Efficient Quasi-Adaptive NIZK

Kairi Kangro

Tartu University

Abstract. This report gives an overview of the Quasi-Adaptive Non-Interactive Zero Knowledge proof system introduced recent papers by Joy and Rutla ([JR13a,JR13b]). This system reduces the proof size for linear subspace languages to constant-sized proofs under the k-linear assumption.

1 Introduction

Non-Interactive Zero Knowledge (NIZK) proofs have found multiple applications in different cryptographic protocols, such as signature schemes and Identity-Based encryption. This implies the need for as efficient NIZK protocols as possible. One of the most well-known efficient NIZK proof systems was given by Groth-Sahai in [GS08], but its proof sizes were still linear in the number of variables and equations. In two recent papers ([JR13a,JR13b]) Jutla and Roy managed to create a NIZK proof system with constant-sized proofs for linear subspace languages under a slightly different Quasi-Adapative NIZK setting.

This report will give an overview of the construction given in [JR13b]. The main novel ideas seem to be the use of the null space of the language in the soundness proof, and the use of a switching lemma which allows the compression of proofs by enabling testing with linear combinations of base vectors, instead of having to check with every base vector.

2 Quasi-Adaptive Non-Interactive Zero Knowledge Proofs

2.1 Zero Knowledge Proofs

A zero knowledge proof or protocol is a method for one party, called the prover, to prove to the other party, called the verifier, that some statement is true, without revealing anything more to the verifier than just the truth of that statement. A zero knowledge protocol has to satisfy the following properties:

- Completeness: When the statement that the prover is trying to prove is true, the verifier should accept.
- Soundness: When the statement that the prover is trying to prove is not true, the probability of the verifier accepting should be negligible.

– Zero-knowledge: When the statement that the prover is trying to prove is true, then the verifier should not learn anything beyond the fact that it is true. This is formalized by showing that there exists a simulator that, given only the statement to be proved, can produce an simulated interaction between a prover and a verifier that is indistinguisable from actual interactions.

Usually, a zero knowledge protocol requires interaction between the prover and the verifier, with the verifier sending challenges to the prover and the prover responding. However, if there exists a trusted third party, it is possible to create a non-interactive zero knowledge protocol (NIZK), where the verifier does not interact with the prover apart from receiving the proof once, by having the trusted third party generate a common reference string (CRS), which will be known both to the prover and the verifier.

2.2 Quasi-Adaptive NIZK

In usual zero knowledge proofs, a so-called witness relation R is considered, with the goal of the prover being to show that for the given statement y, it knows a "witness" w such that $(y, w) \in R$. The authors of [JR13a] consider instead Quasi-Adaptive NIZK proofs on a collection of witness relations $\mathcal{R} = \{R_\rho\}$, where the actual relation to be used is chosen according to some probability distribution $\mathcal{D}$ (both $\mathcal{R}$ and $\mathcal{D}$ may depend on the security parameter λ). Here quasi-adaptiveness means that the CRS may depend on the chosen relation R_ρ, however, the simulator in the zero knowledge proof should work for the whole collection $\mathcal{R}$. Since the CRS may depend on the chosen relation, an associated parameter language $\mathcal{L}_{par}$ is considered, such that a member of this language uniquely identifies a particular relation, and this language member is given as input to the CRS generator.

Definition 1 (Quasi-Adaptive NIZK proof system[JR13a]). *A tuple of algorithms (K_0, K_1, P, 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 $\mathcal{L}_{par}$, if there exists a probabilistic polynomial time simulator (S_1, S_2) such that for all non-uniform PPT adversaries $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ we have:*

1. *Quasi-Adaptive Completeness:*

$$Pr[\lambda \leftarrow K_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; \phi \leftarrow K_1(\lambda, \rho); (x, w) \leftarrow \mathcal{A}_1(\lambda, \phi, \rho); \\ \pi \leftarrow P(\phi, x, w) : V(\phi, x, \pi) = 1 \text{ if } R_\rho(x, w)] = 1.$$

