On the Impossibility of Algebraic NIZK In Pairing-Free Groups

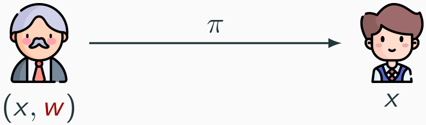
Emanuele Giunta[1,2]

1. IMDEA Software Institute, Madrid, Spain.

2. Universidad Politecnica de Madrid, Spain.

Non-Interactive Zero-Knowledge Arguments

$\mathcal{R}$ an NP relation, $(x, w) \in \mathcal{R}$



Completeness

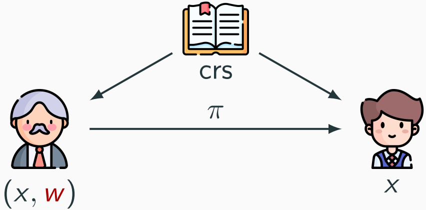
Soundness

Zero-Knowledge

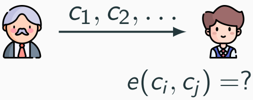
Proof of Knowledge

Requires the **random oracle** or a **trusted setup** (CRS).

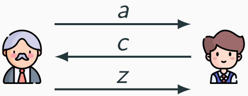
NIZK in the CRS model



Pairing Equations
[GS12]



Correlation-Intractable Hash Functions [CGH04]



NIZK from Prime-Order Groups

Groth-Sahai Proofs [GS12]

- ✅ Uses the group **black-box**
- ❌ Requires **pairings**

Jain-Jin CIHF [JJ21]
from sub-exponential DDH

- ❌ Non **black-box** group usage
- ✅ Does not require **pairings**

$\mathcal{Q}$ Do best of both worlds NIZKs exists?

NIZK from Prime-Order Groups

Groth-Sahai Proofs [GS12]

- ✓ Uses the group **black-box**
- ✗ Requires **pairings**

Jain-Jin CIHF [JJ21]
from sub-exponential DDH

- ✗ Non **black-box** group usage
- ✓ Does not require **pairings**

What does black-box mean?

$\mathcal{Q}$ Do best of both worlds NIZKs exists?

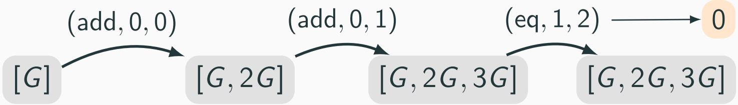
Maurer's Generic Group Model [Mau05]

$(\mathbb{G}, +)$ is modeled as an **oracle machine** with a list of group elements V.

- Initially $V = [G]$
- (add, i, j): append $V[i] + V[j]$ to V
- (eq, i, j): return $V[i] == V[j]$.

$(\mathbb{G}, +)$ is modeled as an **oracle machine** with a list of group elements V.

- Initially $V = [G]$
- (add, i, j): append $V[i] + V[j]$ to V
- (eq, i, j): return $V[i] == V[j]$.



Unlike **Shoup's** model, elements have no (random) representation.

Our Result

We show that these primitives are impossible in Maurer's GGM:

NIZK-AoK for the preimage relation for **one-way functions**.

$\mathcal{R} = \{(x, w) \;:\; f(w) = x\}$

- Discrete Logarithm
- "Powers of τ" $(g^{\tau^i})_{i=1}^{n}$

Our Result

We show that these primitives are impossible in Maurer's GGM:

NIZK-AoK for the preimage relation for **one-way functions**.

$\mathcal{R} = \{(x, w) \ : \ f(w) = x\}$

- Discrete Logarithm
- "Powers of τ" $(g^{\tau^i})_{i=1}^{n}$

NIZK for **hard subset membership** problems.

$x \leftarrow \mathcal{L}, \ z \leftarrow \overline{\mathcal{L}} \quad : \quad x \approx_c z$

- Decisional Diffie-Helman
- MDDH, DLin

Our Result

We show that these primitives are impossible in Maurer's GGM:

NIZK-AoK for the preimage relation for **one-way functions**.

$\mathcal{R} = \{(x, w) \ : \ f(w) = x\}$

- Discrete Logarithm
- "Powers of τ" $(g^{\tau^i})_{i=1}^n$

NIZK for **hard subset membership** problems.

$x \leftarrow \mathcal{L}, \ z \leftarrow \overline{\mathcal{L}} \ \ : \ \ x \approx_c z$

- Decisional Diffie-Helman
- MDDH, DLin

. . . secure against an **unbounded** adversary with **polynomial** GGM queries (**GPPT**).

How to Circumvent our Result?

