Efficient NIZK for NP without Knowledge Assumptions

Alonso González[1]

Mi casita

Abstract. Insert abstract here.

1 Introduction

In this work we construct a NIZK proof system for the language

$$\mathsf{CircuitSat} := \left\{ C : \exists \boldsymbol{x} \in \mathbb{Z}_p^m \text{ s.t. } C \text{ is an algebraic circuit and } C(\boldsymbol{x}) = 1 \right\},$$

with proof size $\kappa + \Theta(\text{depth}(C))$ elements of a bilinear group, where κ is the size of a proof of knowledge of $\boldsymbol{x}$. In the case of binary circuits, i.e. $p = 2$, we have that $\kappa = 2|\boldsymbol{x}| + O(1)$ using the techniques of [?]. In general, κ sould be independent from the circuit.

We organize the circuit gates by level, where level ℓ is formed by the gates at distance ℓ from the output gate. For example, the d-th level, where $d := \text{depth}(C)$, contain the gates whose inputs are only elements from the circuit input $\boldsymbol{x}$ and the 0-th level contains the unique gate whose output is the output of the circuit.

To each gate we might associate a vector of degree 2 polynomials $\boldsymbol{p}_\ell \in \mathbb{Z}_q^{n_\ell}[W_1, \ldots, W_{m_\ell}]$, where $m_\ell \in \mathbb{N}$ is the number of inputs of level ℓ and $n_\ell \in \mathbb{N}$ is the number of outputs (or, equivalently the number of gates) of level ℓ. Note that it must hold that $\sum_{i<\ell} n_i \geq m_\ell \geq n_{\ell-1}$ (TODO: Check this). It must hold that for every $\boldsymbol{x} \in \mathbb{Z}_p^m$

$$C(\boldsymbol{x}) = (\boldsymbol{p}_d \circ \boldsymbol{p}_{d-1} \circ \ldots \circ \boldsymbol{p}_0)(\boldsymbol{x}) \text{ TODO: I need to add id gates}$$

We work on asymmetric bilinear groups and our construction is built from the following primitives:

1. A commitment scheme for vectors in $\mathbb{Z}_q^m$ for wich we can construct a NIZK argument of knowledge of the opening.
2. A commitment scheme for vectors in $\mathbb{Z}_q^m$ with constant-size commitments in $\mathbb{G}_s^k$, $s = 1, 2$, for which we can construct a NIZK argument for the following language

$$\mathcal{L}_{\mathsf{prod},ck_1,ck_2} = \left\{ [\boldsymbol{a}]_1, [\boldsymbol{b}]_2, [\boldsymbol{c}]_1 : \begin{array}{c} [\boldsymbol{a}]_1 = \mathsf{Com}_{ck_1}(\boldsymbol{x}) \text{ and } [\boldsymbol{b}]_2 = \mathsf{Com}_{ck_2}(\boldsymbol{y}) \\ \Longrightarrow [\boldsymbol{c}]_1 = \mathsf{Com}_{ck_3}(\boldsymbol{x} \otimes \boldsymbol{y}) \end{array} \right\},$$

where $\boldsymbol{x} \in \mathbb{Z}_q^m, \boldsymbol{y} \in \mathbb{Z}_q^n, \boldsymbol{x} \otimes \boldsymbol{y} \in \mathbb{Z}_q^{mn}$, $ck_3 = ck_1 \otimes ck_2$, and $\otimes$ denote the kroenecker product.

3. A QA-NIZK argument for the language

$$\mathcal{L} = \left\{ [\boldsymbol{c}]_1, [\boldsymbol{c}']_1 : \begin{array}{l} \text{knowledge of } \boldsymbol{x} \text{ s.t. } [\boldsymbol{c}]_1 = \mathsf{Com}_{ck_1 \otimes ck_2}(\boldsymbol{x}) \Longrightarrow \\ [\boldsymbol{c}']_1 = \mathsf{Com}_{ck'}(\boldsymbol{x}) \end{array} \right\},$$

4. A QA-NIZK argument for the language

$$\mathcal{L} = \left\{ [\boldsymbol{c}]_1, [\boldsymbol{a}']_1, [\boldsymbol{b}']_2 : \begin{array}{l} \text{knowledge of } \boldsymbol{x} \text{ s.t. } [\boldsymbol{c}]_1 = \mathsf{Com}_{ck}(\boldsymbol{x}) \\ \Longrightarrow [\boldsymbol{a}']_1 = \mathsf{Com}_{ck_1}(\boldsymbol{\Gamma}_1 \boldsymbol{x}) \text{ and } [\boldsymbol{b}']_2 = \mathsf{Com}_{ck_2}(\boldsymbol{\Gamma}_2 \boldsymbol{x}) \end{array} \right\},$$

