PRIVACY-PRESERVING SIGNATURES FROM ISOGENIES

Federico Pintore

Department of Mathematics, University of Bari, IT

Joint work with Ward Beullens[1] and Schuichi Katsumata[2]

[1]imec-COSIC, BE

[2]National Institute of Advanced Industrial Science and Technology (AIST), JP

CrypTO Conference 2021 - May 26-27 2021 - Virtual

RING SIGNATURES

Introduced in 2001 by Rivest, Shamir, Tauman.

Proposed application: **whistleblowers**

Privacy-preserving cryptocurrencies: Dash, **Monero**, ZCash

The security of the ring signature used by Monero relies of the hardness of the DLP.

CALAMARI AND FALAFL

- A simple and efficient **generic construction** of OR-proofs from simple algebraic structure (i.e., "admissible" group actions).

- The OR-proof is converted into a **ring signature**, where the signature size scales **logarithmically in N,** better than previously known PQ schemes ($c \cdot 2\lambda \cdot \log_2 N$).

Calamari

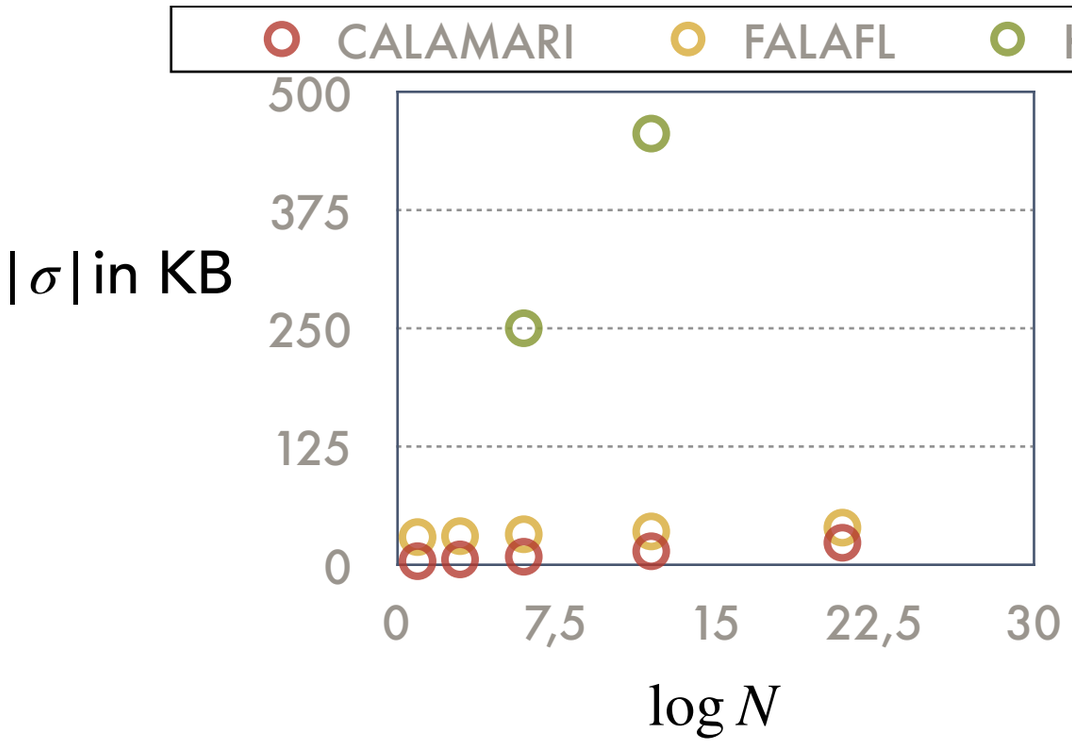
- **first** isogeny-based ring signature
- **smallest signatures** among PQ alternatives

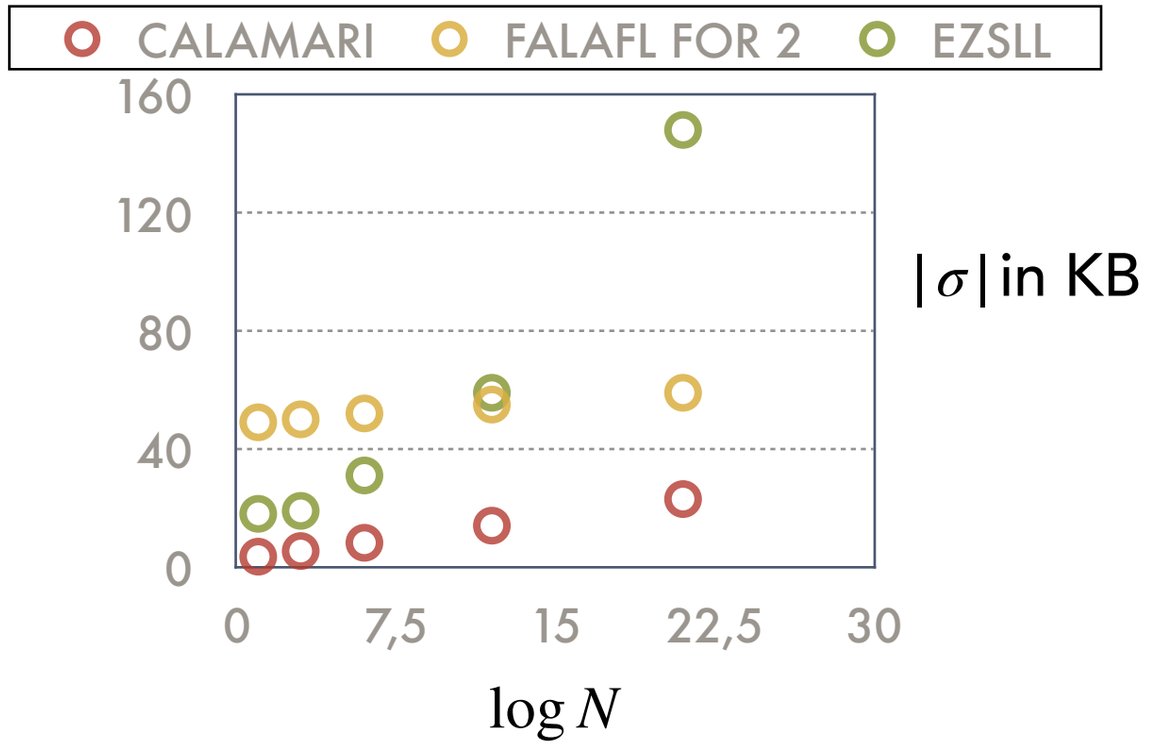
Falafl

- **fast** signing
- smaller signature size than lattice-based alternatives from $N \approx 1024$

POST-QUANTUM RING SIGNATURES

Ring signatures having size that scales logarithmically in N have been proposed only from **symmetric-key** primitives, and **lattice-based** assumptions.





