Lecture 12: NIZKs from the BGN cryptosystem

Zero-knowledge proofs

263-4665-00L

Lecturer: Jonathan Bootle

Announcements

- Exercise sheet 13 posted on Moodle
- Graded, 10% of final grade
- Submit through Moodle on or before 23:59, 15/12/2023
- Please email if you think you've found a typo or mistake

- 15/12/2023 exercise session to be used for exploring libraries for implementing zero-knowledge
- Still working on extra (optional, non-examinable) video about reducing verification costs for polynomial commitments.

Last time

- Compiling IP/IOP protocols into zero-knowledge argument.
- NIZKs without setup only cover languages in **BPP**.

Agenda

- **Non-interactive zero-knowledge (NIZK) definitions**

Pairing-based constructions of NIZK

- From reasonable cryptographic assumptions

$O(N)$ proof size for Boolean circuits

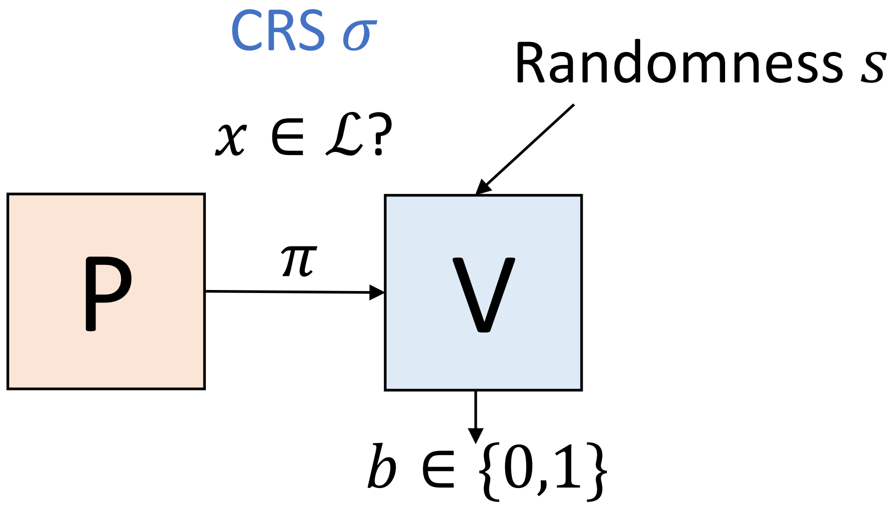
- From strong cryptographic assumptions

$O(1)$ proof size for Arithmetic circuits

Syntax for non-interactive zero-knowledge

- Include a common reference string (CRS)

containing ingredients used in the proof.



Definition:

A *non-interactive proof system* for an NP relation $\mathcal{R}$ consists of three efficient algorithms (K, P, V) which are

- the CRS generator $K(1^\lambda) \to \sigma$,
- the prover $P(\sigma, x, w) \to \pi$,
- the verifier $V(\sigma, x, \pi) \to b$.

Suppressing random inputs

K may take $|x|$ or even x as input

Ideally σ is uniformly random but may be structured

Security of non-interactive proofs

Easy to modify to get computational and statistical security notions

- **Completeness:** $\forall (x, w) \in \mathcal{R}$,

Adaptive

$$\Pr[b = 1 | \sigma \leftarrow K(1^\lambda), \pi \leftarrow P(\sigma, x, w), b \leftarrow V(\sigma, x, \pi)] = 1$$

- **Soundness:** $\forall P^*$,

$$\Pr[x \notin \mathcal{L}_\mathcal{R}, b = 1 | \sigma \leftarrow K(1^\lambda), (x, \pi) \leftarrow P^*(\sigma), b \leftarrow V(\sigma, x, \pi)] \approx 0$$

Adaptive

- **Zero-knowledge:** $\exists$ efficient simulators (S_1, S_2) such that $\forall A$ producing $(x, w) \in \mathcal{R}$,

Simulated σ indistinguishable from normal σ

$$\{(\sigma, \pi) : \sigma \leftarrow K(1^\lambda), (x, w) \leftarrow A(\sigma), \pi \leftarrow P(\sigma, x, w)\}$$
$$\approx \{(\sigma, \pi) : (\sigma, \tau) \leftarrow S_1(1^\lambda), (x, w) \leftarrow A(\sigma), \pi \leftarrow S_2(\sigma, x, \tau)\}$$

Simulation trapdoor τ (replaces oracle access to V^*)

In non-adaptive definitions, x is not chosen based on σ

These are *single-theorem* definitions. No security guarantees reusing σ for many x.