Using group elements representation

(Hashing, Padding)

Using more structure

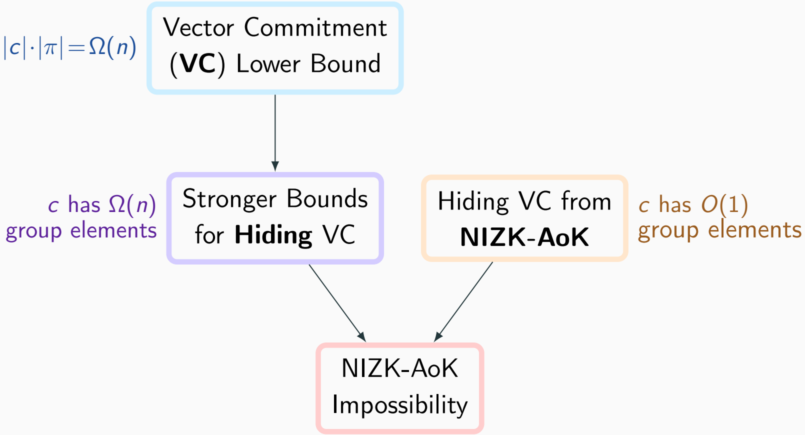
(Pairing, Unknown order)

Using external hardness assumptions

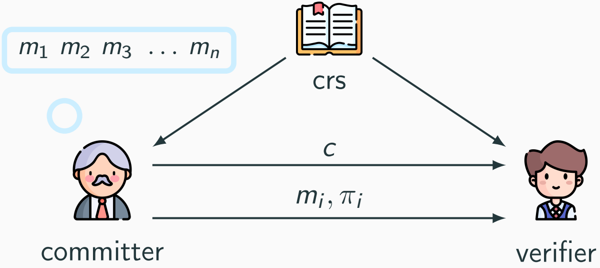
(RSA, LWE, iO)

NIZK-AoK Impossibility

Overview


$|c| \cdot |\pi| = \Omega(n)$
Vector Commitment (**VC**) Lower Bound
c has $\Omega(n)$ group elements
Stronger Bounds for **Hiding** VC
Hiding VC from **NIZK-AoK**
c has $O(1)$ group elements
NIZK-AoK Impossibility

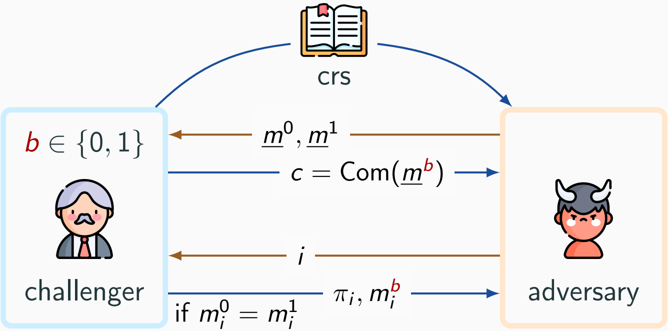
Algebraic VC Lower Bounds [CFGG22]



Position Binding: Computing two openings for position i is hard.

[CFGG22]: In Maurer's GGM, $|c| \cdot |\pi_i| = \Omega(n)$.

Algebraic Hiding VC Lower Bound



Improved Bound: For any VC in Maurer's GGM

Hiding + Position Binding $\Rightarrow$ c contains $\geq n$ group elements.

Hiding VC from NIZK-AoK (DLog)

Let $h : \mathbb{F}_q \to \{0, 1\}$ be an hard-core predicate for DLog
I.e. $h(x)$ is hard to guess given only g^x.

$$\textbf{CRS} = g_1, \ldots, g_n \qquad \text{Uniformly Sampled}$$

$$\textbf{Com}(b_1, \ldots, b_n) = \prod_{i=1}^{n} g_i^{x_i} \qquad h(x_i) = b_i$$

$$\textbf{Open}(b_i) = x_i,\ (g^{x_j}, \pi_j)_{j \neq i} \qquad \text{AoK for } x_j$$

- The commitment only contains 1 group element!

Hiding VC from NIZK-AoK (OWF family)

$f_k : \{0,1\}^\mu \to \mathbb{G}^m$ OWF family, with key space $k \sim \mathbb{G}^\kappa$

$$\textbf{CRS} = \boxed{k_1, \ldots, k_n}$$

Uniformly Sampled

$$\textbf{Com}(b_1, \ldots, b_n) = \prod_{i=1}^{n} f_{k_i}(x_i), \ \boxed{r_1, \ldots, r_n}$$

$\langle x_i, r_i \rangle = b_i$

$$\textbf{Open}(b_i) = x_i, \ (f_{k_j}(x_j), \boxed{\pi_j})_{j \neq i}$$

AoK for x_j

Hiding VC from NIZK-AoK (OWF family)

$f_k : \{0,1\}^\mu \to \mathbb{G}^m$ OWF family, with key space $k \sim \mathbb{G}^\kappa$

$$\textbf{CRS} = k_1, \ldots, k_n$$

Uniformly Sampled

$$\textbf{Com}(b_1, \ldots, b_n) = \prod_{i=1}^{n} f_{k_i}(x_i),\ r_1, \ldots, r_n$$

$\langle x_i, r_i \rangle = b_i$

$$\textbf{Open}(b_i) = x_i,\ (f_{k_j}(x_j), \pi_j)_{j \neq i}$$

AoK for x_j

- [GL89]: $\langle x, r \rangle$ is an hardcore predicate for $F_k(x, r) = (f_k(x), r)$
- In GPPT time, $f_k(\cdot)$ can be restricted to be collision resistant
- The commitment only contains $O(1)$ group elements!

