IVC in the Open-and-Sign Random Oracle Model

Joint work with Mary Maller & Arantxa Zapico

Nicolas Mohnblatt, zkSecurity
Asiacrypt 2025

ZKSECURITY

Overview

Three main aspects of our work

1. **Systematisation of knowledge**: give a unifying view of IVC constructions.

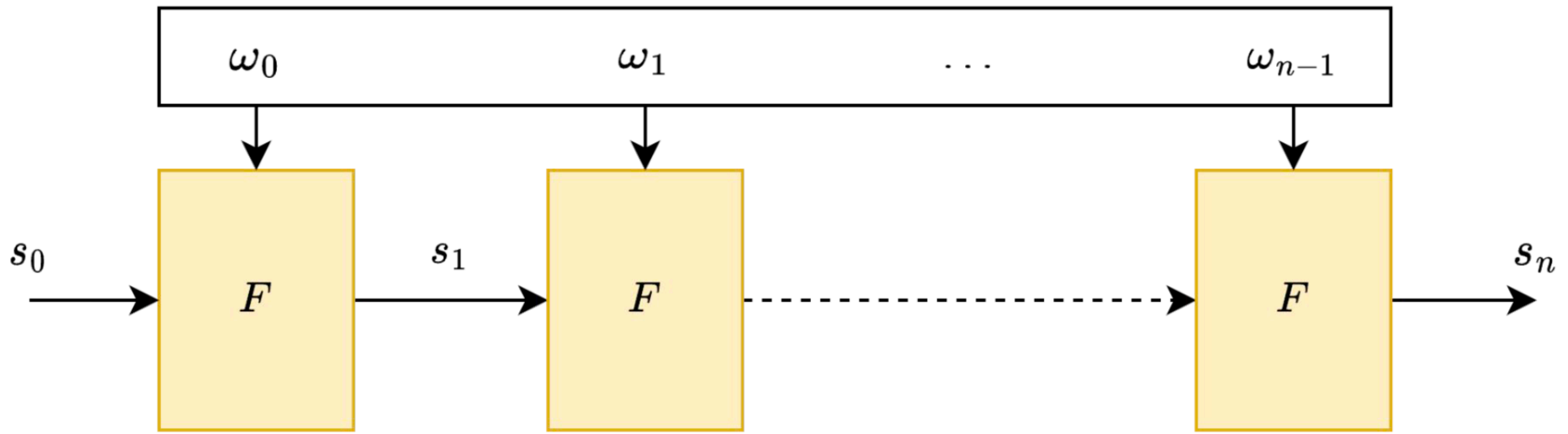
2. **Cross-pollination**: aggregate results and insights across all generations of IVC schemes; particularly for dealing with cycle of elliptic curves.

3. **Security model**: separate construction from heuristics using an appropriate security model.

Incrementally verifiable computation (IVC)

[Val08]

- Consider a long computation, iterating a function F:



- Goal: produce a proof π_n of knowledge of $\omega_0, \dots, \omega_{n-1}$ such that s_n is correct.

- $\mathbf{V}$ is given F, n, s_0, s_n.

