An Algebraic Framework for Updatable and Universal SNARKs

Carla Ràfols and *Arantxa Zapico*

Crypto 2021

Universitat Pompeu Fabra Barcelona

Obra Social "la Caixa"

Pairing-Based (zk)SNARKs

State of the art

Interactive Proof-Systems [GMR89] → ZK proofs for all NP [GMW] → . . . → Succinct arguments without PCPs [Gro10] → QAPs [GGPR13] & Pinnocchio [PGHR13] → ZeroCash → Most efficient zk-SNARK [Gro16]

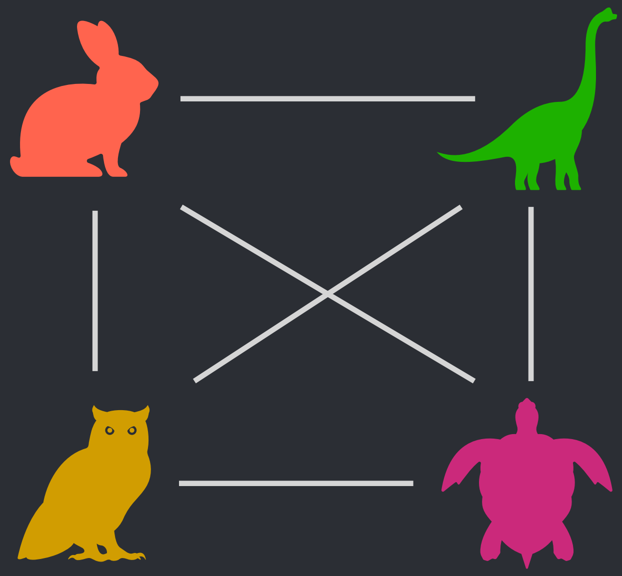
Trusted Setup!!!

Multiparty Computation (Zcash Ceremony)

One ceremony per relation!!!

Updatable and Universal SNARKs

- Multiparty Computation Model:



- Updatable Model:

Updatable and Universal (zk)SNARKs

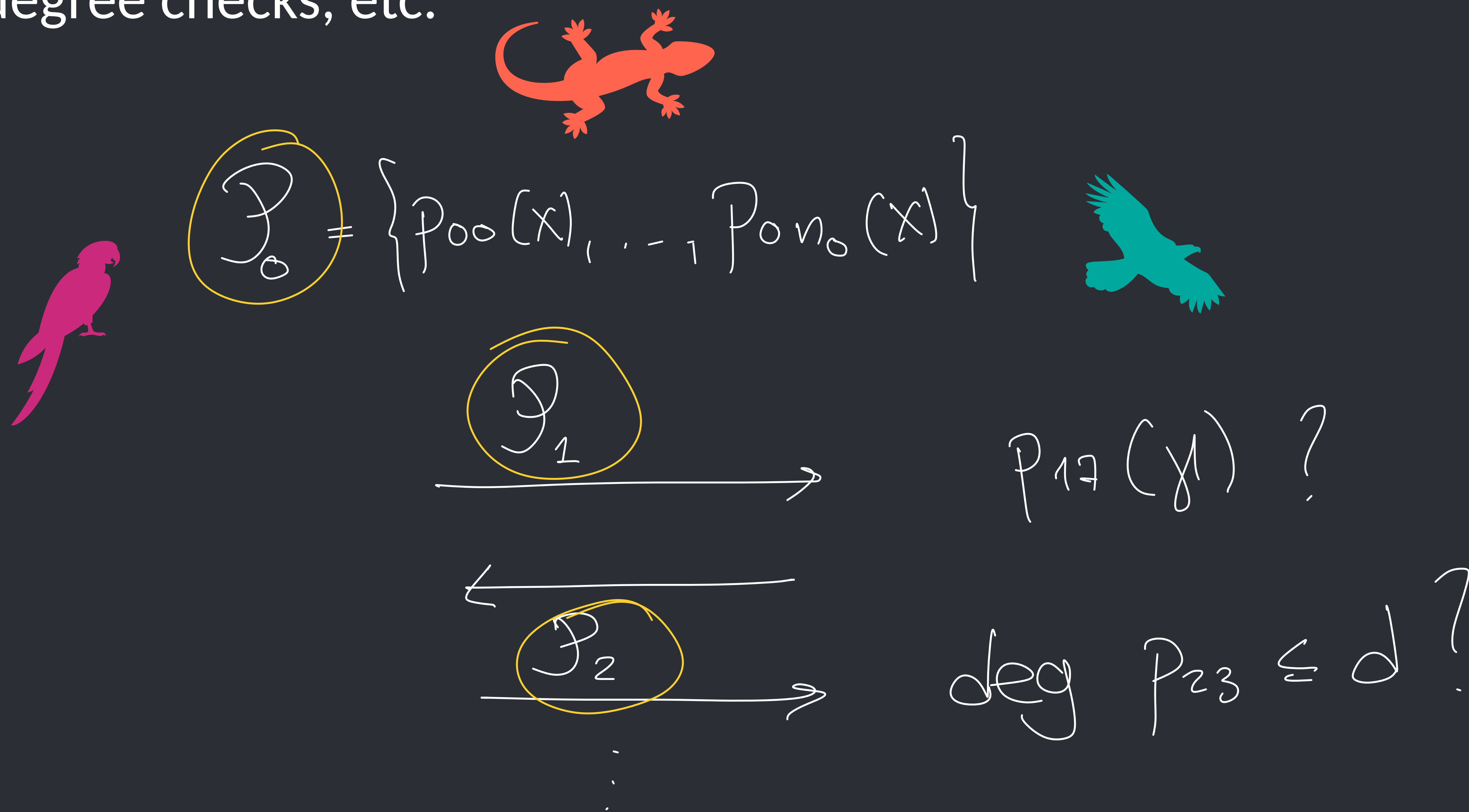
Common Design Principle

Information Theoretical Object + Cryptographic Compiler = SNARK

Sonic[MBKM19] — Plonk[GWC19] — Marlin[CHMMVW20] — Lunar[CFFQH20] — Claymore[SZ21]

Polynomial Holographic:

- *Indexer* computes relation-dependent polynomials
- *Prover's* messages include polynomials
- *Verifier* has oracle access to both sets of polynomials, can do degree checks, etc.



Motivation

Can we break further the information theoretical object?

1. Extract
2. Compare
3. Combine
4. Improve

Algebraic Intuition

Circuit Satisfiability

- quadratic: $a_i b_i = c_i \qquad \forall\, i = 1, \ldots, m$
- linear: $a_i = \sum_{j=1}^{m} f_{ij} c_j,\ b_i = \sum_{j=1}^{m} g_{ij} c_j \qquad \forall\, i = 1, \ldots, m$

$$\exists\, \vec{a}, \vec{b}, \vec{c} \in \mathbb{F}^m \text{ s.t. for given } \mathbf{F}, \mathbf{G} \in \mathbb{F}^{m \times m}:$$

1. $\vec{a} \circ \vec{b} = \vec{c}$
2. $\begin{pmatrix} \mathbf{I} & \mathbf{0} & -\mathbf{F} \\ \mathbf{0} & \mathbf{I} & -\mathbf{G} \end{pmatrix} \begin{pmatrix} \vec{a} \\ \vec{b} \\ \vec{c} \end{pmatrix} = \begin{pmatrix} \mathbf{W}_a & \mathbf{W}_b & \mathbf{W}_c \end{pmatrix} \begin{pmatrix} \vec{a} \\ \vec{b} \\ \vec{c} \end{pmatrix} = \mathbf{W} \begin{pmatrix} \vec{a} \\ \vec{b} \\ \vec{c} \end{pmatrix} = \vec{0}$

Algebraic Intuition

Circuit Satisfiability

$$\begin{pmatrix} \mathbf{I} & \mathbf{0} & -\mathbf{F} \\ \mathbf{0} & \mathbf{I} & -\mathbf{G} \end{pmatrix} \begin{pmatrix} \vec{a} \\ \vec{b} \\ \vec{c} \end{pmatrix} = \begin{pmatrix} \mathbf{W}_a & \mathbf{W}_b & \mathbf{W}_c \end{pmatrix} \begin{pmatrix} \vec{a} \\ \vec{b} \\ \vec{c} \end{pmatrix} = \mathbf{W} \begin{pmatrix} \vec{a} \\ \vec{b} \\ \vec{c} \end{pmatrix} = \vec{0}$$

$$(\vec{W}_a, \vec{W}_b, \vec{W}_c)_i \cdot (\vec{a}, \vec{b}, \vec{c}) = 0$$

- Sample a random vector $(\vec{d}_a, \vec{d}_b, \vec{d}_c)$ in the rowspace of $\mathbf{W}$.

$$(\vec{d}_a, \vec{d}_b, \vec{d}_c) = \sum_{i=1}^{2m} \alpha_i (\vec{W}_a, \vec{W}_b, \vec{W}_c)_i$$

- Check one inner product $(\vec{d}_a, \vec{d}_b, \vec{d}_c) \cdot (\vec{a}, \vec{b}, \vec{c}) = 0$.

