almost an identical manner.

Consider bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with pairing e into a third group $\mathbb{G}_T$. Consider equations of the type

$$\sum_{i=1}^{n} y_i\cdot\mathbf{a}_i \;+\; \sum_{i=1}^{m} b_i\cdot\mathbf{x}_i=\mathbf{t}_1 \tag{9}$$

where the variables y_i are to take values in $\mathbb{Z}_q$, the variables $\mathbf{x}_i$ are to take values in $\mathbb{G}_1$. The constants $\mathbf{a}_i$ are in $\mathbb{G}_1$, and scalar constants b_i are in $\mathbb{Z}_q$. Moreover, $\mathbf{t}_1$ is in $\mathbb{G}_1$.

When the bilinear group is symmetric, i.e. $\mathbb{G}_1=\mathbb{G}_2$, and under the DLIN assumption, the Groth-Sahai NIZK proof of the above equation requires commitments to the variables, each commitment being of size *three* group elements (for both y_i or $\mathbf{x}_i$). In addition it requires a proof of *nine* group elements. When there are multiple equations of the above kind in the same variables, the commitments to the variables remain the same, but each equation requires nine group elements. In other words, if there are $m+n$ variables and k equations, the full proof of the k equations has size $3\cdot(m+n)+9k$ group elements.

We will now show that in the quasi-adaptive setting, the full proof of the k equations can be obtained with size $3\cdot(m+n)+9$ group elements. We first describe how the proof is done in the Groth-Sahai system, and then we will point out the relevant changes. The proofs and commitments actually belong to the $\mathbb{Z}_q$-module $\mathbb{G}^3$ (where $\mathbb{G}=\mathbb{G}_1=\mathbb{G}_2$).

We will write these groups in additive notation, and the bilinear pairing operation $e(A, B)$ written in infix notation as $A \otimes B$, with the pairing operation defining a tensor product $\mathbb{G} \otimes \mathbb{G}$ over $\mathbb{Z}_q$. Without loss of generality (see e.g. A2.2 in [Eis95]), we can assume that $\mathbb{G}_T = \mathbb{G} \otimes \mathbb{G}$. Further, this naturally extends to a tensor product $\mathbb{G}^3 \otimes \mathbb{G}^3$. One can also define a tensor product $\mathbb{Z}_q \otimes \mathbb{G}$, but since $\mathbb{G}$ is a $\mathbb{Z}_q$-module, this tensor product is just $\mathbb{G}$.

Let $\iota_1 : \mathbb{Z}_q \to \mathbb{G}^3$, $\iota_2 : \mathbb{G} \to \mathbb{G}^3$, $p_1 : \mathbb{G}^3 \to \mathbb{Z}_q$, $p_2 : \mathbb{G}^3 \to \mathbb{G}$ be group homomorphisms s.t. $\iota_1 \circ p_1$, and $\iota_2 \circ p_2$ are identity maps in $\mathbb{Z}_q$ and $\mathbb{G}$ resp. Note that the maps ι_1 and ι_2 naturally define a group homomorphism ι_T from $\mathbb{Z}_q \otimes \mathbb{G}$ $(= \mathbb{G})$ to $\mathbb{G}^3 \otimes \mathbb{G}^3$, and similarly p_1 and p_2 define a group homomorphism p_T from $\mathbb{G}^3 \otimes \mathbb{G}^3$ to $\mathbb{Z}_q \otimes \mathbb{G}$ $(= \mathbb{G})$.

The NIZK common reference string (CRS) consists of three elements from $\mathbb{G}^3$, i.e. $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3 \in \mathbb{G}^3$. They are chosen as follows: $\boldsymbol{u}_1 = (\alpha \cdot \mathbf{g}, \mathcal{O}, \mathbf{g})$, and $\boldsymbol{u}_2 = (\mathcal{O}, \beta \cdot \mathbf{g}, \mathbf{g})$, and $\boldsymbol{u}_3 = r\boldsymbol{u}_1 + s\boldsymbol{u}_2$, for random $\alpha, \beta, r, s \in \mathbb{Z}_q$, and random $\mathbf{g} \in \mathbb{G} \backslash \mathcal{O}$. This real-world CRS $\vec{\boldsymbol{u}}$ is sometimes also referred to as the *binding* CRS.