Knowledge soundness

Definition:

(K, P, V) is a *proof of knowledge* for a relation $\mathcal{R}$ if $\exists$ efficient extractors E_1, E_2 such that for all P^*,

Extractor's σ indistinguishable from normal σ

Extraction trapdoor ξ
(replaces oracle access to P^*)

- $\{\sigma : (\sigma, \xi) \leftarrow E_1(1^\lambda)\} \approx \{\sigma : \sigma \leftarrow K(1^\lambda)\}$, and

- $\Pr\left[\begin{array}{c} V(\sigma, x, \pi) = 0 \\ \vee\ (x, w) \in \mathcal{R} \end{array} : \begin{array}{c} (\sigma, \xi) \leftarrow E_1(1^\lambda), (x, \pi) \leftarrow P^*(\sigma) \\ w \leftarrow E_2(\sigma, \xi, x, \cancel{pi}) \end{array}\right] \approx 1.$

π

$V(\sigma, x, \pi) \Rightarrow (x, w) \in \mathcal{R}$

$=1$

How can we trust the CRS?

- Simulation trapdoors let us produce proofs without knowing witnesses (breaking soundness)
- Extraction trapdoors let us extract witnesses from proofs (breaking ZK)
- Trapdoor σ are indistinguishable from normal σ.

Mitigate risks using

- "Subversion resistant" NIZK constructions
- "Updatable CRS" NIZK constructions
- "Verifiable CRS" NIZK constructions
- MPC protocols to generate σ

How can we trust the CRS?

[2] This curious property makes our result potentially applicable. For instance, all libraries in the country possess identical copies of the random tables prepared by the Rand Corporation. Thus, we may think of ourselves as being already in the scenario needed for noninteractive zero-knowledge

TV & Videos Newsletters Podcasts **CoinDesk** Indices Consensus

Markets Companies Policy Technology Web3 Learn Layer 2 Sponsored Content

Bitcoin $16,951.26 -0.55% Ethereum $1,275.48 -0.93% Binance Coin $291.19 -2.34% XRP $0.39707680 -2.47% Bi Crypto Prices → CoinDesk Market Index →

Tech

Edward Snowden Played Key Role in Zcash Privacy Coin's Creation

The NSA whistleblower and privacy advocate was one of six participants in the cryptocurrency's fabled 2016 "trusted setup" ceremony, using a pseudonym.

By Naomi Brockwell Apr 27, 2022 at 10:17 p.m. Updated Apr 28, 2022 at 7:13 p.m.

Agenda

- Non-interactive zero-knowledge (NIZK) definitions ✓

Pairing-based constructions of NIZK

- **From reasonable cryptographic assumptions**
  - The BGN cryptosystem
  - BGN bit proofs
  - BGN proofs for CSAT