- **Falafl:** $|\sigma| = 0.5 \log N + 29$ KB
- **Raptor:** $|\sigma| = 1.3\ N + 1.5$ KB

ROADMAP

1. OR-proofs

2. Admissible Group Actions

3. A new OR-Proof

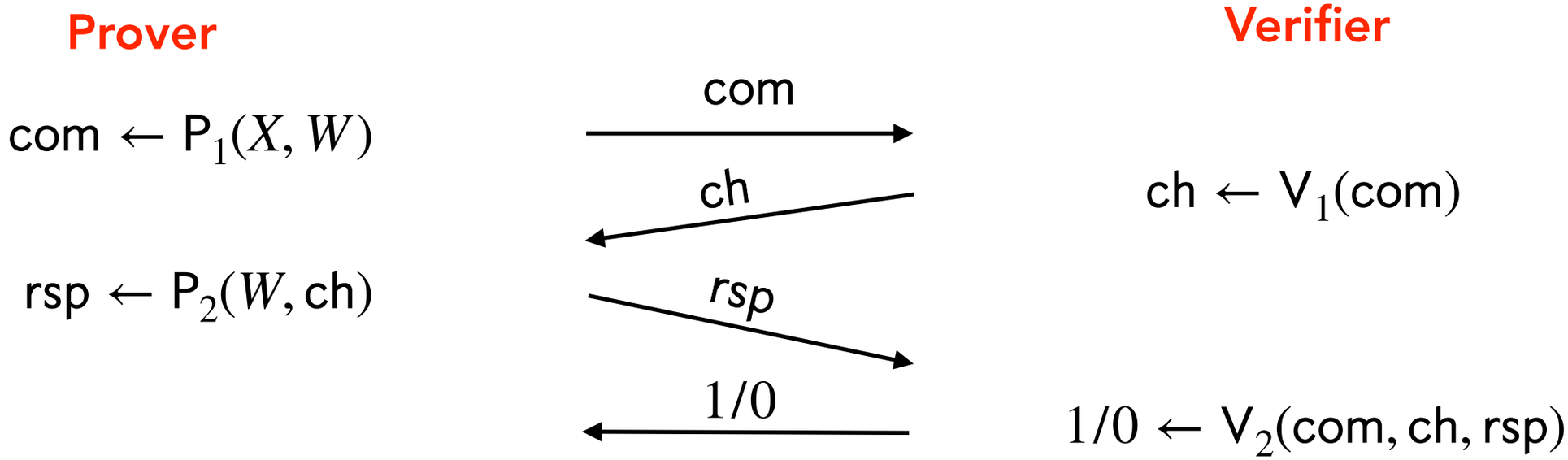
4. Calamari and Falafl

SIGMA PROTOCOLS

Let $R \subset X \times W$ be a binary relation. A sigma protocol

$$\Pi_\Sigma = (P = (P_1, P_2), V = (V_1, V_2))$$

for R is a **three-move interactive protocol** between a **prover** (holding a verification-secret key pair$(X, W) \in R$) and a **verifier** (holding X).



SIGMA PROTOCOLS

Let $R \subset X \times W$ be a binary relation. A sigma protocol

$$\Pi_\Sigma = (P = (P_1, P_2), V = (V_1, V_2))$$

for R is a **three-move interactive protocol** between a **prover** (holding a verification-secret key pair$(X, W) \in R$) and a **verifier** (holding X).

Required properties

- Correctness with abort
- **(Non-abort) Honest-Verifier Zero-Knowledge**
- Special Soundness
- …

OR-PROOFS & RING SIGNATURES

An **OR-Proof** for the binary relation $R \subset \mathsf{X} \times \mathsf{W}$ is a sigma protocol for

$$R_{\mathsf{OR}} = \{((X_1, \ldots, X_N), (W, I)) \,|\, N \in \mathbb{N}, I \in [N],\ (X_I, W) \in R\}$$

An OR-Proof, with negligibly-small soundness error, can be turned into a **ring signatures** by means of the Fiat-Shamir transform.

- $\mathsf{ch} = H(\mathsf{com}, \mathsf{R}, m)$
- $\sigma = (\mathsf{com}, \mathsf{ch}, \mathsf{rsp})$

ROADMAP

1. OR-proofs 

2. Admissible Group Actions

3. A new OR-Proof

4. Calamari and Falafl

ADMISSIBLE GROUP ACTIONS (AGAs)

A **AGA** with respect to $X_0 \in \mathrm{X}$ is a tuple $(\mathbb{G}, \mathrm{X}, S_1, S_2, \delta, D_{\mathrm{X}})$, where:

- $\mathbb{G}$ is a **group** and S_1, S_2 are **symmetric subsets** of $\mathbb{G}$ ($s \in S_i \Rightarrow -s \in S_i$);
- X is a **finite set**;
- $\delta \in [0,1]$;
- D_{X} is a distribution over a set of **group actions** $\star : \mathbb{G} \times \mathrm{X} \to \mathrm{X}.$

$$(g, X) \mapsto g \star X$$

  - $0_G \star X = X$;
  - $g_1 \star (g_2 \star X) = (g_1 + g_2) \star X$

ADMISSIBLE GROUP ACTIONS (AGAs)

A **AGA** with respect to $X_0 \in \mathrm{X}$ is a tuple $(\mathbb{G}, \mathrm{X}, S_1, S_2, \delta, D_{\mathrm{X}})$, where:

- $\mathbb{G}$ is a **group** and S_1, S_2 are **symmetric subsets** of $\mathbb{G}$ ($s \in S_i \Rightarrow -s \in S_i$);
- X is a **finite set**;
- $\delta \in [0,1]$;
- D_{X} is a distribution over a set of **group actions** $\star : \mathbb{G} \times \mathrm{X} \to \mathrm{X}$.

For the set $S_3 = \cap_{g \in S_1} \{S_2 + g\}$, it holds $|S_3| = \delta \cdot |S_2|$.

Given $X = g \star X_0$, with g sampled uniformly in S_1, it is **hard to find** g.

Example (DHKE on a group $\mathbb{H}$): $\mathrm{X} = \mathbb{H}^*$, $\mathbb{G} = S_1 = S_2 = \mathbb{Z}_q^*$, $\delta = 1$, $\star = exp$

NOTATION

Given an **AGA** $(\mathbb{G}, \mathsf{X}, S_1, S_2, \delta, D_{\mathsf{X}})$ with respect to $X_0 \in \mathsf{X}$ we denote:

- $|g|$ = bits to represent $g \in \mathbb{G}$;
- x = bits to represent $X \in \mathsf{X}$.

The size of a transcript (com, ch, rsp) is denote by $|\mathsf{trans}|$.

The size of a ring signature is denote by $|\sigma|$.