2. *Quasi-Adaptive Soundness:*

$$Pr[\lambda \leftarrow K_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; \phi \leftarrow K_1(\lambda, \rho); (x, \pi) \leftarrow \mathcal{A}_2(\lambda, \phi, \rho) : \\ V(\phi, x, \pi) = 1 \text{ and } \neg(\exists w : R_\rho(x, w))] \approx 0.$$

3. *Quasi-Adaptive Zero Knowledge:*

$$Pr[\lambda \leftarrow K_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; \phi \leftarrow K_1(\lambda, \rho) : \mathcal{A}_3^{P(\phi,\cdot,\cdot)}(\lambda, \phi, \rho) = 1] \approx$$
$$Pr[\lambda \leftarrow K_0(1^m); \rho \leftarrow \mathcal{D}_\lambda; (\phi, \tau) \leftarrow S_1(\lambda, \rho) : \mathcal{A}_3^{S(\phi,\tau,\cdot,\cdot)}(\lambda, \phi, \rho) = 1],$$

where $S(\phi, \tau, x, w) = S_2(\phi, \tau, x)$ for $(x, w) \in R_\rho$ and both oracles (i.e. P and S) output failure if $(x, w) \notin R_\rho$.

Note that ϕ is the CRS in the above definition.

3 Algebraic background

Zero-knowledge constructions are often based on groups with a bilinear map, which satisfy some security assumption. The definition of a bilinear map is as follows:

Definition 2 (Bilinear Map). *Let $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$ be cyclic additive groups with the same order and $\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3$ be their respective generators. Then $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ is called a bilinear map if $e(a\mathbf{g}_1, b\mathbf{g}_2) = (ab)\mathbf{g}_3$ for all $a, b \in \mathbb{Z}$.*

In the proof of soundness, we also need to know something about null-spaces of matrices. The null-space of a $t \times n$ matrix A is the set of all vectors $\vec{x}$ for which $A \cdot \vec{x} = 0$. The soundness proof uses the following lemma [WIKI]:

Lemma 1. *Let A be a $t \times n$ matrix whose first t columns are independent. Then there exists an $n \times n - t$ matrix of the form $\begin{bmatrix} W^{t\times(n-t)} \\ I^{(n-t)\times(n-t)} \end{bmatrix}$, whose columns form a complete basis for the null-space of A.*

4 Quasi-Adaptive Proof of Linear Subspaces

In this section, we will give an overview of the QA-NIZK construction in [JR13b], which requires only k-element proofs under the k-linear assumption.

4.1 Linear Subspace languages

Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be cyclic additive groups of prime order q with a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ chosen by a group generation algorithm, and let $\mathbf{g}_1$ and $\mathbf{g}_2$ be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. The bilinear map e extends naturally to $\mathbb{Z}_q$ vector spaces of the same dimension by summation: $e(\vec{\mathbf{a}}, \vec{\mathbf{b}}^T) = \sum_{i=1}^n e(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_i)$.

In the construction, we consider languages that are linear subspaces of the $\mathbb{Z}_q$ vector spaces of $\mathbb{G}_1$, that is, languages

$$L_{\mathbf{A}} = \{\vec{x} \cdot \mathbf{A} \in \mathbb{G}_1^n | \vec{x} \in \mathbb{Z}_q^t\},$$

where the parameter $\mathbf{A}$ is a $t \times n$ matrix of $\mathbb{G}_1$ elements. The associated witness relation for language $L_{\mathbf{A}}$ is $R_{\mathbf{A}} = \{(\vec{\mathbf{z}}, \vec{x}) | \vec{\mathbf{z}} = \vec{x} \cdot \mathbf{A}\}$. The associated parameter

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

For the construction to work, the distribution $\mathcal{D}$ also needs to satisfy some conditions, namely it needs to be robust and efficiently witness-samplable.

