# New Straight-Line Extractable NIZKPs for Cryptographic Group Actions

Joint work with A. Flamini, E. Signorini, G. Tognolini

**Federico Pintore,** **University of Trento (IT)**

**Workshop on Cryptographic Tools for Blockchains (EC26) - Rome (IT) - 9/5/2026**

# Motivation

**Straight-line extractable NIZKPs** guarantee that behind a valid proof there exists an actual witness.

This feature is desirable in different scenarios, e.g. composable security for cross-chain bridges and zk-rollups.

**Cryptographic group actions** have proven to be flexible tools to construct (advanced) post-quantum primitives.

*Can they be used to build **compact** PQ straight-line extractable NIZKPs?*

# Straight-line extractable NIZKPs

A **NIZKP** (in the ROM) for a set of binary relations $\{R_\lambda \subset \mathsf{X}_\lambda \times \mathsf{W}_\lambda\}_{\lambda \in \mathbb{N}^*}$ is a pair of PPT algorithms ($\mathsf{Prove}^{\mathsf{RO}}$, $\mathsf{Verify}^{\mathsf{RO}}$).

The probability that $\mathsf{Prove}^{\mathsf{RO}}$ produces an invalid proof $\pi = \perp$ is denoted by $\epsilon_c^{\mathsf{Prove}}$ and called **completeness error**.

NIZKPs are required to be zero-knowledge.

**Straight-line extractability** requires the existence of a PPT algorithm Ext that, for any adversary $\mathscr{A}$, if $\mathscr{A}$ can generate a valid proof $\pi$ for a statement x, and Ext is given x, $\pi$ and all random-oracle queries made by $\mathscr{A}$, then Ext will be able to extract a witness for x with probability $\geq (1 - \epsilon_s^{\mathsf{Ext}})$

$\epsilon_s^{\mathsf{Ext}}$ is the **soundness error.**

# Generic transforms

NIZKPs are often obtained from **Sigma protocols** (see next slide) via **generic transforms**.

The most used is the Fiat-Shamir transform, but the NIZKPs it produces are generally not straight-line extractable.

Existing (generic) solutions:

- Pass transform
- Unruh transform
- Fischlin transform

# Generic transforms

NIZKPs are often obtained from **Sigma protocols** (see next slide) via **generic transforms**.

The most used is the Fiat-Shamir transform, but the NIZKPs it produces are generally not straight-line extractable.

Existing (generic) solutions:

- Pass transform
- Unruh transform

→ Proofs incur an overhead

- Fischlin transform

# A Sigma protocol $\Sigma_\star$ from group actions

Let $X$ be a set and $\mathbb{G}$ a group, both finite. A (left) **group action** of $\mathbb{G}$ on $X$ is a map $\star : \mathbb{G} \times X \to X$, $(g, x) \mapsto g \star x$ s.t. for all $x \in X$, $g_1, g_2 \in \mathbb{G}$, it holds $1_\mathbb{G} \star x = x$ and $g_2 \star (g_1 \star x) = g_2 g_1 \star x$.

**Prover**$(x = w \star x_0, w)$ **Verifier**$(x)$

$P_1$ $y \leftarrow \mathbb{G}$

$\text{com} = y \star x_0$

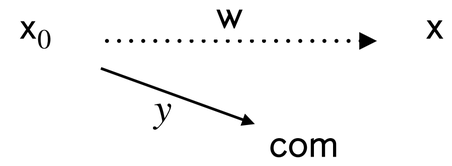
$P_2$ $\text{resp} = \begin{cases} y & \text{if ch} = 0 \\ y \cdot w^{-1} & \end{cases}$

ch

$\text{ch} \leftarrow \{0,1\}$ $V_1$

resp

$1/0 \leftarrow V_2(x, \text{com}, \text{ch}, \text{resp})$ $V_2$



# The fixed-weight technique

$\Sigma_\star$ is correct, honest-verifier zero-knowledge and 2-special sound, i.e. a dishonest prover has success probability $1/2$.

To make it negligibly small, $\Sigma_\star$ is repeated in parallel $t$ times. Let $\Sigma_\star^t$ be the new Sigma protocol.