ROADMAP

1. OR-proofs 

2. Admissible Group Actions 

3. A new OR-Proof

4. Calamari and Falafl

CONSTRUCTING AN OR-PROOF FOR AGAs - N=1

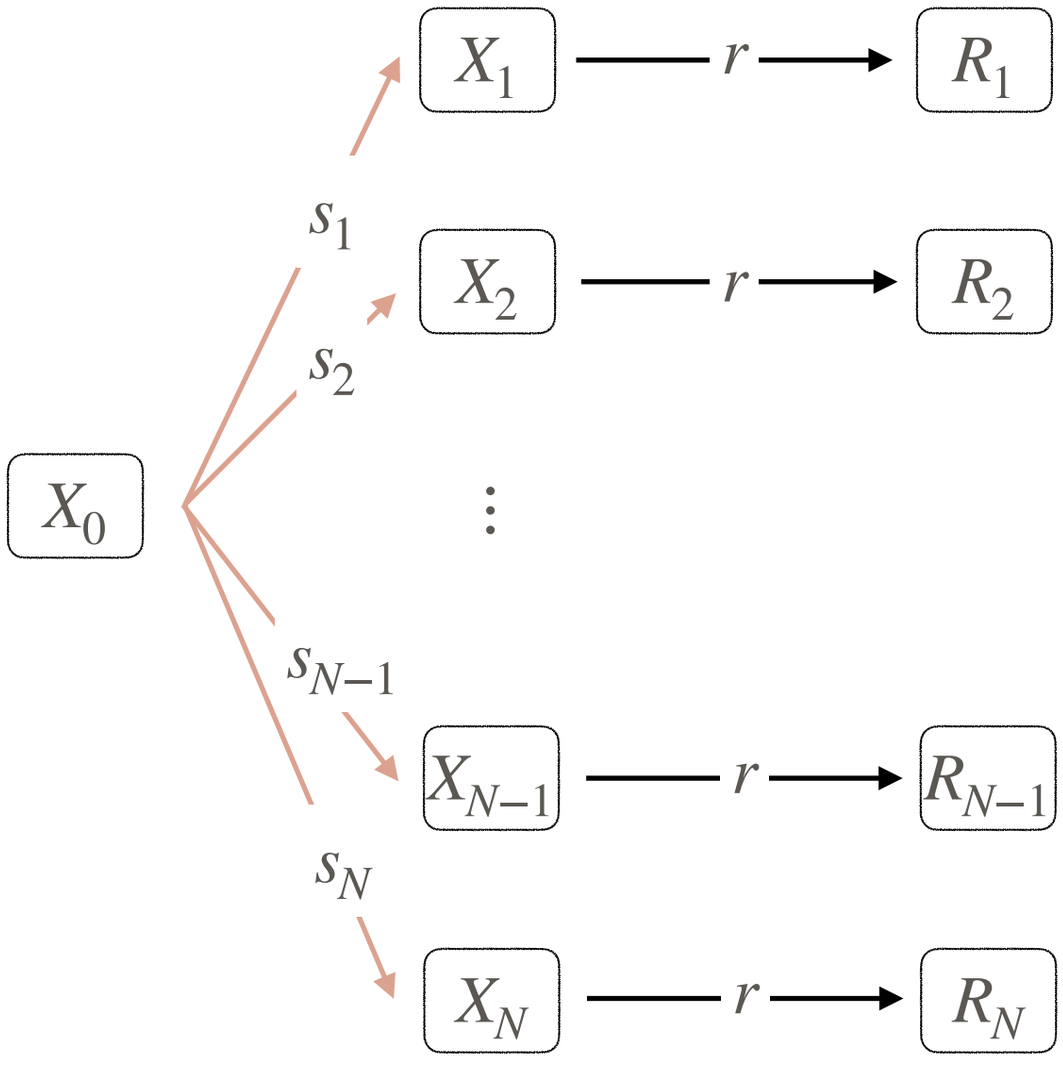
$\text{com} = R$

$\text{rsp}_0 = r + s$

$\text{rsp}_1 = r$

$$R = \{(X, s) \,|\, s \in S_1, X \in \mathsf{X}, X = s \star X_0\}$$

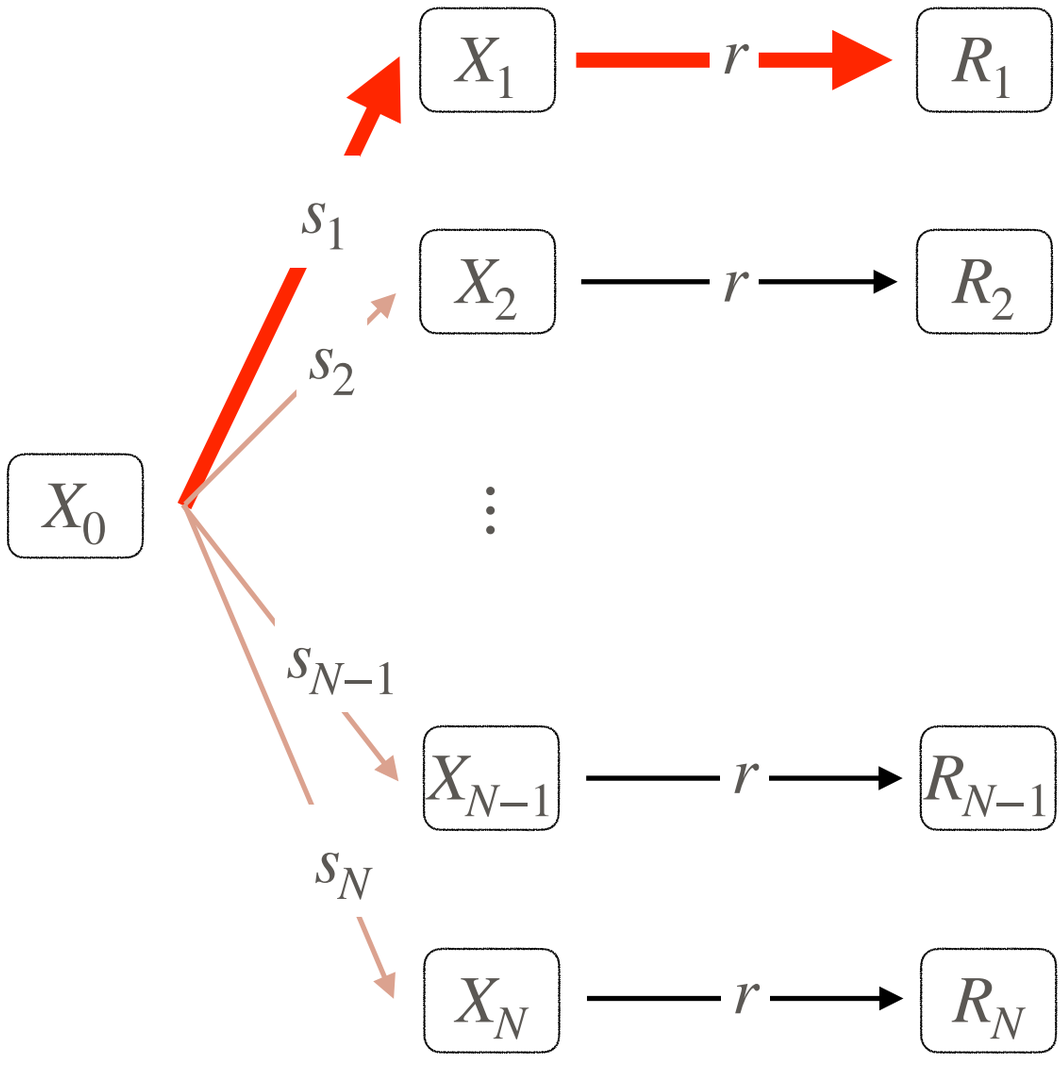
CONSTRUCTING AN OR-PROOF FOR AGAs - N



$\mathsf{com} = (R_1, \ldots, R_N)$