Definition 3 (Robust and Efficiently Witness-Samplable Distributions [JR13b]). *Let the $t \times n$ dimensional matrix $\mathbf{A}$ bet chosen according to a distribution $\mathcal{D}$ on $\mathcal{L}_{par}$. The distribution $\mathcal{D}$ is called robust if with probability close to one the left-most t columns of $\mathbf{A}$ are full-ranked. The distribution is called efficiently witness-samplable if there is a probalistic polynomial time algorithm such that it outputs a pair of matrices $(\mathbf{A}, A)$ that satisfy the relation $\mathcal{R}_{par}$ and the resulting distribution of the output $\mathbf{A}$ is the same as $\mathcal{D}$.*

4.2 QA-NIZK Construction

We will now describe the QA-NIZK (K_0, K_1, P, V) given in [JR13b] 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 under the k-linear assumption.

- **Algorithm** K_0. Algorithm K_0 is the group generator for which the security assumption holds, taking as input the security parameter m and outputting $\lambda = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \mathbf{g}_1, \mathbf{g}_2)$.
- **Algorithm** K_1. Let $s = n - t$. Algorithm K_1 generates the CRS as follows. First, it generates a $t \times k$ matrix D with elements chosen randomly from $\mathbb{Z}_q$, and chooses k elements $\{b_v\}_{v\in[1,k]}$, k^3 elements $\{t_{uvw}\}_{u,v,w\in[1,k]}$ and sk elements $\{r_{iu}\}_{i\in[1,s],u\in[1,k]}$ also randomly from $\mathbb{Z}_q$. Then it defines a $s \times k$ matrix R and a $k \times k$ matrix B as follows:

$$R_{iw} = \sum_{u=1}^{k}\sum_{v=1}^{k} r_{iu}t_{uvw}, i \in [1,s], w \in [1,k]$$

$$B_{vw} = \sum_{u=1}^{k} b_v t_{uvw}, v, w \in [1,k]$$

  It then creates the two parts of the CRS, CRS_p and CRS_v (the first is used by the prover, the second by the verifier) as follows:

$$CRS_p = \mathbf{A} \cdot \begin{bmatrix} D \\ RB^{-1} \end{bmatrix}$$

$$CRS_v = \begin{bmatrix} DB \\ R \\ -B \end{bmatrix} \cdot \mathbf{g}_2$$

- **Prover P**. Given a language candidate $\vec{\mathbf{z}} = \vec{x} \cdot \mathbf{A}$ with witness vector $\vec{x}$, the prover generates the k-element proof as $\vec{\mathbf{p}} = \vec{x} \cdot CRS_p$

– **Verifier V**. Given candidate $\vec{\mathbf{z}}$ and proof $\vec{\mathbf{p}}$, the verifier checks that the following k equations hold:

$$e\left([\vec{\mathbf{z}}|\vec{\mathbf{p}}], CRS_v\right) \stackrel{?}{=} 0_T^{1\times k}$$

5 Proof

Before we start proving that the system described in the previous section is indeed a QA-NIZK system, we need to define our security assumption, in this case, the k-linear assumption.

Definition 4 (k-linear assumption [Sha07,HK07]). *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 and has generators $\mathbf{g}_1, \ldots, \mathbf{g}_{k+1} \stackrel{\$}{\leftarrow} \mathbb{G}$, the k-linear asserts that it is computationally infeasible to distinguish between $(\mathbf{g}_1, \ldots, \mathbf{g}_{k+1}, x_1 \cdot \mathbf{g}_1, \ldots, x_{k+1} \cdot \mathbf{g}_{k+1})$ and $(\mathbf{g}_1, \ldots, \mathbf{g}_{k+1}, x_1 \cdot \mathbf{g}_1, \ldots, (x_1 + \cdots + x_k) \cdot \mathbf{g}_{k+1})$ for $x_1, \ldots, x_{k+1} \stackrel{\$}{\leftarrow} \mathbb{Z}_q$. More formally for all PPT adversaries A there exists a negligible function $\nu()$ such that*