"Compressed" Linear Algebra

Let $\mathbb{H} = \{\mathsf{h}_1, \ldots, \mathsf{h}_m\} \subset \mathbb{F}_p^*$.

$$\lambda_i(X) = \prod_{j \neq i} \frac{(X - \mathsf{h}_j)}{(\mathsf{h}_i - \mathsf{h}_j)}, \qquad t(X) = \prod_j (X - \mathsf{h}_j)$$

Linear Algebra World	Polynomial World
$\vec{y} = (y_1, \ldots, y_m)$	$Y(X) = \sum_{i=1}^{m} y_i \lambda_i(X)$

From Vectors to Polynomials

- Sample $(\vec{d}_a, \vec{d}_b, \vec{d}_c)$ and compute $D_a(X), D_b(X), D_c(X)$
- From $A(X), B(X), C(X)$ and $D_a(X), D_b(X), D_c(X)$:

1. $\vec{a} \circ \vec{b} = \vec{c}$

$$A(X)B(X) - C(X) = t(X)H_1(X)$$

2. $(\vec{d}_a, \vec{d}_b, \vec{d}_c) \cdot (\vec{a}, \vec{b}, \vec{c}) = 0$

$$(D_a(X), D_b(X), D_c(X)) \cdot (A(X), B(X), C(X)) = XR(X) + t(X)H_2(X)$$

Checkable Subspace Sampling (CSS)

1. $\vec{\alpha}$**W**

$$\vec{\alpha}(Y) = (\alpha_1(Y), \ldots, \alpha_{2m}(Y))$$

$$\vec{\alpha} = \vec{\alpha}(y), \text{ for } y \text{ sent by the verifier}$$

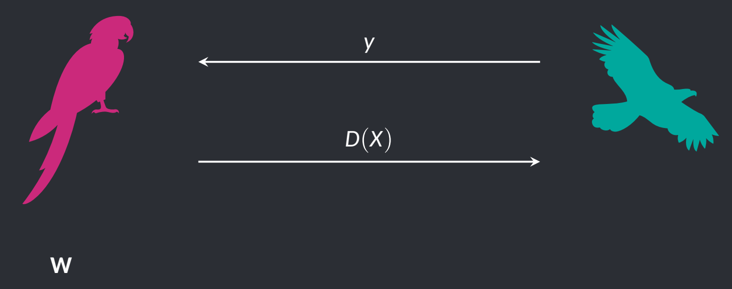
2. $\vec{D}(X) = (D_a(X), D_b(X), D_c(X))$

$$\begin{aligned}\vec{D}(X) &= \sum_{j=1}^{3m} (d_a, d_b, d_c)_j \lambda_j(X) = \sum_{j=1}^{3m} \left(\sum_{i=1}^{2m} \alpha_i (W_a, W_b, W_c)_{ij} \right) \lambda_j(X) \\ &= \sum_{j=1}^{3m} \sum_{i=1}^{2m} \alpha_i(y) (W_a, W_b, W_c)_{ij} \lambda_j(X) \\ &= W(X, y)\end{aligned}$$

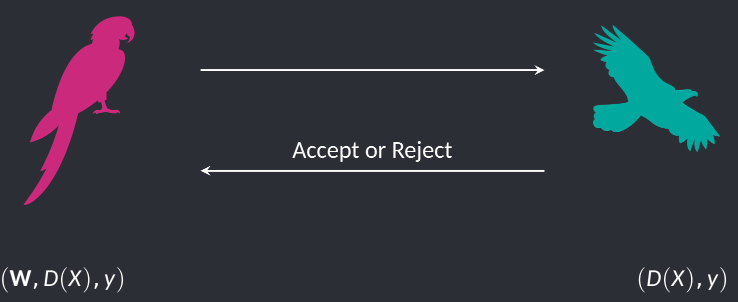
Checkable Subspace Sampling

Definition

- *Offline phase:* Indexer outputs polynomials describing matrix **W**.
- *Online phase:*
  - *Sampling:*



  - *Prove Sampling:*



  - *Decision phase:* Verifier accepts only if $D(X)$ encodes vector in the rowspace of **W** sampled according to x.

Checkable Subspace Sampling

State-of-the-art

- Sonic:
  - Signature of correct computation: evaluation of $s(X, Y)$.
  - Complexity grows according to decomposition $\mathbf{W}$ as a sum of permutation matrices.
  - Amortized CSS: efficient and unrestricted.
- Marlin, Lunar:
  - Linear encoding for sparse matrices, relatively large SRS.
- Our work:
  - Extended Vandermonde Sampling.
  - Reduce SRS size by decomposing Marlin's CSS into simpler building blocks.
  - Limited fan-out.

Take away details

Why?

- Decomposing constructions of universal and updatable SNARKs into blocks that have a well defined algebraic meaning.
- Captures several constructions.
- In fact, CSS is the main bottleneck in efficiency/generality in these constructions.
- Isolating this component allows to focus on improvements.
- Mix and match: we can combine different CSS arguments.

Thank you!

https://eprint.iacr.org/2021/590

carla.rafols@upf.edu, arantxa.zapico@upf.edu