$$R_{\mathsf{OR}} = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

CONSTRUCTING AN OR-PROOF FOR AGAs - N



Verification reveals I

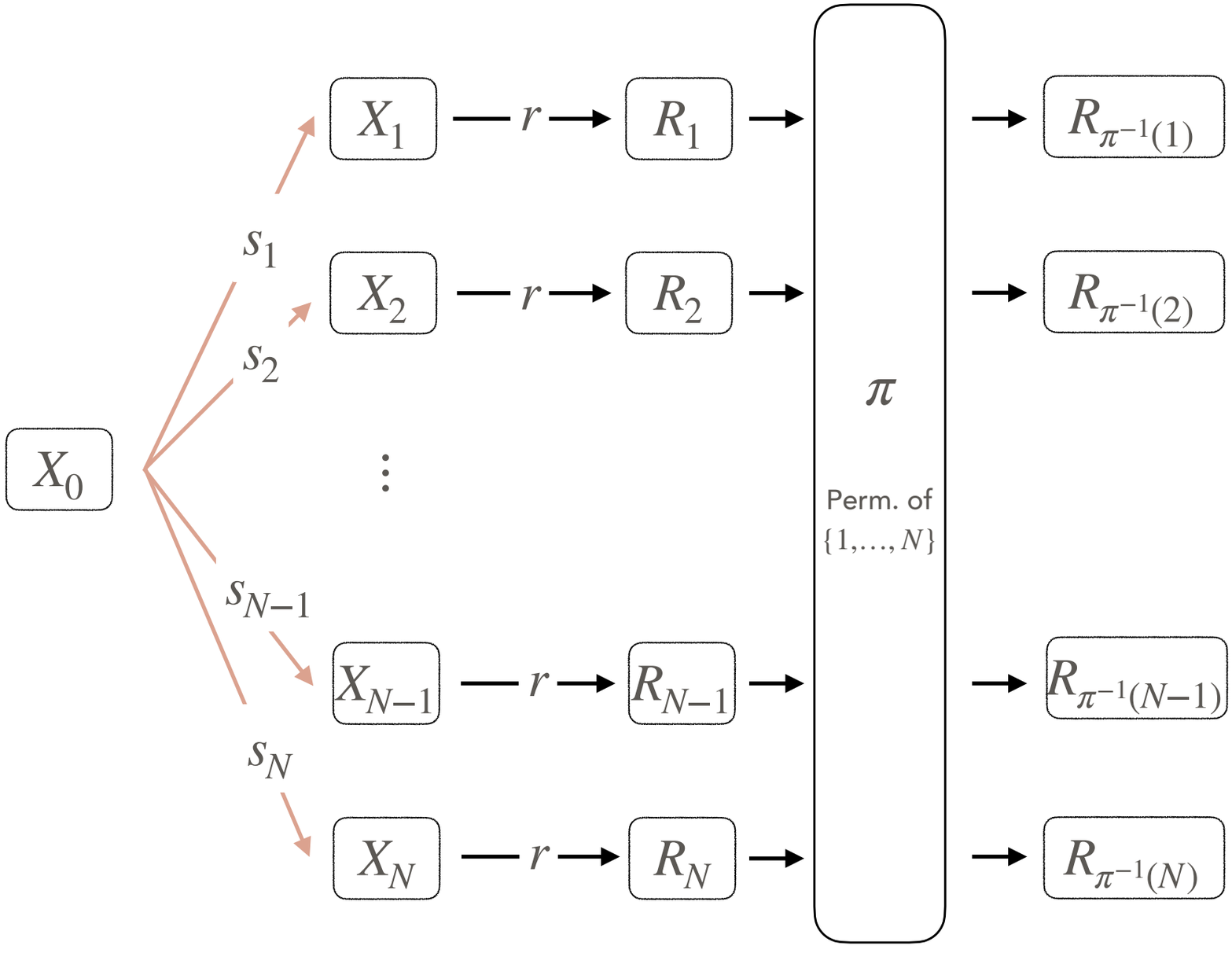
$\mathsf{com} = (R_1, \ldots, R_N)$

$\mathsf{rsp}_0 = r + s$

$\mathsf{rsp}_1 = r$

$$R_{\mathsf{OR}} = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

CONSTRUCTING AN OR-PROOF FOR AGAs - N



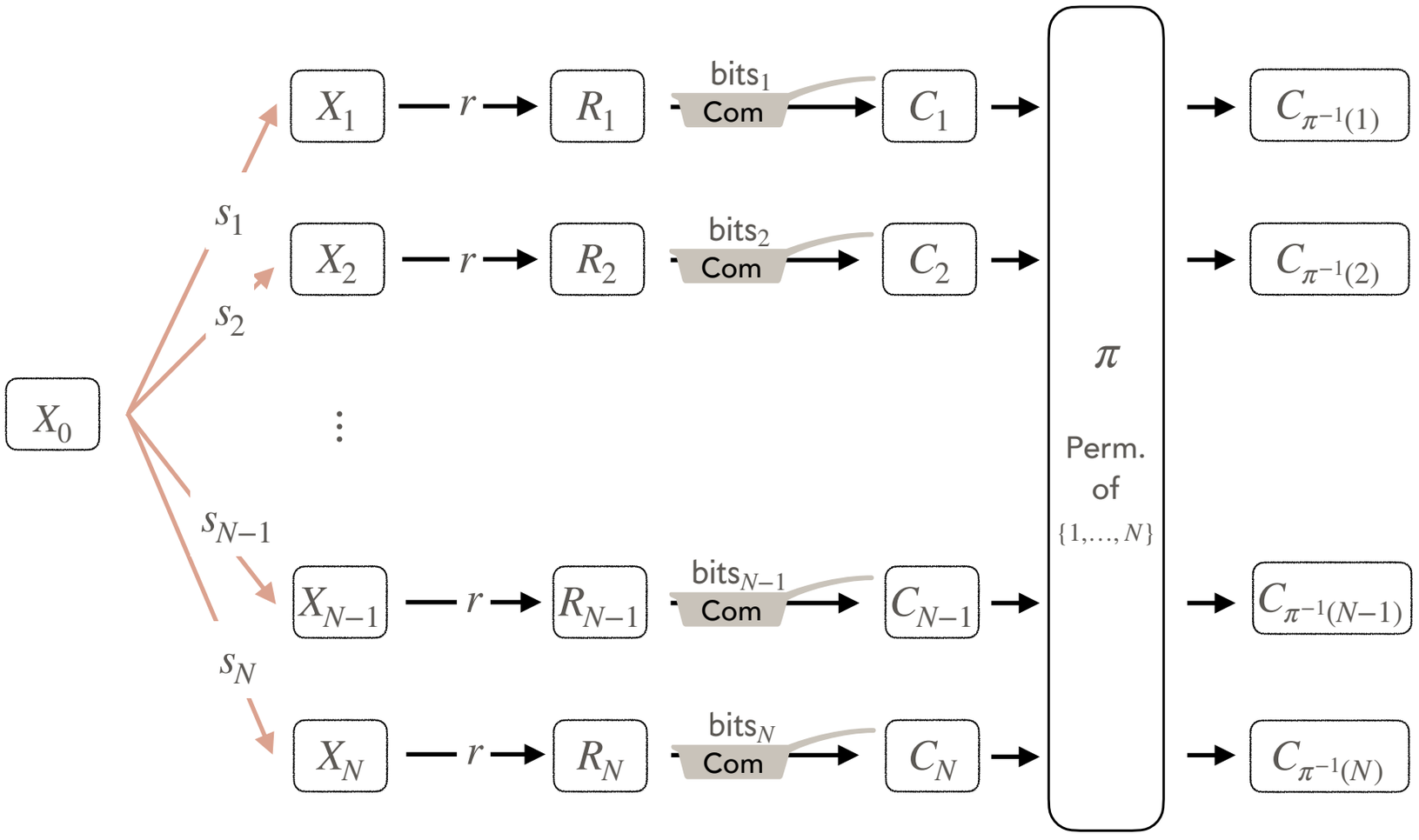
$$\text{com} = (R_{\pi^{-1}(1)}, \ldots, R_{\pi^{-1}(N)})$$