$$\left| \begin{array}{c} Pr[(q, \mathbb{G}) \leftarrow \mathcal{G}(1^m); \mathbf{g}_1, \ldots, \mathbf{g}_{k+1} \stackrel{\$}{\leftarrow} \mathbb{G}; x_1, \ldots, x_{k+1} \stackrel{\$}{\leftarrow} \mathbb{Z}_q : \\ A(\mathbf{g}_1, \ldots, \mathbf{g}_{k+1}, x_1 \cdot \mathbf{g}_1, \ldots, x_{k+1} \cdot \mathbf{g}_{k+1}) = 1] - \\ Pr[(q, \mathbb{G}) \leftarrow \mathcal{G}(1^m); \mathbf{g}_1, \ldots, \mathbf{g}_{k+1} \stackrel{\$}{\leftarrow} \mathbb{G}; x_1, \ldots, x_{k+1} \stackrel{\$}{\leftarrow} \mathbb{Z}_q : \\ A(\mathbf{g}_1, \ldots, \mathbf{g}_{k+1}, x_1 \cdot \mathbf{g}_1, \ldots, (x_1 + \cdots + x_k) \cdot \mathbf{g}_{k+1}) = 1] \end{array} \right| < \nu(m)$$

Now we give the main proof ideas for the following theorem (for detailed proofs, especially for soundness, refer to [JR13b]).

Theorem 1. *[JR13b] The algorithms (K_0, K_1, P, V) described in the previous section 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 $\mathbb{G}_2$.*

5.1 Completeness

If $\vec{\mathbf{z}} = \vec{x} \cdot \mathbf{A}$ for some $\vec{x}$, then the left hand side of the verification equation becomes:

$$\begin{aligned} & e\left([\vec{\mathbf{z}}|\vec{\mathbf{p}}], CRS_v\right) = e\left([\vec{x} \cdot \mathbf{A}|\vec{\mathbf{p}}], CRS_v\right) \\ & = e\left(\vec{x} \cdot \mathbf{A} \cdot \left[I^{n\times n} \middle| \begin{matrix} D \\ RB^{-1} \end{matrix}\right] \cdot \begin{bmatrix} DB \\ R \\ -B \end{bmatrix}, \mathbf{g}_2\right) \\ & = e\left(\vec{x} \cdot \mathbf{A} \cdot \left(\begin{bmatrix} DB \\ R \end{bmatrix} - \begin{bmatrix} D \\ RB^{-1} \end{bmatrix} \cdot B\right), \mathbf{g}_2\right) = e(0_1^{1\times k}, \mathbf{g}_2) = 0_T^{1\times k}, \end{aligned}$$

which proves completeness.

5.2 Zero Knowledge

The CRS is generated as usual, but the simulator retains as a trapdoor the matrix $\begin{bmatrix} D \\ RB^{-1} \end{bmatrix}$. Then given a language candidate $\vec{\mathbf{z}}$, it generates the proof as $\vec{\mathbf{p}} = \vec{\mathbf{z}} \cdot \begin{bmatrix} D \\ RB^{-1} \end{bmatrix}$. If $\vec{\mathbf{z}} = \vec{x} \cdot \mathbf{A}$ for some $\vec{x}$, then this is equal to the proof the prover would generate, and hence the simulated proofs of language members are distributed identically to the real world, giving us perfect Zero Knowledge.

5.3 Soundness

The soundness proof is by far the most complicated part of the proof for this system, and hence we will only be giving an intuition of the proof here. For the full proof, see [JR13b]. The proof uses null-spaces of the language and a so-called switching lemma, also introduced in [JR13b], that allows the proof to be compressed to constant size.

