Succinct Proofs and Polynomial Commitments

Last Time:

Fiat-Shamir Heuristic

Replacing $\mathcal{V}$ with H in a public-coin protocol yields a non-interactive (RO) proof

This Time:

1. Succinct Proofs

2. Succinctness from the PCP Theorem !!!
   (and merkle trees)

3. Polynomial Commitments

Succinct Proofs: Motivation

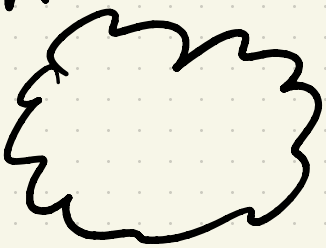
- Verifiable outsourcing

Alice

untrusted

Amazon

$\xrightarrow{f,\ x}$



short!

$O(1)$

$y \leftarrow f(x)$

$\xleftarrow{y,\ \pi}$

$\pi \leftarrow \mathrm{Prove}(f, x, y)$

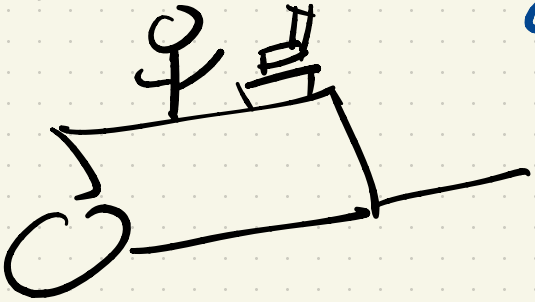
not too slow

$\mathrm{Verify}(f, x, y, \pi) \leftarrow$ fast!

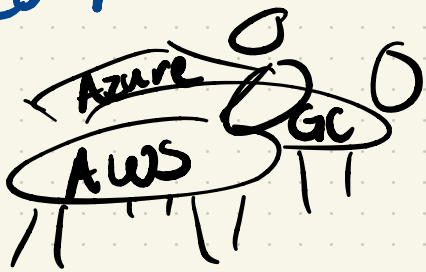
$O(|x|+|y|)$

$\downarrow$

$\{0,1\}$



herd of untrusted computers



Formalizing Succinctness: SNARGs

- $R(x, w)$ an NP-relation
- Verifier knows x
- Prover knows x, w
- Two algs:
  - $\text{Prove}(R, x, w) \to \pi$
  - $\text{Verify}(R, x, \pi) \to \{0, 1\}$
- Succinctness
  - $|\pi|$, T_{verify} are $o(|w|)$ (ideally: $|\pi| = O(1)$, $T_{ver} = O(|x|)$)
- Non-interactive (e.g. via Fiat-Shamir)
- ARGument (not proof!)
  - $\to$ sound only for poly-time P^*.
- "SNARG"

Extensions to SNARGs

- Can add zero knowledge
- Can add knowledge-soundness
- together, these give a "ZK-SNARK"
- today, we'll stick to SNARGs
- really, SARGs (interactive)
  - Fiat-Shamir yields a SNARG

How to build a SNARG?

Strawman: $\mathcal{V}_R$ - the NP-verifier

$\pi = w$ ← too big

$\text{Verify}(R, x, \pi) = \mathcal{V}_R(x, \pi)$

$O(|x| + |w|)$ time, just to <u>read the input</u>.

Necessary?

Can we "spot check" proofs?

Amazingly, YES!

The PCP Theorem

"Probabilistically Checkable Proofs"

For any $R(x, w) \in NP$

there are

- $\text{PCP.Prove}_R(x, w) \to \pi \in \{0,1\}^{\text{poly}(|x|)}$
- $\text{PCP.Verify}_R(x, \pi) \to \{0,1\}$

which are complete & sound.

Furthermore,

$\text{PCP.Verify}_R(x, \pi)$ reads only

3 (random) bits of π

and runs in $O(|x|)$

time.

PCP story

$P(x,w) \to \pi$: 

$V(x) \to \{0,1\}$

- Complex proof
  - Multiple papers (80s, 90s)
    - Credits to: Arora, Babai, Feige, Goldwasser, Lovasz, Lund, Motwani, Rackoff, Safra, ...
  - Won the Gödel Prize ↻ for excellent single works
  - $O(1)$ bits
- Improvement [Johan Håstad '01]
  - 3 bits
  - Won the Gödel Prize, <u>again</u>
- Simpler proof [Irit Dinur '07]
  - based on expander graphs
  - only ?? 44 pages
  - won the Gödel prize <u>again</u>
- Applications to hardness of approximation
- We'll just use it...