NIZK for hard subset membership
Impossibility

Overview

message space $|M| \geq |\mathsf{vk}|$

Signatures Impossibility
[DHH+21, CFGG22]

message space $|M| = 1$

Signatures from **NIZK** for
Hard Subset Membership

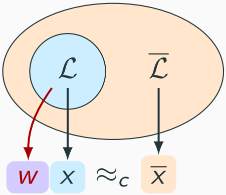
NIZK for HSMP
Impossibility

Hard Subset Membership Problems

Hard Subset Membership Problem

Can sample indistinguishably
from $\mathcal{L}$ (with a witness) and $\overline{\mathcal{L}}$.

Eg. **DDH**, **MDDH**, **DLin**.



Signatures from NIZK

Single element message space $M = \{0\}$.

$$\begin{aligned}
\textbf{crs} &= \boxed{x} \longleftarrow \boxed{\overline{\mathcal{L}}} && \text{False statement} \\
\textbf{vk} &= \boxed{\text{NIKZ.crs}} \longleftarrow \boxed{\mathcal{S}(1^\lambda)} && \text{Simulated crs} \\
\textbf{sk} &= \boxed{\text{td}} \\
\textbf{Sign}(0) &= \boxed{\pi} \longleftarrow \boxed{\mathcal{S}(\text{td}, x)} && \text{Simulated proof}
\end{aligned}$$

Correctness: $\mathcal{S}$ cannot tell x is false $\Rightarrow$ π is almost always correct.

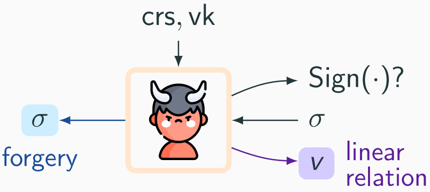
Signature Adversary [CFGG22]

Without loss of generality crs, vk are vectors of group elements.

Either:

- Finds a forgery σ
- Finds $v : \langle v, \mathsf{vk} \rangle = 0$.

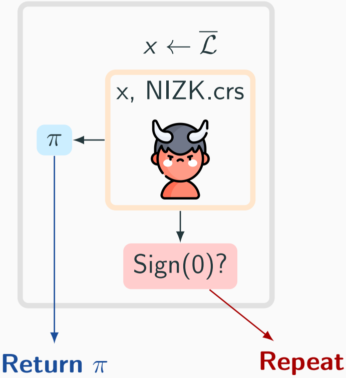
Fails with probability $\frac{1}{\mathsf{poly}(\lambda)}$



In our case $\mathsf{crs} = x \in \overline{\mathcal{L}}$ and $\mathsf{vk} = \mathsf{NIZK.crs}$

NIZK Adversary

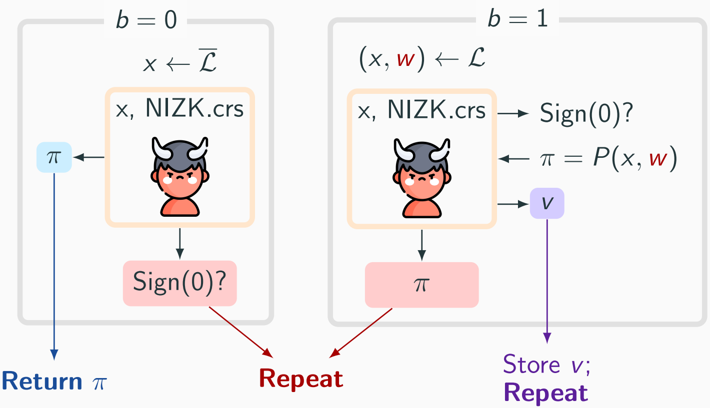
Initially get NIZK.crs



NIZK Adversary

Initially get NIZK.crs

$b \leftarrow \{0,1\}$



Conclusion

Conclusion & Open Questions

We proved that in **Maurer's GGM**, there exist **GPPT** adversaries breaking the security of any

- **NIZK-AoK** for the preimage relation of many OWF families,
- **NIZK** for hard subset membership problems.

Open questions:

- Can **witness hiding** be achieved?
- Do NIZK for non-trivial non-HSMP languages exists?

Thanks for your attention!