Constant-Size Multiplicative Homomorphic Commitments. Both Groth-Sahai and Pedersen commitments are special cases of the following general commitment scheme

$$ck := [\mathbf{G}]_s = [\mathbf{G}_0|\mathbf{G}_1] \in \mathbb{G}_s^{k\times(n+r)}, \quad \mathsf{Com}_{ck}(\boldsymbol{x};\boldsymbol{\rho}) = [\mathbf{G}_0]_s\boldsymbol{x} + [\mathbf{G}_1]_s\boldsymbol{\rho}.$$

Groth-Sahai commitments correspond to the case $k = n + r$, which defines perfectly binding commitments if $\mathbf{G}$ is invertible, and Pedersen commitments correspond to the case $k = 1$, which defines perfectly hiding commitments. We will consider the case $k > 1$ which has been called *somewhere statiscally binding* commitments and is a mixture between Groth-Sahai and Pedersen commitments.

With this formulation is easy to derive commitments to $\boldsymbol{x} \otimes \boldsymbol{y}$ from commitments to $\boldsymbol{x} \in \mathbb{Z}_q^m$ and $\boldsymbol{y} \in \mathbb{Z}_q^n$, as follows

$$\mathsf{Com}_{ck_3}(\boldsymbol{x} \otimes \boldsymbol{y}; \boldsymbol{\rho}_3) := \mathsf{Com}_{ck_1}(\boldsymbol{x}; \boldsymbol{\rho}_1) \otimes \mathsf{Com}_{ck_2}(\boldsymbol{y}; \boldsymbol{\rho}_2),$$

where $ck_2 := [\mathbf{H}_0|\mathbf{H}_2]_1, ck_3 = [\mathbf{G} \otimes \mathbf{H}]_T$ and

$$\boldsymbol{\rho}_3 = \begin{pmatrix} \mathbf{0}_m \\ \boldsymbol{\rho}_1 \end{pmatrix} \otimes \begin{pmatrix} \boldsymbol{y} \\ \frac{1}{2}\boldsymbol{\rho}_2 \end{pmatrix} + \begin{pmatrix} \boldsymbol{x} \\ \frac{1}{2}\boldsymbol{\rho}_1 \end{pmatrix} \otimes \begin{pmatrix} \mathbf{0}_n \\ \boldsymbol{\rho}_2 \end{pmatrix}$$

($\boldsymbol{\rho_3}$ has a different form?).

This approach has the disadvantage that once we compute $[\boldsymbol{c}]_T = \mathsf{Com}_{ck_3}(\boldsymbol{x} \otimes \boldsymbol{y})$ we are stucked in the target group and no more multiplications are possible. But one can still *bootstrap* commitment $[\boldsymbol{c}]_T$ (in some analogy with FHE techniques, when one bootstraps for diminishing the error) by bringing it to one of the base groups $\mathbb{G}_s$ and requiring the verifier to check that

$$e([\boldsymbol{a}]_1, [\boldsymbol{b}]_2) = e([\boldsymbol{c}]_s, [\mathbf{I}]_{2-s+1}).$$

Going a step forward, we will have to give two shares of $[\boldsymbol{c}]_s$, $[\boldsymbol{c}']_1$ and $[\boldsymbol{d}']_2$, such that $\boldsymbol{c} = \boldsymbol{c}' + \boldsymbol{d}'$. We omit the "primes" in the shares and now the verifier checks that

$$e([\boldsymbol{a}]_1, [\boldsymbol{b}]_2) = e([\boldsymbol{c}]_1, [\mathbf{I}]_2) + e([\mathbf{I}]_1, [\boldsymbol{d}]_2).$$

The first share is computed using commitment key $ck_{3,1} := [\mathbf{G} \otimes \mathbf{H} - \mathbf{Z}]_1$ and the second share is computed using commitment key $ck_{3,1} := [\mathbf{Z}]_2$, for $\mathbf{Z} \leftarrow \mathbb{Z}_q^{k_1k_2\times mn}$.

Arguments of Equal Opening. Given $[\boldsymbol{c}]_1 = \mathsf{Com}_{ck}(\boldsymbol{x}; \boldsymbol{\rho})$, where $ck = ck_1 \otimes ck_2$, we want to show that $[\boldsymbol{c}']_1$ can be also oppened to $\boldsymbol{x}$ but ck' is a random commitment key.