$$\text{rsp}_0 = (r + s, \pi(I))$$
$$\text{rsp}_1 = (r, \pi)$$

ZK broken if $X_i = X_j$

$$R_{\text{OR}} = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

CONSTRUCTING AN OR-PROOF FOR AGAs - N



$$\text{com} = (C_{\pi^{-1}(1)}, \ldots, C_{\pi^{-1}(N)})$$

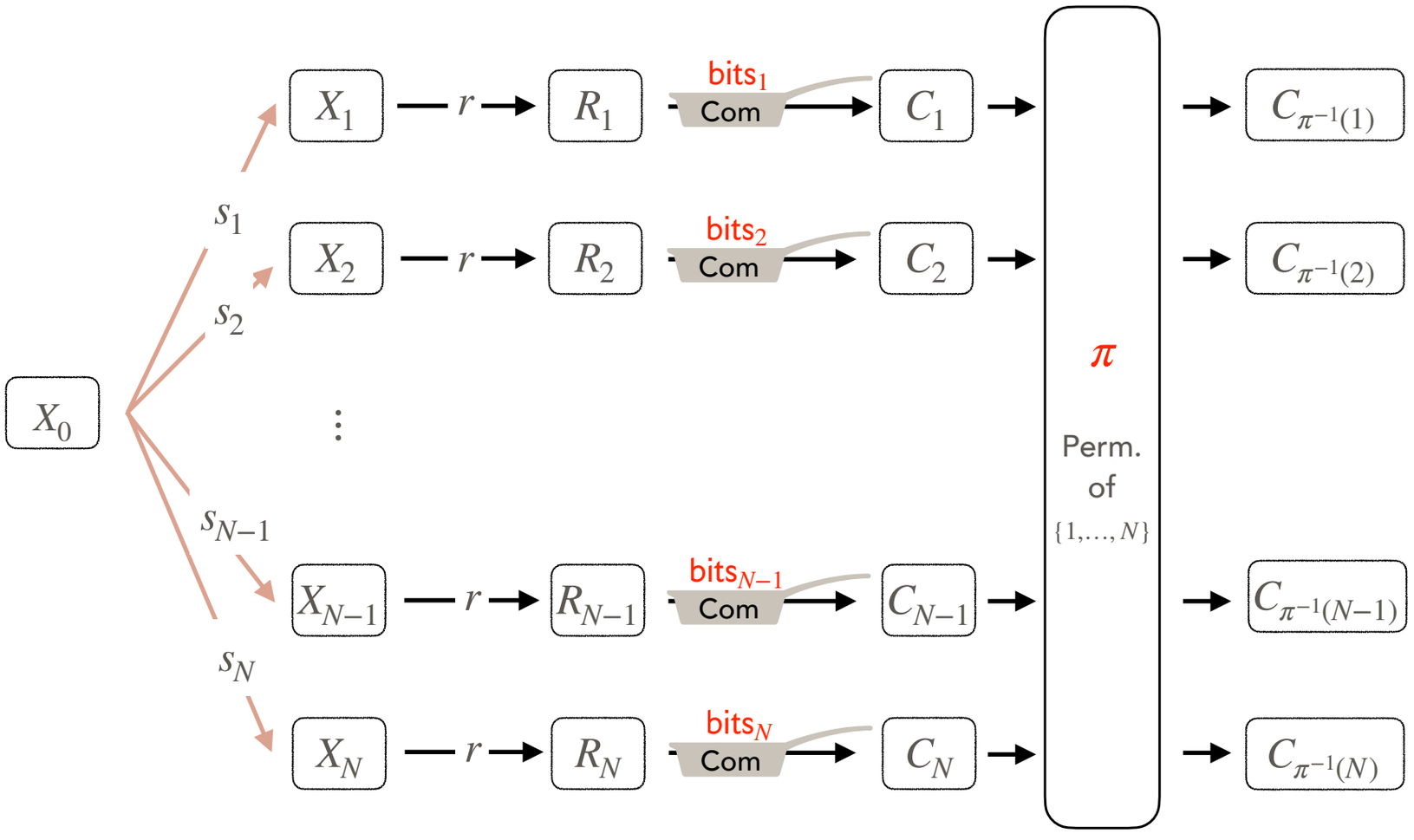
$$\text{rsp}_0 = (r + s, \text{bits}_I, \pi(I))$$
$$\text{rsp}_1 = (r, (\text{bits}_1, \ldots, \text{bits}_N), \pi)$$

$$|\text{trans}_0| = 2\lambda N + 1 + |g| + \lambda + \log N$$
$$|\text{trans}_1| = 2\lambda N + 1 + |g| + \lambda N + |\pi|$$