$O(N)$ proof size for Boolean circuits

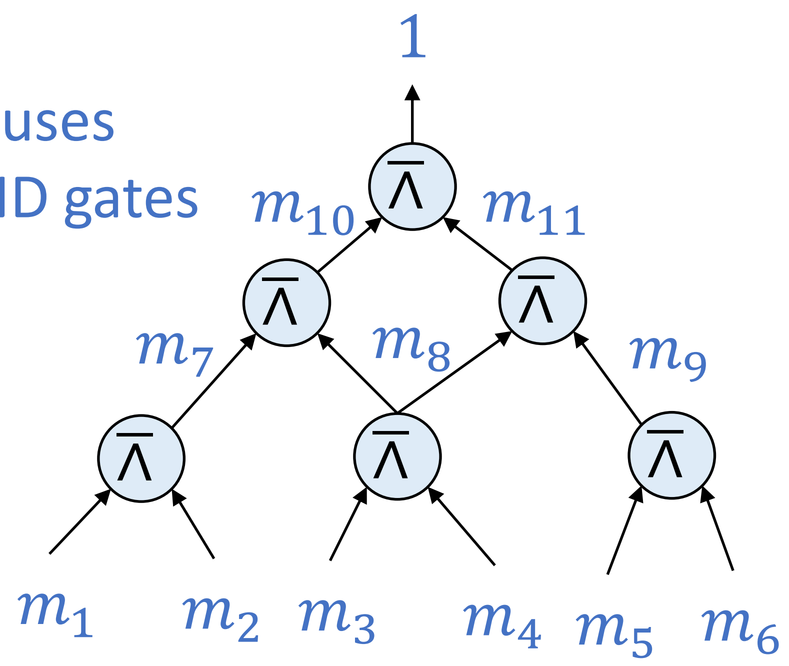
- From strong cryptographic assumptions

$O(1)$ proof size for Arithmetic circuits

Boolean circuit NIZK idea

$\mathbb{x}$ = circuit description
$\mathbb{w}$ = satisfying wire values

W.L.O.G. uses only NAND gates



Instance: circuit over $\mathbb{Z}_2$ with output.

Witness: input wire values giving correct output.

a	b	c	$\overline{a \wedge b} == c$	$a+b+2c-2$
0	0	0	0	-2
0	0	1	1	0
0	1	0	0	-1
0	1	1	1	1
1	0	0	0	-1
1	0	1	1	1
1	1	0	1	0
1	1	1	0	2

$$\overline{a \wedge b} = c \Leftrightarrow a + b + 2c - 2 \in \{0,1\}$$

Proof idea:

- Commit to each wire value.
- Prove each wire value $\in \{0,1\}$.
- Prove $\mathrm{a} + \mathrm{b} + 2\mathrm{c} - 2 \in \{0,1\}$ for wires around each gate.

Need a commitment scheme with NI bit proofs

Composite-order symmetric pairings

Definition:

A *symmetric bilinear group* is a triple of two groups of order $n = pq$ (where p, q are distinct primes) and a *bilinear map* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ satisfying

$$\forall a, b \in \mathbb{Z}_p, \forall G_1, G_2 \in \mathbb{G},$$
$$e(a \cdot G_1, b \cdot G_2) = ab \cdot e(G_1, G_2)$$

Pairing maps 'multiply DLOGs'

which is non-degenerate i.e.

If $\mathbb{G} = \langle G_1 \rangle = \langle G_2 \rangle$, then $\mathbb{G}_T = \langle e(G_1, G_2) \rangle$

Changes from last time:

- Order n instead of p
- "Type 1" symmetric setting with $\mathbb{G}_1 \cong \mathbb{G}_2 \cong \mathbb{G}$

Facts

Claim: (symmetry)

$\forall G_1, G_2 \in \mathbb{G}, e(G_1, G_2) = e(G_2, G_1)$

Proof:

Let $\mathbb{G} = \langle G \rangle$. Write $G_1 = a \cdot G$ and $G_2 = b \cdot G$. Then

$e(G_1, G_2) = ab \cdot e(G, G) = ba \cdot e(G, G) = e(G_2, G_1)$ by bilinearity.

Both claims together imply homomorphism in the right input

Claim:

$\forall G_1, G_2, H \in \mathbb{G}, e(G_1 + G_2, H) = e(G_1, H) + e(G_2, H)$.

Proof: exercise

The Boneh-Goh-Nissim Cryptosystem

Large enough that n is difficult to factor e.g. $O(\lambda^3)$ bits

Setup: on input $\lambda \in \mathbb{N}$, sample distinct primes p, q and composite order symmetric bilinear group $e, \mathbb{G}, \mathbb{G}_T$ of order $n = pq$, and $G, H \in \mathbb{G}$.