To do so we will give a QA-NIZK argument that $\boldsymbol{c}/\boldsymbol{c}'$ is in the linear span of

$$\mathbf{J} := \begin{pmatrix} \mathbf{G}_0 \otimes \mathbf{H}_0 & \mathbf{G}_0 \otimes \mathbf{H}_1 & \mathbf{G}_1 \otimes \mathbf{H}_0 & \mathbf{G}_1 \otimes \mathbf{H}_1 & \mathbf{0} \\ \mathbf{G}'_0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{G}'_0 \end{pmatrix}$$

However, the QA-NIZK argument only shows the existence of some $\boldsymbol{w}$ such that $\boldsymbol{c}/\boldsymbol{c}' = \mathbf{J}\boldsymbol{w}$ but it might be the case that $\boldsymbol{c}'$ still can't be oppened to $\boldsymbol{x}$ — i.e. $\boldsymbol{w}$ can't be $\boldsymbol{x}$ appended with some other vector. We will show that this is not the case.

Assume that $[\boldsymbol{c}]_1 = \mathsf{Com}_{ck}(\boldsymbol{x}; \boldsymbol{\rho})$ but $[\boldsymbol{c}']_1 \neq \mathsf{Com}_{ck'}(\boldsymbol{x}; \boldsymbol{\rho}')$ for any $\boldsymbol{\rho}'$, and assume also that the adversary provides a valid proof $[\pi]_1$ for $[\boldsymbol{c}]/[\boldsymbol{c}']_1$. Define $[\boldsymbol{c}^\dagger]_1 := \mathsf{Com}_{ck'}(\boldsymbol{x}; \mathbf{0})$ and note that $\boldsymbol{c}/\boldsymbol{c}^\dagger$ is in the immage of $\mathbf{J}$ and thus we can compute a proof $[\pi^\dagger]_1$ for $[\boldsymbol{c}]/[\boldsymbol{c}^\dagger]_1$. By the properties of the QA-NIZK arguments for linear spaces, we get that $[\pi - \pi^\dagger]_1$ is a proof for $[0]_1/[\boldsymbol{d}]_1$, where $\boldsymbol{d} = \boldsymbol{c} - \boldsymbol{c}^\dagger \neq \mathbf{0}$. We will show that $\mathbf{0}/\boldsymbol{d}$ is not in the immage of $\mathbf{J}'$, such that $[\mathbf{J}']_1$ is computationally indistinguishable from $[\mathbf{J}]_1$.

Let $\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{u}'_0, \boldsymbol{u}'_1$ randomly chosen from $\mathbb{Z}_q^k$. We compute $\mathbf{J}'$ in the same way that $\mathbf{J}$ is computed, but now ck_1, ck_2 and ck' are computed as follows

$$\begin{aligned} ck_1 &= [\mathbf{G}_0|\mathbf{G}_1]_1 = [\boldsymbol{u}_0\mathbf{A}_0|\boldsymbol{u}_1\mathbf{A}_1]_1 \\ ck_2 &= [\mathbf{H}_0|\mathbf{H}_1]_2 = [\boldsymbol{v}_0\mathbf{B}_0|\boldsymbol{v}_1\mathbf{B}_1]_2 \\ ck' &= [\mathbf{G}'_0|\mathbf{G}'_1]_1 = [\boldsymbol{u}'_0\mathbf{A}_0 \otimes \mathbf{B}_0 + \boldsymbol{u}_1\mathbf{C}_0|\boldsymbol{u}_1\mathbf{C}_1]_1 \end{aligned} \tag{1}$$

since $[\boldsymbol{u}]_s\mu$, $\mu \leftarrow \mathbb{Z}_q$ is indistinguishable from a random element in $\mathbb{G}_s^k$ as long as the DDH assumption is hard in $\mathbb{G}_s$, it follows that the new commitment keys are indistinguishable from the original ones.

There is still a technical problem when using the DDH assumption and computing $[\mathbf{J}]_1$: when using the DDH assumption in $\mathbb{G}_2$ to change the distribution of ck_2 we can only compute $[\mathbf{J}]_2$. This problem has already arised and solved in [**?**] and we use a similar solution in our final proof system. For the sake of clarity, for this intuitive explanation we just assume that ck_1, ck_2 and ck' are sampled from (1) in the real game (although this will make impossible to prove zero-knowledge).

Going back to the problem of whether $\mathbf{0}/\boldsymbol{d}$ is in the immage of $\mathbf{J}$, we get that now this is not the case. Indeed,