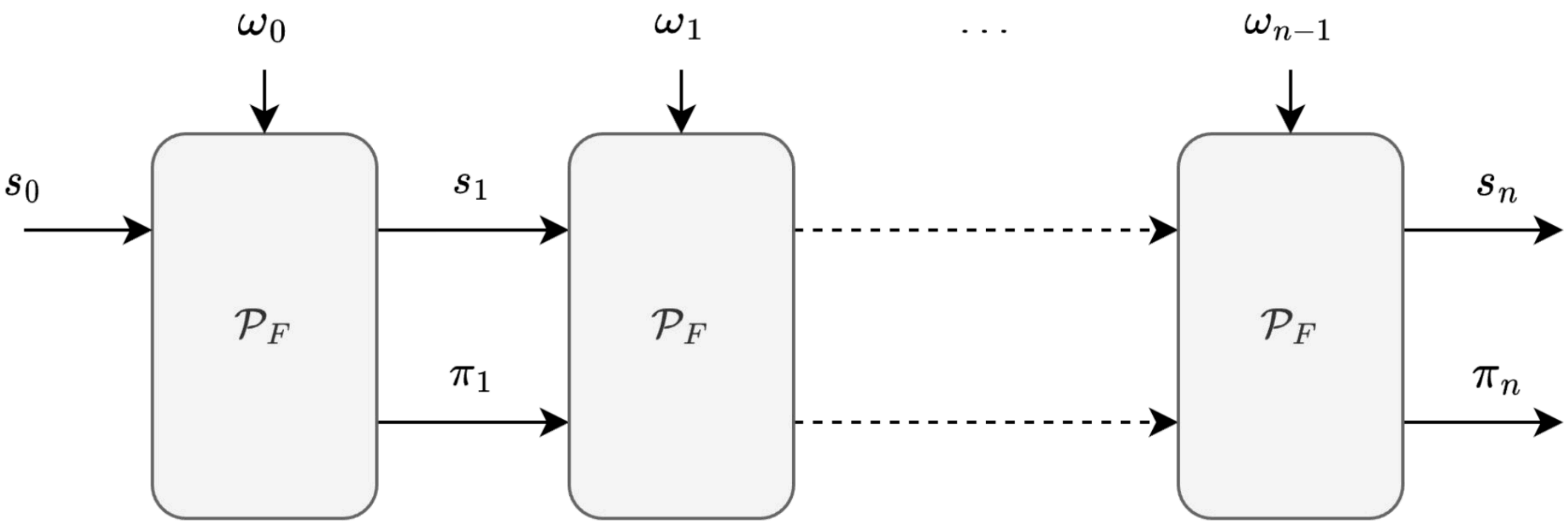
π_n can be generated *incrementally* and
$|\pi_n|$ is constant w.r.t n

ZKSECURITY

Incrementally verifiable computation (IVC)

[Val08]

- To realise IVC, we define a prover $\mathbf{P}_F$ that takes as inputs s_i, ω_i and a proof π_i and **updates both the state and proof**.



- Q: what are proofs and how are they updated?