$$R_{\text{OR}} = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

CONSTRUCTING AN OR-PROOF FOR AGAs - N

$(r, \pi, \text{bits}_1, \ldots, \text{bits}_N) \leftarrow \text{PRG(seed)}$



$$\text{com} = (C_{\pi^{-1}(1)}, \ldots, C_{\pi^{-1}(N)})$$

$$\text{rsp}_0 = (r + s, \text{bits}_I, \pi(I))$$

$$\text{rsp}_1 = (r, (\text{bits}_1, \ldots, \text{bits}_N), \pi)$$

seed

$$|\text{trans}_0| = 2\lambda N + 1 + |g| + \lambda + \log N$$

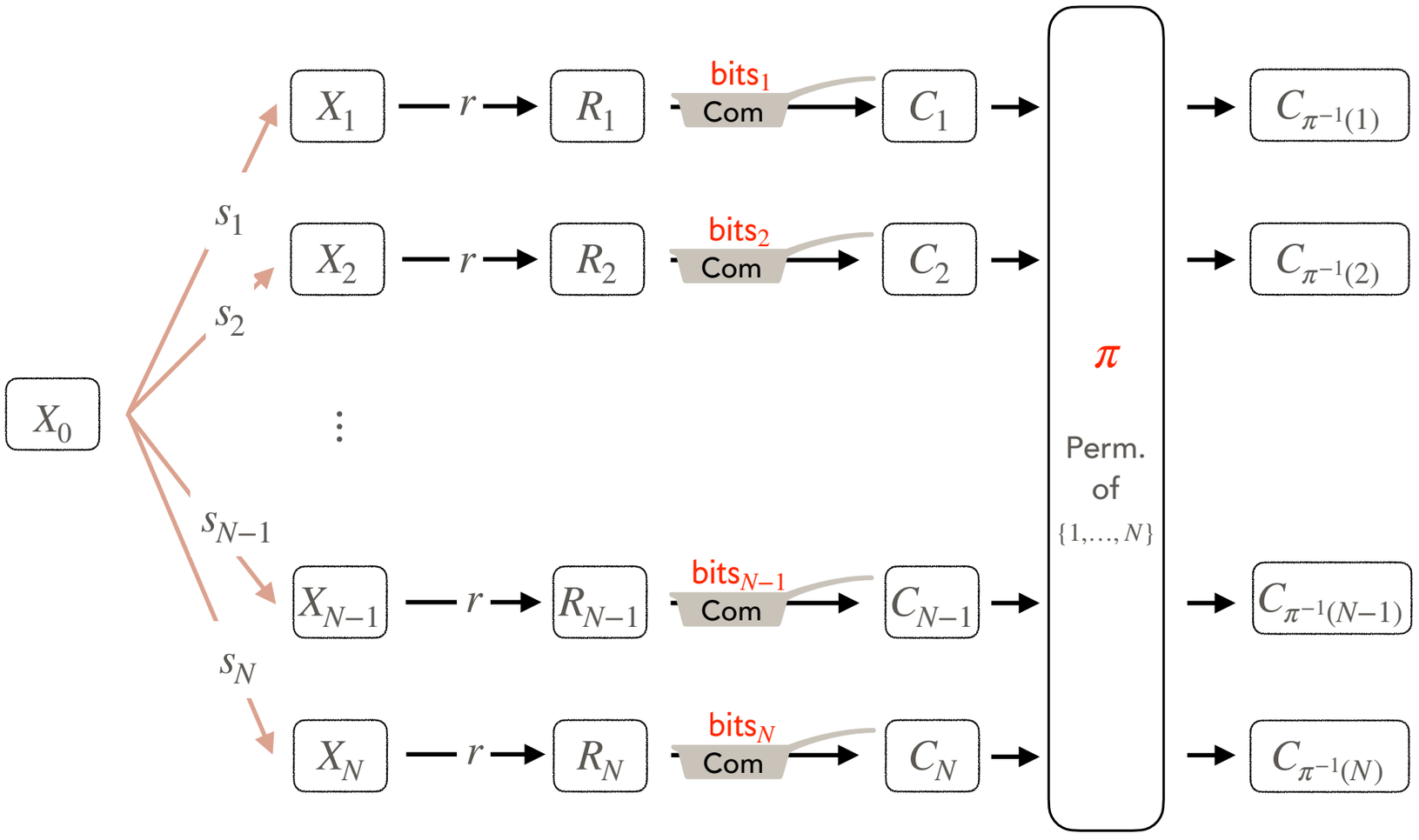
$$|\text{trans}_1| = 2\lambda N + 1 + |g| + \lambda N + |\pi|$$

λ

$$R_{\text{OR}} = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

CONSTRUCTING AN OR-PROOF FOR AGAs - N

$(r, \pi, \text{bits}_1, \ldots, \text{bits}_N) \leftarrow \text{PRG(seed)}$



$\text{com} = (C_{\pi^{-1}(1)}, \ldots, C_{\pi^{-1}(N)})$

$\text{rsp}_0 = (r + s, \text{bits}_I, \pi(I))$

$\text{rsp}_1 = (r, (\text{bits}_1, \ldots, \text{bits}_N), \pi)$

seed

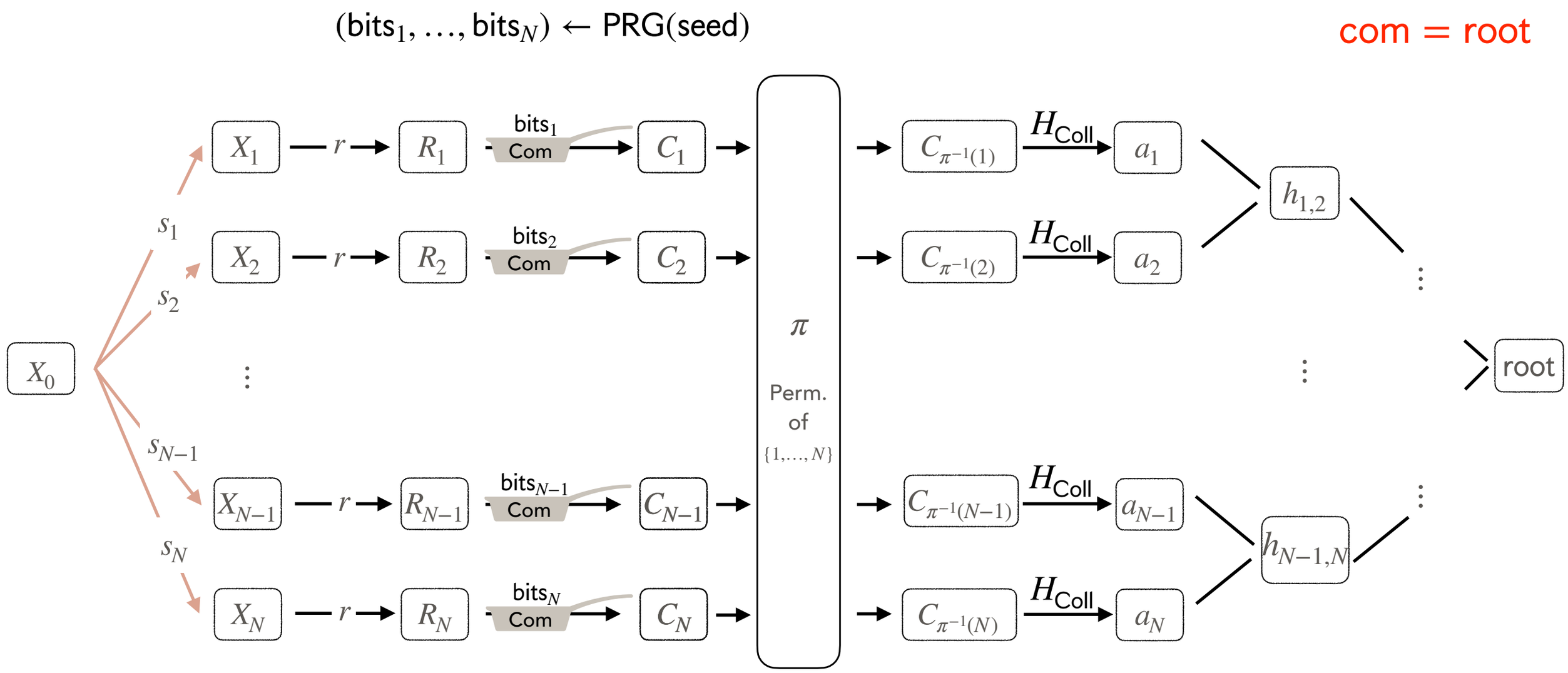
$|\text{trans}_0| = 2\lambda N + 1 + |g| + \lambda + \log N$