PCP + Merkle Tree = SNARG

[Kilian '92] [Micali '94]

Prover(x, w)		Verifier(x)
$\pi \leftarrow \mathrm{PCP.Prove}_R(x, w)$		
$c \leftarrow \mathrm{Merkle.Commit}(\pi)$		$\mathrm{PCP.Queries}_R(x) \to i_1, i_2, i_3$
	$\xrightarrow{c}$	
	$\xleftarrow{(i_j)}$	
for $j \in \{1,2,3\}$: $p_j \leftarrow \mathrm{Merkle.Open}(\pi, i_j)$, $x_j \leftarrow \pi[i_j]$		
	$\xrightarrow{((x_j, p_j))}$	
		$3\times$ MerkleVerify $\wedge$ PCP.Verify

Complete? Perfectly!

Sound? Yes, because (informal)

→ PCP is sound

→ Merkle openings are correct (assuming collision resistance)

Zero Knowledge?

→ No (V sees 3 bits)

→ but ZK can be added [Kilian '97]

Succinct?

→ Yes: $O(\log_2|w|)$ communication

Practical?

→ No :(

Merkle Trees + PCP Theorem

- very practical
- used frequently

- theoretical
- unimplemented
- big constants

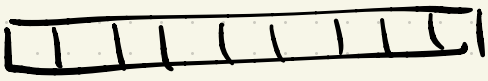
Observation: Our two subsystems are unbalanced...

Idea: Use a weaker proof system (~~PCP~~)

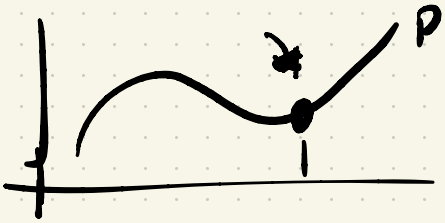
and a stronger commitment scheme

Polynomial Commitments

- vector commitments open to elements
  polynomial commitments open to evaluations

x: 

(i, x_i)



$(x, p(x))$

Prover (polynomial f) | **Verifier ()**

$c \leftarrow \text{Commit}(f)$

$\xrightarrow{\quad c \quad}$

$x_1 \xleftarrow{\$} ?$

$\xleftarrow{\quad x_1 \quad}$

$y_1 \leftarrow f(x_1)$

$\pi_1 \leftarrow \text{Open}(f, x_1) \xrightarrow{\quad y_1, \pi_1 \quad}$

$\text{Check}(\pi_1, c, x_1, y_1)$

In more detail, a polynomial commitment scheme has 4 algorithms:

degree bound public parameters

- $\text{Setup}(d) \to pp$
- $\text{Commit}(pp, f) \to c$
- $\text{Open}(pp, f, x) \to \pi$
- $\text{Check}(pp, c, x, y, \pi) \to \{0,1\}$

Correctness:

$\forall d \ \forall f.\ \deg(f) \le d \ \forall x \in \mathbb{F}$

$$\Pr\left[\begin{array}{l} pp \leftarrow \text{Setup}(d) \\ c \leftarrow \text{Commit}(pp, f) \\ \pi \leftarrow \text{Open}(pp, f, x) \\ y \leftarrow f(x) \end{array} : \text{Check}(pp, c, x, y, \pi) = 1\right]$$

is 1.

Evaluation Binding

$\forall d \; \forall$ PPT $\mathcal{A}$

$$\Pr\left[\begin{array}{l} pp \leftarrow \mathrm{setup}(d) \\ (f, c, x, y, y', \pi, \pi') \leftarrow \mathcal{A}(d, pp) \\ : \; 1 = \mathrm{Check}(pp, c, x, y, \pi) \\ \quad \wedge \; 1 = \mathrm{Check}(pp, c, x, y', \pi') \end{array}\right]$$

is negligible in λ

There are various "knowledge" <u>security definitions</u> too

- e.g. "a prover who creates valid openings must "know" a matching polynomial"
- important, but complex
- we'll ignore them.

Polynomial Review

(univariate!)

A polynomial $p: \mathbb{F} \to \mathbb{F}$ is a function defined by

$$p(x) = \sum_{i=0}^{d} c_i x^i \qquad c_i \in \mathbb{F}$$

a polynomial's degree is its largest non-zero coefficient.