Unifying IVC constructions

A brief history of IVC

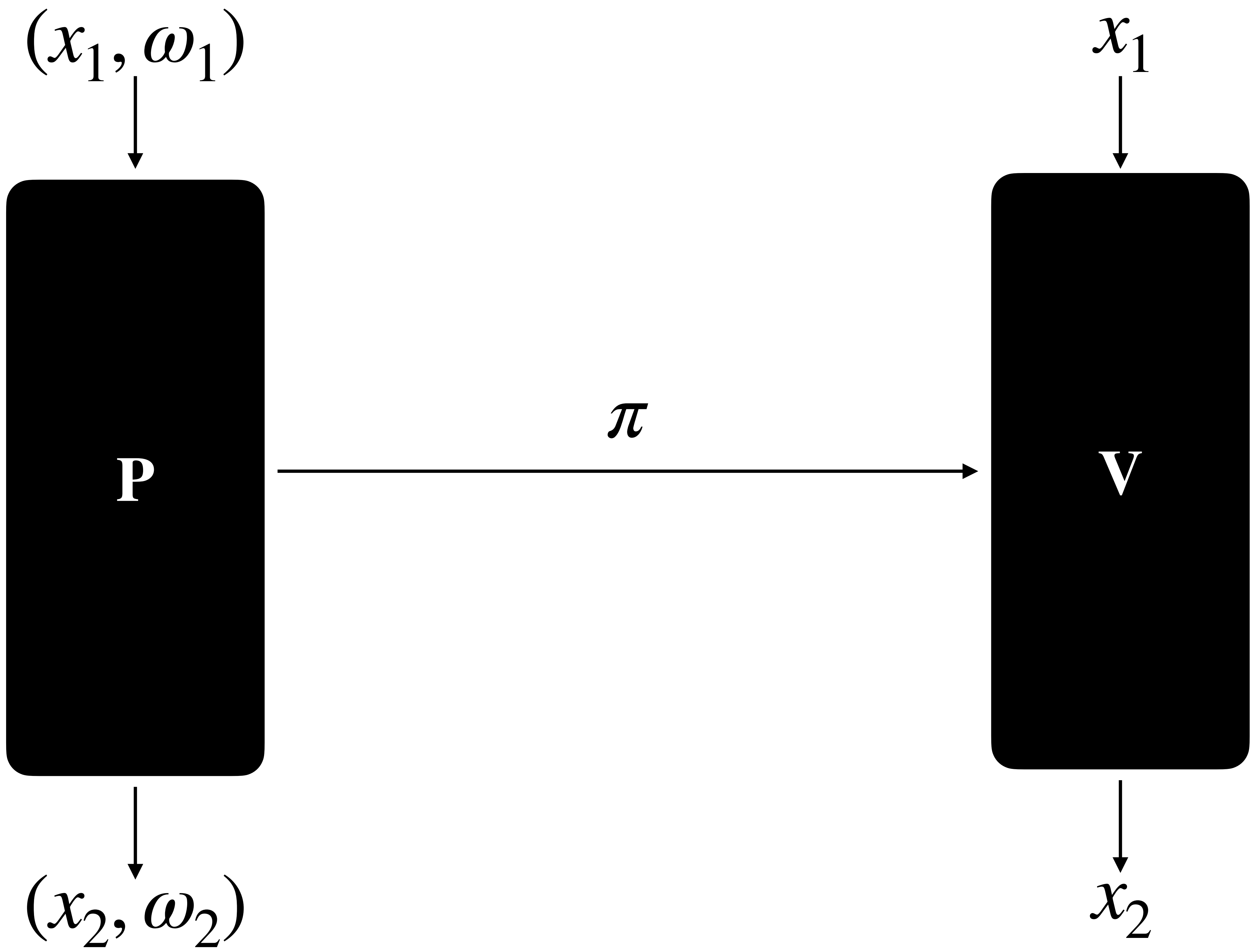
- The first generation of IVC constructions rely on the **recursive composition of SNARKs** for arithmetic circuits [Val08, BCCT13, BCTV14, COS20].
- Second generation relaxes this requirement: only need a **NARK with short proofs** and an **accumulation scheme** [BGH19, BCMS20, BDFG21].
- Third generation relaxes this further: **NARK with "split" proofs** and an **accumulation scheme** [BCLMS21, KST21, and follow ups].

We show that all three generations can be described in a single framework

Reductions of knowledge

[KP23]