$|\text{trans}_1| = 2\lambda N + 1 + |g| + \lambda N + |\pi|$

λ

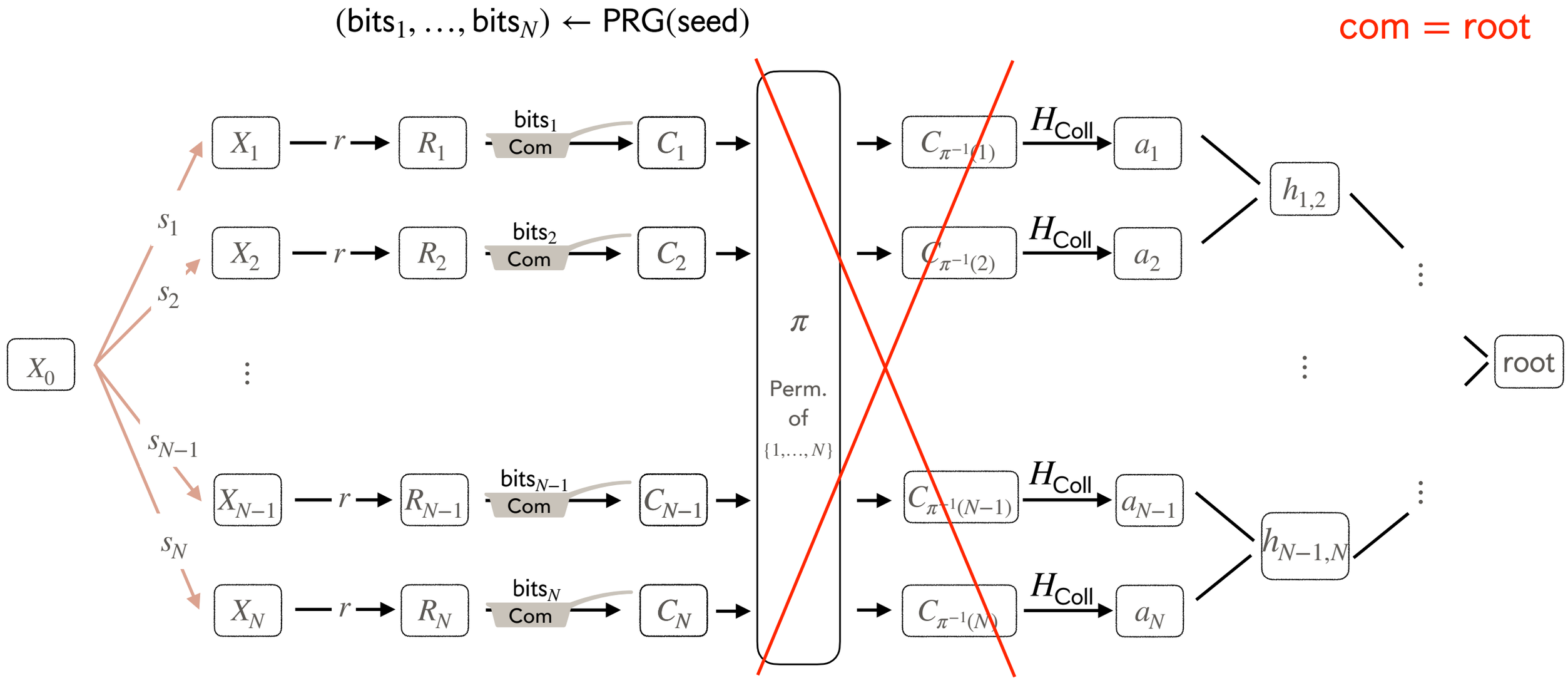
$$R_{\text{OR}} = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

OR-PROOF FOR AGAs - OPTIMISATION 1



$$R = \{((X_1, \ldots, X_N), (s, I) \,|\, s \in S_1, X_i \in \mathsf{X}, I \in [N], X_I = s \star X_0\}$$

OR-PROOF FOR AGAs - OPTIMISATION 1



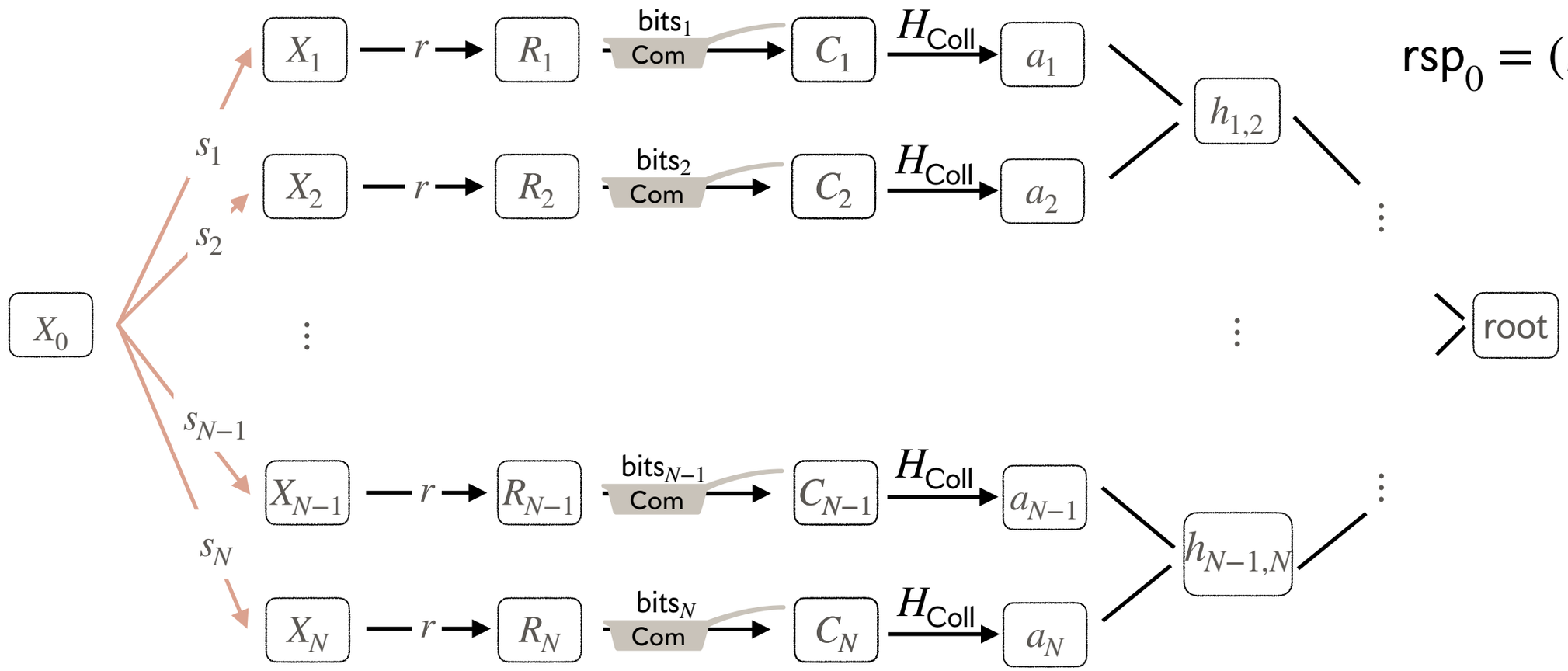
The permutation is no longer needed!