The map $\iota_2(\mathcal{Z})$ is just $(\mathcal{O}, \mathcal{O}, \mathcal{Z})$, and $p_2(\mathcal{Z}_1, \mathcal{Z}_2, \mathcal{Z}_3) = \mathcal{Z}_3 - \alpha^{-1}\mathcal{Z}_1 - \beta^{-1}\mathcal{Z}_2$, which shows that $\iota_2 \circ p_2$ is an identity map. It also shows that $p_2(\boldsymbol{u}_1) = p_2(\boldsymbol{u}_2) = p_2(\boldsymbol{u}_3) = \mathcal{O}$. Now, the **commitments** to elements $\mathcal{Z}$ in $\mathbb{G}$ are made by picking r_1, r_2, r_3 at random from $\mathbb{Z}_q$, and setting $c_2(\mathcal{Z}) = \iota_2(\mathcal{Z}) + r_1\boldsymbol{u}_1 + r_2\boldsymbol{u}_2 + r_3\boldsymbol{u}_3$. Thus, $p_2(c_2(\mathcal{Z})) = \mathcal{Z}$, and hence the name binding CRS.

The map $\iota_1(z)$ is $\iota_2(z \cdot \mathbf{g})$, and hence commitment to $z \in \mathbb{Z}_q$ is $c_1(z) = c_2(z \cdot \mathbf{g})$.

For equations of the form (9) , i.e. $\vec{y} \cdot \vec{\mathbf{a}} + \vec{b} \cdot \vec{\mathbf{x}} = \mathbf{t}_1$, a proof $\vec{\boldsymbol{\pi}}$ (along with commitments to variables) is obtained by setting $\vec{\boldsymbol{\pi}} = S^\top \iota_2(\vec{\mathbf{a}}) + R^\top \iota_1(\vec{b}) + \vec{\boldsymbol{\theta}}$, where R is the matrix of rows (r_1, r_2, r_3), coming from $c_2(\mathbf{x}_i)$, one for each committed variable $\mathbf{x}_i$, and S is the matrix of rows (r_1, r_2, r_3), coming from $c_1(y_i)$, one for each committed variable y_i. Note, $\vec{\boldsymbol{\pi}}$ is vector of three $\mathbb{G}^3$ elements. The vector $\vec{\boldsymbol{\theta}}$ is set to be a random linear combination of $H_i\vec{\boldsymbol{u}}$, where H_i are finitely many matrices, and form a basis for the solutions to $\vec{\boldsymbol{u}} \bullet H\vec{\boldsymbol{u}} = 0$. It turns out that these matrices H_i are independent of the ZK simulator trapdoors α and β.

Let "$\bullet$" denote the dot product of vectors of elements from $\mathbb{G}^3$ and $\mathbb{G}^3$ w.r.t. product $\otimes$. The commitments $\vec{c_1}, \vec{c_2}$ and the proof are **verified** by the following equation:

$$\iota_1(\vec{b}) \bullet \vec{c_2} + \vec{c_1} \bullet \iota_2(\vec{\mathbf{a}}) = \iota_1(1) \bullet \iota_2(\mathbf{t}_1) + \vec{\boldsymbol{u}} \bullet \vec{\boldsymbol{\pi}}.$$

Quasi-Adaptive Aggregation. In the quasi-adaptive setting [JR13b], the NIZK CRS is allowed to depend on the language parameters, but with the further requirement that the ZK simulation be uniform. In the above context, the language parameters are $\vec{\mathbf{a}}$ and $\vec{\mathrm{b}}$. Note $\mathbf{t}_1$ is *not* a language parameter, as it is a quantity produced by the prover.

So, let there be k equations in the same variables, with the j-th equation being

$$\vec{y} \cdot \vec{\mathbf{a}}^j + \vec{b}^j \cdot \vec{\mathbf{x}} = \mathbf{t}_1^j \tag{10}$$