$$\boxed{\Pi : R_1 \to R_2}$$



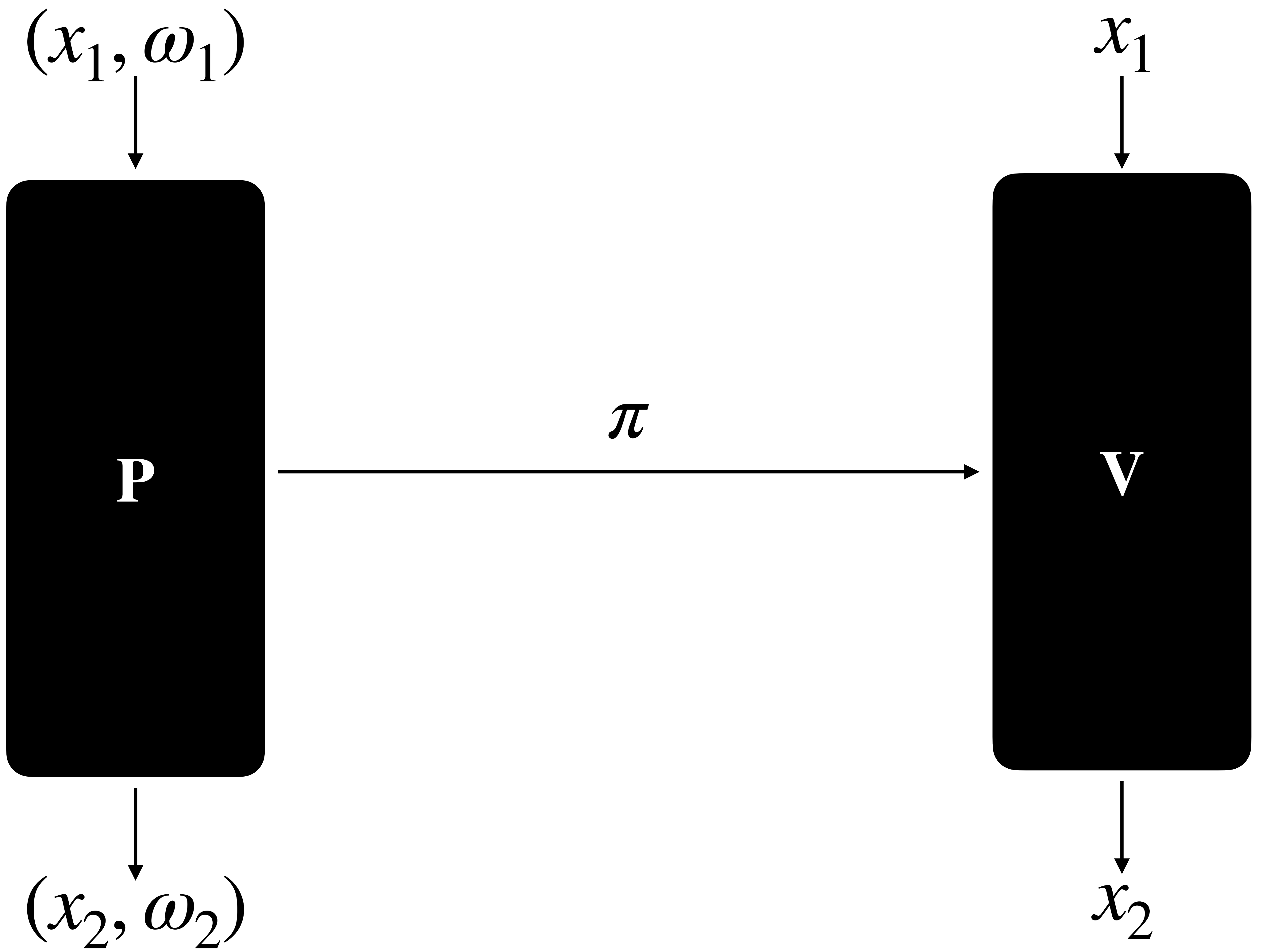
- generalisation of arguments of knowledge and accumulation schemes.

- **completeness**: if $(x_1, \omega_1) \in R_1$, then $(x_2, \omega_2) \in R_2$.

- **knowledge soundness**: if $\exists \omega_2$ s.t. $(x_2, \omega_2) \in R_2$, then we can extract ω_1 s.t. $(x_1, \omega_1) \in R_1$.

Reductions of knowledge
[KP23]

$$\boxed{\Pi : R_1 \to R_2}$$



- A (S)NARK for R is a reduction from $R \to R_{\text{truth}}$.
- Define an accumulation (or folding) scheme to be a reduction $R \times R' \to R'$.

IVC from RoKs

A unifying view

arithmetic circuits (NP-complete)

$$\Pi_{\text{prime}} : R_{\text{arith}} \rightarrow R_{\text{inter}}$$

intermediate relation

$$\Pi_{\text{acc}} : R_{\text{prime}} \times R_{\text{acc}} \rightarrow R_{\text{acc}}$$

check that a pair $(x, \omega)^{\text{inter}}$ is in R_{inter} and that Π_{prime} was applied honestly