Polynomials support

- $(+)$ $(-)$ $(\times)$
- quotient-remainder division
  - $f(x) = q(x)\,d(x) + r(x)$

    $\deg(r) < \deg(d)$
  - because they're a "euclidean domain"

- A polynomials roots are the inputs where it is zero

Notation: $\mathbb{F}^{\leq d}[X]$

variable name

max degree

set of polynomials

coeffients from here

Polynomial Facts:

"Schwartz-Zippel Lemma"

- for all $f \in \mathbb{F}^{\leq d}[X]$,

$$\Pr[x \xleftarrow{\$} \mathbb{F} : f(x) = 0] \leq \frac{d}{|\mathbb{F}|}$$

- $f(X)$ is divisible by $X - a$ iff it has a root at a.

$\Rightarrow$ $f(a) = y$ iff $f(X) - y$ is divisible by $X - a$

Polynomial Commitments from pairings

"KZG" construction: [Kate, Zaverucha, Goldberg '10]

Given $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ with generators g_1, g_2 and orders p.

must discard α!

Setup(d): $\alpha \xleftarrow{\$} \mathbb{F}_p$

$$pp \leftarrow \left((g_1^{\alpha^0}, g_1^{\alpha^1}, \ldots g_1^{\alpha^d}), g_2^{\alpha} \right)$$

Commit(pp, f):

$$c \leftarrow g_1^{f(\alpha)} = \prod_{i=0}^{d} (g_1^{\alpha^i})^{f_i}$$

τ from pp

Open(pp, f, x): $f'(X) \leftarrow \dfrac{f(X) - f(x)}{X - x}$

$$\pi \leftarrow g_1^{f'(\alpha)} = \prod_{i=0}^{d-1} (g_1^{\alpha^i})^{f'_i}$$

Check(pp, c, x, y, π):

$$e(\pi, g_2^{\alpha} / g_2^{x}) \stackrel{?}{=} e(c / g_1^{y}, g_2)$$

Correctness

$$e(\pi, g_2^{\alpha - x}) \stackrel{?}{=} e(g_1^{f(\alpha) - y}, g_2)$$

$$f'(\alpha)(\alpha - x) \stackrel{?}{=} f(\alpha) - y$$

$$f'(\alpha) \stackrel{?}{=} \frac{f(\alpha) - y}{\alpha - x}$$

✓, by defn.

Evaluation Binding

Assuming "t-SDH", KZG'10 is eval. binding, for degree bound t.

t-SDH: Given

$$(g_1, g_1^{\alpha}, g_1^{\alpha^2}, \ldots g_1^{\alpha^t}, g_2, g_2^{\alpha})$$

← Basis of RO-free BLS signatures

it is hard to find

$$y, g_1^{\frac{1}{\alpha - y}}$$

Proof: Suppose A is an index-binding adv. for KZG'10. We build B, a t-SDH adv.

A	B	t-SDH Challenger
		$\alpha \xleftarrow{\$} \mathbb{F}$
	$\xleftarrow{\text{same, as PP}}$	$g_1^{\alpha}\ g_1^{\alpha^2} \cdots g_1^{\alpha^t}$ $g_2\ g_2^{\alpha}$
	$\xrightarrow{c,\ x,\ y,\ \pi,\ y',\ \pi'}$	

$y \neq y'$

now what?

$e(\pi, g_2^{\alpha}/g_2^{x}) = e(c/g_1^{y}, g_2)$ $\quad$ $e(\pi', g_2^{\alpha}/g_2^{x}) = e(c/g_1^{y'}, g_2)$

$\downarrow$ $\qquad\qquad$ $\downarrow$

$\pi^{\alpha - x} = c/g_1^{y}$ $\qquad$ $\pi'^{\alpha - x} = c/g_1^{y'}$

divide!

$$(\pi/\pi')^{\alpha - x} = g_1^{y' - y}$$

$$h \leftarrow (\pi/\pi')^{\frac{1}{y' - y}} = g_1^{\frac{1}{\alpha - x}}$$

computable, since $y \neq y'$ $\longrightarrow$ (x, h)

t-SDH break.

Knowledge-soundness provable in the algebraic group model, see

"Marlin" Chiesa, Hu, Maller, Mishra, Vesely, Ward '19

"Sonic" Maller, Bowe, Kohlweiss, Meiklejohn '19

→ requires slight changes to scheme.

→ see "Marlin" for details

Problem: Trusted Setup

A trusted setup is a setup procedure whose randomness must be discarded for security

→ Controversial! (who runs its)

→ Motivates secure multiparty computation (MPC)

→ See RadioLab's "The Ceremony" for the story behind running a trusted setup

Recap:

1. Succinct Arguments

   $|\pi| = o(|\omega|)$

2. Succinctness from the PCP theorem

   ↑ cool, but impractical

3. Polynomial Commitments

   → Hope: stronger commitment, more practical SNARK

Next Time:

Succinctness from polynomial commitments