In the above setting the prover produces k proofs, $\vec{\boldsymbol{\pi}}^j$. We would like the prover to give a random linear combination of these proofs, where the randomness is fixed in the CRS setup. In the DLIN setting, we need two different linear combinations. Thus, let the CRS generator choose two random $\mathbb{Z}_q$-vectors $\vec{\rho}$ and $\vec{\psi}$. The prover is required to produce $\vec{\boldsymbol{\pi}}_\rho = \sum_{j\in[1,k]} \rho_j \cdot \vec{\boldsymbol{\pi}}^j$ and $\vec{\boldsymbol{\pi}}_\psi = \sum_{j\in[1,k]} \psi_j \cdot \vec{\boldsymbol{\pi}}^j$. To be able to do so, the prover needs $\sum_j \rho_j \cdot \iota_2(\vec{\mathbf{a}}^j)$, $\sum_j \rho_j \cdot \iota_1(\vec{b}^j)$ (and similar terms using ψ_j). The $\vec{\boldsymbol{\theta}}$ terms in the proofs need not be linearly combined, and the prover can just add one such term to each of $\vec{\boldsymbol{\pi}}_\rho$ and $\vec{\boldsymbol{\pi}}_\psi$, as its purpose is only to allow zero-knowledge simulation (i.e. witness hiding). The CRS generator can certainly produce these elements and give them as part of the CRS. The CRS generator also needs to give as part of the verification CRS the terms $\langle \iota_1(\rho_j)\rangle_j$ and $\langle \iota_1(\psi_j)\rangle_j$. In order to apply the switching lemma, we show in the proof of the theorem below that if $\vec{\mathbf{a}}^j$ are efficiently witness samplable, then the CRS generator can also simulate this verification CRS given $\rho_j \cdot \mathbf{g}$ and $\psi_j \cdot \mathbf{g}$.

The verification is now done as follows:

$$(\sum_j \rho_j \cdot \iota_1(\vec{b}^j)) \bullet \vec{c_2} + \vec{c_1} \bullet (\sum_j \rho_j \cdot \iota_2(\vec{\mathbf{a}}^j)) = \sum_j (\iota_1(\rho_j) \bullet \iota_2(\mathbf{t}_1^j)) + \vec{\boldsymbol{u}} \bullet \vec{\boldsymbol{\pi}}_\rho \quad (11)$$

$$(\sum_j \psi_j \cdot \iota_1(\vec{b}^j)) \bullet \vec{c_2} + \vec{c_1} \bullet (\sum_j \psi_j \cdot \iota_2(\vec{\mathbf{a}}^j)) = \sum_j (\iota_1(\psi_j) \bullet \iota_2(\mathbf{t}_1^j)) + \vec{\boldsymbol{u}} \bullet \vec{\boldsymbol{\pi}}_\psi \quad (12)$$

Theorem 2. *The above system constitutes a computationally-sound quasi-adaptive NIZK proof system for equations (10) with parameters $\langle \vec{\mathbf{a}}^j \rangle_j$, $\langle \vec{b}^j \rangle_j$, whenever $\langle \vec{\mathbf{a}}^j \rangle_j$ are chosen according to an efficiently witness-samplable distribution, and given any group generation algorithm for which the DLIN assumption holds.*

Proof of the theorem can be found in [JR13a]. Since Groth-Sahai proofs of more general equations (involving quadratic terms) require pairing of adversarially supplied commitments with each other, the switching lemma is not directly applicable. It remains an open problem to aggregate such NIZK proofs.

6 Extensions and Applications

Tags. We extend the system of Section 4 to include tags mirroring [JR13b]. The tags are elements of $\mathbb{Z}_q$, are included as part of the proof and are used as part of the defining equations of the language. We still get k element proofs based on the k-linear assumption. Details are in [JR13a].

KDM-CCA2 Encryption [CCS09]. In the paper [CCS09], the authors construct a public key encryption scheme simultaneously secure against key dependent chosen plaintext (KDM) and adaptive chosen ciphertext attacks (CCA2). They apply a Naor-Yung "double encryption" paradigm to combine any KDM-CPA secure scheme with any IND-CCA2 secure scheme along with an appropriate

NIZK proof, to obtain a KDM-CCA2 secure scheme. In a particular construction, they obtain short ciphertexts by combining the KDM-CPA secure scheme of [BHHO08] with the IND-CCA2 scheme of [CS98], along with a Groth-Sahai NIZK proof. We show that the NIZK proof required in this construction can be considerably shortened. We defer the reader to [CCS09] for details of the scheme, and just describe the equations to be proved here. Consider bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ in which the K-linear and L-linear assumptions hold, respectively.