Lemma 2 (Switching lemma [JR13b]). *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*

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

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

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

Soundness is proved by transforming the standard soundness game over a sequence of games, and showing that in one case, the probability of the adversary winning can be bounded by the switching lemma, and in the other case, the adversary winning would be equivalent to breaking the k-linear assumption.

The first game, $\mathbf{G}_0$, is just the standard soundness game: adversary $\mathcal{A}$ wins if it can break soundness, i.e., if it can produce a "proof" $\vec{\mathbf{p}}$ such that $e\left([\vec{\mathbf{z}}|\vec{\mathbf{p}}], CRS_v\right) = 0_T^{1\times k}$, but $\vec{\mathbf{z}}$ does not belong into the language $L_{\mathbf{A}}$.

In the next game, $\mathbf{G}_1$, the CRS generator is additionally given the witness A of language parameter $\mathbf{A}$. This can be done efficiently and without changing the distribution due to the efficiently witness-samplable property. Then, the null-space of A is used in generating the CRS: since A is $t \times (t+s)$ rank t matrix (due to robustness), there exists a rank s matrix $\begin{bmatrix} W^{t\times s} \\ I^{s\times s} \end{bmatrix}$, whose columns form

a complete basis for the null-space of A. Matrices R and B are generated as in the real CRS, and additionally, matrix $D'^{t\times k}$ with elements chosen randomly from $\mathbb{Z}_q$ is generated and matrix D is considered to be set to $D = D' + WRB^{-1}$. Then

$$CRS_p = \mathbf{A} \cdot \begin{bmatrix} D \\ RB^{-1} \end{bmatrix} = \mathbf{A} \cdot \left(\begin{bmatrix} D' \\ 0^{s\times k} \end{bmatrix} + \begin{bmatrix} W \\ I^{s\times s} \end{bmatrix} \cdot RB^{-1} \right) = \mathbf{A} \cdot \begin{bmatrix} D' \\ 0^{s\times k} \end{bmatrix}$$

$$CRS_v = \begin{bmatrix} DB \\ R \\ -B \end{bmatrix} \cdot \mathbf{g}_2 = \begin{bmatrix} D'B + WR \\ R \\ -B \end{bmatrix} \cdot \mathbf{g}_2$$

Note that D is distributed identically to the previous game, and the rest of the computations are the same, hence these two games are statistically indistinguishable and therefore the advantage of the adversary remains the same as in the previous game.

Now suppose that $\mathcal{A}$ wins $\mathbf{G}_1$. Partition matrix A as $\left[A_0^{t\times t} | A_1^{t\times s}\right]$ and the candidate vector $\vec{\mathbf{z}}$ as $\left[\vec{\mathbf{z}}_0^{1\times t} | \vec{\mathbf{z}}_1^{1\times s}\right]$. Since A_0 has rank t, $\vec{\mathbf{z}}_0$ can be extended to an unique vector $\vec{\mathbf{z}}'$ which is a member of $L_{\mathbf{A}}$ and can be computed as $\vec{\mathbf{z}}' = [\vec{\mathbf{z}}_0 | -\vec{\mathbf{z}}_0 \cdot W]$, where $W = -A_0^{-1}A_1$. The proof of $\vec{\mathbf{z}}'$ can be computed as $\vec{\mathbf{p}}' = \vec{\mathbf{z}}_0 \cdot D'$. Since both $(\vec{\mathbf{z}}, \vec{\mathbf{p}})$ (since $\mathcal{A}$ wins $\mathbf{G}_1$) and $(\vec{\mathbf{z}}', \vec{\mathbf{p}}')$ (by construction) pass the verification test, we obtain $(\vec{\mathbf{z}}'_1 - \vec{\mathbf{z}}_1) \cdot R = (\vec{\mathbf{p}}' - \vec{\mathbf{p}}) \cdot B$, where $\vec{\mathbf{z}}'_1 = -\vec{\mathbf{z}}_0 \cdot W$. This gives us the following set of equalities: for all $w \in [1, k]$