No indices involved in the verification

OR-PROOF FOR AGAs - OPTIMISATION 1

$(\text{bits}_1, \ldots, \text{bits}_N) \leftarrow \text{PRG}(\text{seed})$

com = root



$\text{rsp}_0 = (r + s, \text{bits}_I, \text{path})$

$\text{rsp}_1 = \text{seed}$

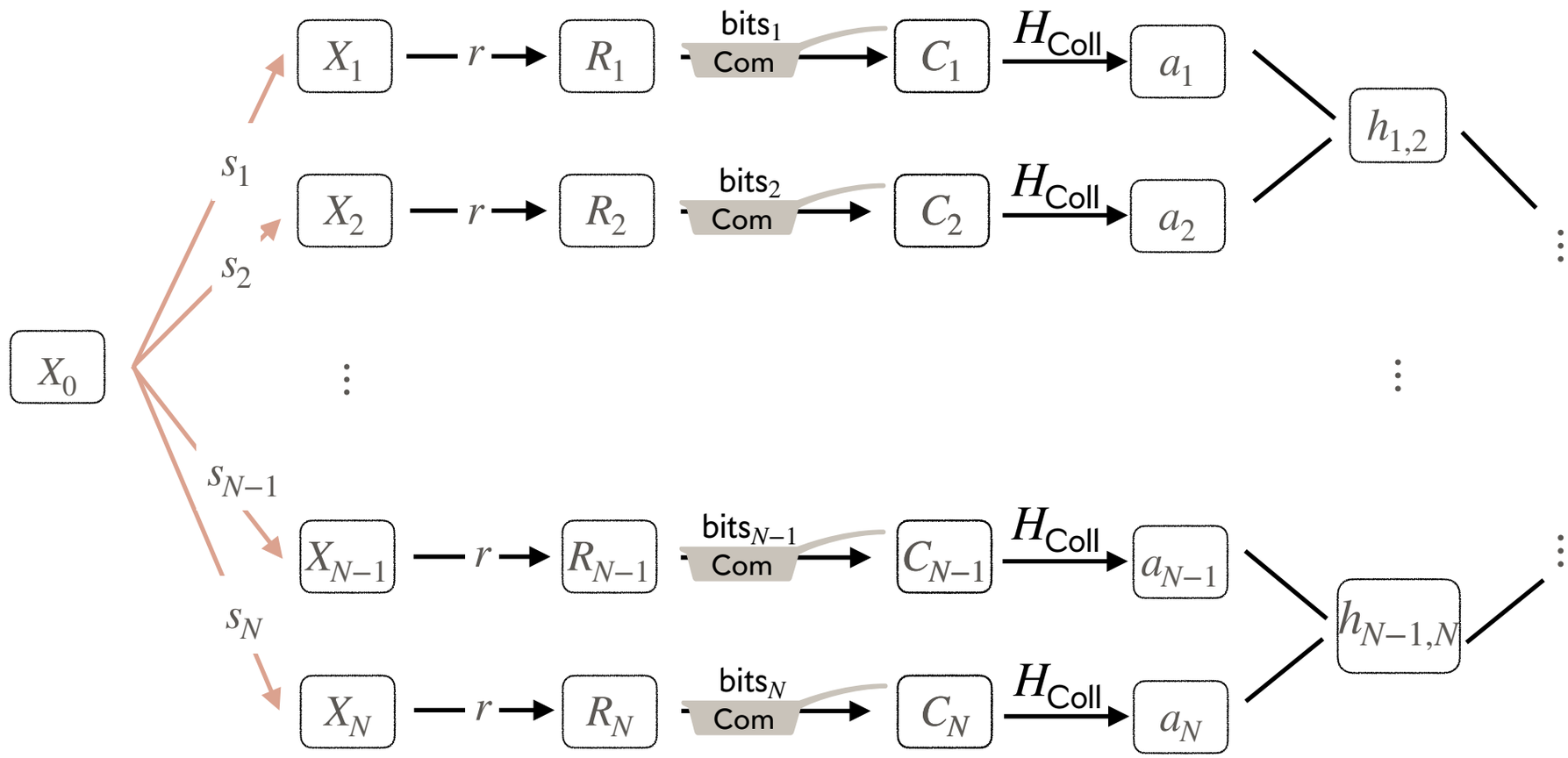
$|\text{trans}_0| = 2\lambda + 1 + |g| + \lambda + 2\lambda(\log N - 1)$

$|\text{trans}_1| = 2\lambda + 1 + \lambda$

OR-PROOF FOR AGAs - OPTIMISATION 1

$(\text{bits}_1, \ldots, \text{bits}_N) \leftarrow \text{PRG}(\text{seed})$

com = root



$\text{rsp}_0 = (r + s, \text{bits}_I, \text{path})$

$\text{rsp}_1 = \text{seed}$

$|\text{trans}_0| = 1 + |g| + \lambda + 2\lambda \log N$

$|\text{trans}_1| = 2\lambda + 1 + \lambda$

OR-PROOF FOR AGAs - FURTHER OPTIMISATIONS

To make the challenge error negligible small, λ parallel runs are executed.

We choose M, K such that $\binom{M}{K} \geq 2^{\lambda}$ and we set the

challenge space to $C_{M,K} = \{\text{ch} \in \{0,1\}^M : w(\text{ch}) = M - K\}$

It could be reduced to λ

$$|\sigma| = 2\lambda + M + (M-K)\lambda + K(|g| + \lambda + 2\lambda(\log N - 1))$$

$|\text{com}|$ $|\text{ch}|$ $|\text{rsp}_1|$ $|\text{rsp}_0|$

ROADMAP

1. OR-proofs 
2. Admissible Group Actions 
3. A new OR-Proof 
4. Calamari and Falafl

CA(LA)MARI

Given a prime p, the **ideal class group** $\mathbb{G} = \mathrm{Cl}(\mathcal{O})$ of $\mathcal{O} = \mathbb{Z}\left[\sqrt{-p}\right]$ **acts** freely and transitively on the **set** X **of supersingular elliptic curves** E over $\mathbb{F}_p$ s.t. $\mathrm{End}_p(E) \simeq \mathcal{O}$.

GAIP problem: given $X_0 \in \mathrm{X}$ and a uniform $X \in \mathrm{X}$, find $a \in \mathbb{G}$ s.t. $a \star X_0 = X$.

Only for the set of parameters CSIDH-512 the structure of $\mathbb{G}$ is known.

- $\lambda = 128$
- $M = 247,\ K = 30$
- $|g| = 258\ (|\mathbb{G}| \approx 2^{257.1})$

Experimental results $(N = 8)$: $|\sigma| \approx \log N + 3.5\mathrm{KB}$

Signing ≈ 79 s

Thanks for your attention

Federico Pintore

Department of Mathematics, University of Bari (IT)

federico.pintore@gmail.com