Let $\vec{\mathbf{g}}_1, \cdots, \vec{\mathbf{g}}_K, \mathbf{h}_1, \cdots, \mathbf{h}_K$ be part of the public key of the KDM-CPA secure encryption scheme and let $\vec{\mathbf{f}}_1, \cdots, \vec{\mathbf{f}}_K, \mathbf{c}_1, \cdots, \mathbf{c}_K, \mathbf{d}_1, \cdots, \mathbf{d}_K, \mathbf{e}_1, \cdots, \mathbf{e}_K$ be part of the public key of the IND-CCA2 secure encryption scheme. Let $(\vec{\mathbf{g}}, \mathbf{h}) \in \mathbb{G}_1^N \times \mathbb{G}_1$ be a ciphertext from the KDM-CPA secure encryption scheme and $(\vec{\mathbf{f}}, \mathbf{a}, \mathbf{b}) \in \mathbb{G}_1^{K+1} \times \mathbb{G}_1 \times \mathbb{G}_1$ be a ciphertext from the IND-CCA2 secure encryption scheme, with label l. Let $t = H(\vec{\mathbf{f}}, \mathbf{a}, l)$, where H is a collision resistant hash. The purpose of the NIZK proof is to establish that they encrypt the same plaintext. This translates to the following statement:

$$\exists r_1, \cdots, r_K, w_1, \cdots, w_K : \begin{pmatrix} \vec{\mathbf{g}} = \sum_{i=1}^{K} r_i \cdot \vec{\mathbf{g}}_i \ \wedge \ \vec{\mathbf{f}} = \sum_{i=1}^{K} w_i \cdot \vec{\mathbf{f}}_i \wedge \\ \mathbf{b} = \sum_{i=1}^{K} w_i \cdot (\mathbf{d}_i + t \cdot \mathbf{e}_i) \wedge \\ \mathbf{h} - \mathbf{a} = \sum_{i=1}^{K} r_i \cdot \mathbf{h}_i - \sum_{i=1}^{K} w_i \cdot \mathbf{c}_i \end{pmatrix}$$

This translates into $N + K + 3$ equations in $2K$ variables. Using the Groth-Sahai NIZK scheme, this requires $(2K)(L+1)$ elements of $\mathbb{G}_2$ and $(N+K+3)L$ elements of $\mathbb{G}_1$. In our scheme this requires L elements of $\mathbb{G}_1$ in the proof - **1** under DDH and **2** under DLIN assumptions in $\mathbb{G}_2$.

CCA2-IBE Scheme [JR13b]. The definition of CCA2-secure encryption [BDPR98] naturally extends to the Identity-Based Encryption setting [CHK04]. In [JR13b], the authors construct a fully adaptive CCA2-secure IBE, which also allows public verification of the assertion that a ciphertext is valid for the particular claimed identity. The IBE scheme has four group elements (and a tag), where one group element serves as one-time pad for encrypting the plaintext. The remaining three group elements form a linear subspace with one variable as witness and three integer tags corresponding to: (a) the identity, (b) the tag needed in the IBE scheme, and (c) a 1-1 (or universal one-way) hash of some of the elements. It was shown that if these three group elements can be QA-NIZK proven to be consistent, and given the unique proof property of the QA-NIZKs, then the IBE scheme can be made CCA2-secure. Since, there are three components, and one variable the QA-NIZK required only two group elements under SXDH. We slightly shorten the proof to one element under SXDH. We defer the reader to [JR13b] for details of the original system, and just describe the Key Generation and Encryption steps in [JR13a].

References

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In

Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 26–45. Springer, August 1998.

[BFI+10] Olivier Blazy, Georg Fuchsbauer, Malika Izabachène, Amandine Jambert, Hervé Sibert, and Damien Vergnaud. Batch Groth-Sahai. In Jianying Zhou and Moti Yung, editors, *ACNS 10*, volume 6123 of *LNCS*, pages 218–235. Springer, June 2010.

[BHHO08] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision Diffie-Hellman. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 108–125. Springer, August 2008.

[CCS09] Jan Camenisch, Nishanth Chandran, and Victor Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, April 2009.

[CHK04] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222. Springer, May 2004.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, August 1998.

[Dam] Ivan Damgård. On Σ protocols. http://www.daimi.au.dk/ ivan/Sigma.pdf.

[Eis95] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, August 1986.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, April 2008.

[HK07] Dennis Hofheinz and Eike Kiltz. Secure hybrid encryption from weakened key encapsulation. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer, August 2007.

[JR13a] Charanjit Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. Cryptology ePrint Archive, Report 2013/670, 2013. http://eprint.iacr.org/2013/670.

[JR13b] Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, December 2013.

[LPJY14] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT*, volume 8441 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2014.

[Sha07] Hovav Shacham. A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. http://eprint.iacr.org/.