accumulator

IVC from RoKs

A unifying view

$\Pi_{\text{prime}} : R_{\text{arith}} \to R_{\text{inter}}$

$\Pi_{\text{acc}} : R_{\text{prime}} \times R_{\text{acc}} \to R_{\text{acc}}$

- An IVC proof at step i is a tuple $((x, \omega)_i^{\text{prime}}, (x, \omega)_i^{\text{acc}}) \in R_{\text{prime}} \times R_{\text{acc}}$.
- Proving process:
  1. run Π_{acc} to obtain a new accumulator $(x, \omega)_{i+1}^{\text{acc}} \in R_{\text{acc}}$.
  2. produce a claim $(x, \omega)_{i+1}^{\text{arith}} \in R_{\text{arith}}$ for the statement "compute F and verify Π_{acc}".
  3. run Π_{prime} on $(x, \omega)_{i+1}^{\text{arith}}$ to obtain a new pair $(x, \omega)_{i+1}^{\text{prime}} \in R_{\text{prime}}$.
  4. output the new proof $((x, \omega)_{i+1}^{\text{prime}}, (x, \omega)_{i+1}^{\text{acc}}) \in R_{\text{prime}} \times R_{\text{acc}}$.

ZKSECURITY

Cross-pollination

Instantiating the reductions

Elliptic curve commitments

- Elliptic curve commitments have many benefits:
  - first practical **SNARKs** used ECC.
  - **straightline extraction** in the AGM/GGM or with knowledge assumptions.
  - additive homomorphism allows to make simple **accumulation schemes**.
- To commit to elements of a field $\mathbb{F}$, we use an elliptic curve E of order $\#E = |\mathbb{F}|$.
- problem: E cannot be defined over $\mathbb{F}$, otherwise DLOG is easy [Sma99]. Expressing computations about commitments incurs large arithmetization costs.
  - Q: how to efficiently **"close the loop"**?

Cycles of elliptic curves

in the style of [BCTV14]

- [BCTV14] solution, use a **2-cycles of elliptic curves**:
    - $E^{(\text{ying})}$ is of order $|\mathbb{F}^{(\text{ying})}|$ and defined over a field $\mathbb{F}^{(\text{yang})}$.
    - $E^{(\text{yang})}$ is of order $|\mathbb{F}^{(\text{yang})}|$ and defined over a field $\mathbb{F}^{(\text{ying})}$.
- Cycles are **confusing**. Naively lifting an IVC construction to the cycle setting can lead to **critical soundness bugs** [NBS23].
- we generalise the [NBS23] result to our framework. Requires to **go around the loop twice**. Surprisingly, proof size does not double.
- Future work: include CycleFold [KS24], an alternative approach to supporting cycles

Security modelling

Instantiating Π_{acc}

The "interaction" problem

- Accumulation schemes are usually interactive protocols (or non-interactive in the ROM using Fiat-Shamir).
- This means that the verifier cannot be represented as an arithmetic circuit; we would need circuits (and reductions) for $\mathsf{NP}^{\mathcal{O}}$.

Challenge 1: need to apply FS but also need to represent verifiers as circuits

Cycles of curves (bis)

- Security of ECC constructions often rely on the AGM or GGM for extraction.
- Adapting the AGM to the curve cycle setting is not trivial [LS24]. In particular, EC points have dual representations in IVC security proofs: either as group elements or as pair of base field elements.
- The GGM does not allow group operations to be represented in circuits.

Challenge 2: how can we get straightline extraction for EC commitments in the 2-cycle setting?

Open-and-sign random oracle

- We do not resolve these problems, but instead provide a model that neatly **separates them from the IVC construction**.
- Borrow an idea from the signed ROM of [CT10]: introduce an oracle that observes the prover's messages and produces **signed randomness**.
  - **extractability** comes from the fact that our extractor can observe oracle queries.
  - verifier does not need to call the oracle, it only **verifies signatures**.
- Downside: the model is hard (and sometimes impossible) to instantiate.

More in the paper…

- Show the correspondence between generalised framework and concrete IVC schemes.
- Recover [NBS23] insights on IVC proof malleability.
- Analysis of HyperNova [KS24] over a BCTV14-style curve cycle using our tools.