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

This can be rearranged to:

$$\text{For all } w \in [1,k] : \sum_{u=1}^{k} \sum_{v=1}^{k} \left[t_{uvw} \left(\sum_{i=1}^{s} [(\vec{\mathbf{z}}'_{1i} - \vec{\mathbf{z}}_{1i}) \cdot r_{iu}] - (\vec{\mathbf{p}}'_v - \vec{\mathbf{p}_v}) \cdot b_v \right) \right] = 0_1.$$

Since $\vec{\mathbf{z}}$ is not in the language, there exists an $i \in [1, s]$ such that $\vec{\mathbf{z}}'_{1i} - \vec{\mathbf{z}}_{1i} \neq 0$. Now define the following event F:

$$\text{For some } u, v \in [1,k] : \sum_{i=1}^{s} [(\vec{\mathbf{z}}'_{1i} - \vec{\mathbf{z}}_{1i}) \cdot r_{iu}] - (\vec{\mathbf{p}}'_v - \vec{\mathbf{p}_v}) \cdot b_v \neq 0.$$

We say that $\mathcal{A}$ wins game $\mathbf{G}_2$ if $\mathcal{A}$ wins $\mathbf{G}_1$ and event F does not occur. It is possible to show that using the switching lemma on the t values and some information-theoretic arguments that the probability that $\mathcal{A}$ wins $\mathbf{G}_1$ and event F occurs is negligible, hence the probability of $\mathcal{A}$ winning $\mathbf{G}_2$ is negligibly close to the probability of $\mathcal{A}$ winning $\mathbf{G}_1$. Now define event E as follows:

$$\text{For some } u \in [1,k] : \sum_{i=1}^{s} [(\vec{\mathbf{z}}'_{1i} - \vec{\mathbf{z}}_{1i}) \cdot r_{iu}] \neq 0.$$

It is possible to show that the probability of $\mathcal{A}$ winning $\mathbf{G}_2$ and event E occurring is bounded above by the advantage of the adversary in the k-linear assumption.

We say that $\mathcal{A}$ wins game $\mathbf{G}_3$ if it wins $\mathbf{G}_2$ and event E does not occur. Using the switching lemma on the r values and some information-theoretic arguments, it is possible to show that the probability of $\mathcal{A}$ winning the game $\mathbf{G}_3$ is negligible. Hence, under the k-linear assumption, soundness holds.

6 Conclusion

In this report we gave an overview of a Quasi-Adaptive NIZK proof system with constant-sized proofs for linear subspaces. For future work, it would be interesting to see how well this system can be used with different existing cryptographic protocols that use NIZK proofs (the authors of [JR13a] give quite a few samples, but there are probably a lot more places that it could be used).

References

[GS08] J. Groth,A. Sahai *Efficient non-interactive proof systems for bilinear groups*, EUROCRYPT 2008, volume 4965 of Lecture Notes in Computer Science, pages 415-432, 2008

[HK07] D. Hofheinz, E. Kiltz. *Secure hybrid encryption from weakened key encapsulation*, Advances in Cryptology - CRYPTO 2007, volume 4622 of Lecture Notes in Computer Science, pages 553-571, 2007

[JR13a] C. S. Jutla, A.Roy *Shorter Quasi-Adaptive NIZK Proofs for Linear Subspaces*, ASIACRYPT 2013, vol. 8269 of Lecture Notes in Computer Schience, pages 1-20, 2013

[JR13b] C.S Jutla, A.Roy *Switching Lemma for Bilinear Tests and Constant-size NIZK Proofs for Linear Subspaces*, Cryptology ePrint Archive, Report 2013/670, viewed on 30.04.14

[Sha07] H. Shacham *A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants*, Cryptology ePrint Archive, Report 2007/074, viewed on 30.04.14

[WIKI] *Rank-nullity theorem*, second proof, http://en.wikipedia.org/wiki/Rank%E2%80%93nullity_theorem#Proofs, viewed on 20.05.14