In $\Sigma_\star$ when ch $= 0$, the response is an **unstructured object**, which can be replaced by a **random seed**.

To mitigate the response-size growth when moving from $\Sigma_\star$ to $\Sigma_\star^t$ , the repeated Sigma protocol $\Sigma_\star^t$ can be declined so that challenges in $\{0,1\}^t$ have a **fixed weight** $\rho$.

# Fischlin transform

Let ($\text{Prove}_{\text{Fi}}$, $\text{Verify}_{\text{Fi}}$) be the NIZKP deduced by applying the Fischlin transform to a given Sigma protocol.

$\text{Prove}_{\text{Fi}}(x, w)$ — with $(x, w) \in R$ — works as follows

1. it produces $r$ first messages $\text{com}_1, \ldots, \text{com}_r$
2. for **each** $i = 1, \ldots, r$ , it searches for a challenge $\text{ch}_i$ s.t. $\text{RO}(x, (\text{com}_1, \ldots, \text{com}_r), i, \text{ch}_i, \text{resp}_i)$ starts with $b$ zeros.

**First contribution**: the Fischlin transform does not work well with the fixed-weight technique (both on $\Sigma_\star$ and $\Sigma_\star^t$)

# The Group Action Oriented (GAO) transform

**Second contribution**: a straight-line extractable transform — GAO — for $\Sigma_\star$ (and similar Sigma protocols) which achieves fixed-weight proofs by construction.

Let $(\mathsf{Prove}_{\mathsf{GAO}}, \mathsf{Verify}_{\mathsf{GAO}})$ be the NIZKP deduced by applying the GAO transform.

$\mathsf{Prove}_{\mathsf{GAO}}(x, w)$ — with $(x, w) \in R$ — works as follows

1. it produces $L$ first messages $\mathsf{com}_1, \ldots, \mathsf{com}_L$
2. it searches for $\rho$ **first messages** for which $\mathsf{ch}_i \neq 0$ is s.t. $\mathsf{RO}(x, (\mathsf{com}_1, \ldots, \mathsf{com}_r), i, \mathsf{ch}_i, \mathsf{resp}_i)$ starts with $b$ zeros.
3. the remaining challenges are set to $0$

# Further optimisations

**Third contribution**: a **stretch-and-compress** optimisation that reduces the computational cost of GAO by exploiting the asymmetry between expansive commitment generation and cheap RO evaluation.

The idea is to sequentially repeat the GAO transform with different ROs, which allows to target a bigger completeness error within the single executions.

**Fourth contribution**: replacing the inversion predicate with a collision one (inspired by a work by Kondi and shelat).

# A concrete application

We evaluated the effectiveness of our transforms on the group-action-based PQ digital signature **LESS**.

**LESS** is a code-based proposal, which has been admitted to the second round of the NIST standardisation process.

It achieves near-optimal response size, i.e. approximately $2\lambda$ for non-compressed responses.

| **Transform** | $\ell$ | $\rho$ | $k$ | $b$ | $L$ | $\bar{Q}$ | CC | **sig (B)** |
|---|---|---|---|---|---|---|---|---|
| SC-GAO | 1 | 36 | 301 | 3.78 | 392 | 17.2K | 254M (×2.3) | 3233 (×1.2) |
| SC-GAO-Coll | | | 196 | 3.77 | 279 | 8K | 177M (×1.6) | 2977 (×1.1) |
| SC-GAO | 3 | 42 | 92 | 3.20 | 131 | 5.39K | 86M (×2.1) | 2529 (×1.4) |
| SC-GAO-Coll | | | 57 | 3.19 | 97 | 2.53K | 62.2M (×1.5) | 2241 (×1.2) |
| SC-GAO | 7 | 34 | 62 | 3.94 | 85 | 5.58K | 59.6M (×2.2) | 1905 (×1.4) |
| SC-GAO-Coll | | | 33 | 3.91 | 65 | 2.37K | 43.6M (×1.6) | 1649 (×1.2) |

In brackets, comparison with LESS level 1.

A. Flamini, F. Pintore, E. Signorini, G. Tognolini, *New Straight-Line Extractable NIZKPs for Cryptographic Group Actions*, Crypto 2026 (to appear).

**Federico Pintore,** Federico.pintore@unitn.it