References

1/2

- [BCCT13] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. “Recursive composition and bootstrapping for SNARKs and proof-carrying data”. In: Proceedings of the forty-fifth annual ACM symposium on Theory of computing. 2013, pp. 111–120.
- [BCTV14] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. “Scalable Zero Knowledge Via Cycles of Elliptic Curves”. In: Algorithmica 79 (2014), pp. 1102–1160. url: https://api.semanticscholar.org/CorpusID:8825569.
- [BGH19] S. Bowe, J. Grigg, and D. Hopwood. Recursive Proof Composition without a Trusted Setup. Cryptology ePrint Archive, Paper 2019/1021. https : / / eprint . iacr . org / 2019 / 1021. 2019. url: https://eprint.iacr.org/2019/1021.
- [BCLMS21] B. Bünz, A. Chiesa, W. Lin, P. Mishra, and N. Spooner. “Proof-Carrying Data Without Succinct Arguments”. In: Advances in Cryptology – CRYPTO 2021. Ed. by T. Malkin and C. Peikert. Cham: Springer International Publishing, 2021, pp. 681–710. isbn: 978-3-030-84242-0.
- [BCMS20] B. Bünz, A. Chiesa, P. Mishra, and N. Spooner. “Recursive Proof Composition from Accumulation Schemes”. In: Theory of Cryptography. Ed. by R. Pass and K. Pietrzak. Cham: Springer International Publishing, 2020, pp. 1–18. isbn: 978-3-030-64378-2.
- [BDFG21] D. Boneh, J. Drake, B. Fisch, and A. Gabizon. “Halo infinite: Proof-carrying data from additive polynomial commitments”. In: Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41. Springer. 2021, pp. 649–680.
- [COS20] A. Chiesa, D. Ojha, and N. Spooner. “Fractal: Post-quantum and transparent recursive proofs from holography”. In: Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I 39. Springer. 2020, pp. 769–793.
- [CT10] A. Chiesa and E. Tromer. “Proof-Carrying Data and Hearsay Arguments from Signature Cards.” In: ICS. Vol. 10. 2010, pp. 310–331.

References

2/2

- [KP23] A. Kothapalli and B. Parno. “Algebraic Reductions of Knowledge”. In: Advances in Cryptology – CRYPTO 2023. Ed. by H. Handschuh and A. Lysyanskaya. Cham: Springer Nature Switzerland, 2023, pp. 669–701. isbn: 978-3-031-38551-3.

- [KST21] A. Kothapalli, S. Setty, and I. Tzialla. “Nova: Recursive Zero-Knowledge Arguments from Folding Schemes”. In: Advances in Cryptology – CRYPTO 2022. Ed. by Y. Dodis and T. Shrimpton. Cham: Springer Nature Switzerland, 2022, pp. 359–388.

- [KS24] A. Kothapalli and S. Setty. “HyperNova: Recursive Arguments for Customizable Constraint Systems”. In: Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part X. Ed. by L. Reyzin and D. Stebila. Vol. 14929. Lecture Notes in Computer Science. Springer, 2024, pp. 345–379. doi:

- [LS24] H. Lee and J. H. Seo. “On the Security of Nova Recursive Proof System”. In: IACR Cryptol. ePrint Arch. (2024), p. 232. url: https://eprint.iacr.org/2024/232.

- [NBS23] W. Nguyen, D. Boneh, and S. Setty. Revisiting the Nova Proof System on a Cycle of Curves. Cryptology ePrint Archive, Paper 2023/969. https://eprint.iacr.org/2023/969. 2023. url: https://eprint.iacr.org/2023/969.

- [Sma99] N. P. Smart. “The Discrete Logarithm Problem on Elliptic Curves of Trace One”. In: J. Cryptol. 12.3 (1999), pp. 193–196. doi: 10 . 1007 / S001459900052. url: https : / / doi . org / 10 . 1007 / s001459900052.

- [Val08] P. Valiant. “Incrementally verifiable computation or proofs of knowledge imply time/space efficiency”. In: Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008. Proceedings 5. Springer. 2008, pp. 1–18.

Summary

Three main aspects of our work

1. **Systematisation of knowledge**: IVC from RoKs.
2. **Cross-pollination**: lift IVC from RoKs to 2-cycles of elliptic curves + malleability.
3. **Security model**: open-and-sign random oracle model.

ZKSECURITY