Sample $B \in \mathbb{N}$. Output $pp \coloneqq (e, \mathbb{G}, \mathbb{G}_T, G, H, n, B)$.

$B \leq \text{poly}(\lambda)$

Exact sampling method to be discussed

Commit: given $m \in \{0, \ldots, B-1\}, pp$, sample $r \leftarrow \mathbb{Z}_n$.

Compute $C = m \cdot G + r \cdot H$. Output (C, r).

Verify: check $m \in \{0, \ldots, B-1\}$ and $C == m \cdot G + r \cdot H$.

Homomorphic (looks like Pedersen)

For us, a commitment scheme (but can be used as an encryption scheme)

Dual-mode parameter generation

- $\mathbb{G}$ has order $n = pq$.
- $\text{Setup}_{binding}$: $G \leftarrow \mathbb{G},\ s \leftarrow \mathbb{Z}_n^*,\ H = ps \cdot G$.

random generator of order q subgroup

a generator (w.h.p.)

- Setup_{hiding}: $G \leftarrow \mathbb{G},\ s \leftarrow \mathbb{Z}_n^*,\ H = s \cdot G$.

random generator of whole group $\mathbb{G}$

binding setup will output a subgroup, so we define subgroup hiding

Definition:

The subgroup hiding assumption holds if

$$\{\text{Setup}_{binding}(1^\lambda)\} \approx_c \{\text{Setup}_{hiding}(1^\lambda)\}$$
$$\{G, ps \cdot G\} \approx_c \{G, s \cdot G\}$$

The BGN cryptosystem is hiding

Proof:

- Using Setup_{hiding}: $G \leftarrow_{\$} \mathbb{G},\ s \leftarrow_{\$} \mathbb{Z}_n^*,\ H = s \cdot G$. random generator of whole group $\mathbb{G}$
- For $r \leftarrow_{\$} \mathbb{Z}_n$, $r \cdot H$ is uniformly random in $\mathbb{G}$.
- Hence $C = m \cdot G + r \cdot H$ is uniformly random in $\mathbb{G}$.
- Therefore Setup_{hiding} gives *perfect* hiding.

  With Setup_{hiding}, BGN is *equivocable* with equivocation key s.

  $C = m \cdot G + r \cdot H = m' \cdot G + r' \cdot H$ where $r' := r + \frac{m - m'}{s} \bmod n$.

- The output of $\mathrm{Setup}_{binding}$ is computationally indistinguishable from Setup_{hiding} under the subgroup hiding assumption.
- Therefore $\mathrm{Setup}_{binding}$ still gives *computational* hiding.

The BGN cryptosystem is perfectly binding

Proof:

random generator of order q subgroup

- Using $\text{Setup}_{binding}$: $G \leftarrow_\$ \mathbb{G}$, $s \leftarrow_\$ \mathbb{Z}_n^*$, $H = ps \cdot G$.
- Suppose $C = m \cdot G + r \cdot H = m' \cdot G + r' \cdot H$ for distinct $m, m' \in \{0, \dots, B-1\}$.
- Then $e(C, q \cdot G) = e(m \cdot G + r \cdot H, q \cdot G) = e(m \cdot G + rps \cdot G, q \cdot G)$
$$= qm \cdot e(G,G) + rspq \cdot e(G,G) = qm \cdot e(G,G)$$
- Similarly, $e(C, q \cdot G) = qm' \cdot e(G,G)$. Hence $q(m - m') \cdot e(G,G) = 0$.
- By non-degeneracy, $e(G,G)$ has order n so $n \mid q(m - m')$.
- Hence $q(m - m') = kn$, so $(m - m') = kp$.
- $m \equiv m' \bmod p$ but $B \ll p$ so $m = m'$.

With $\text{Setup}_{binding}$, BGN is *extractable* with extraction key ~~s~~. $q \cdot G$

Compute $e(C, q \cdot G)$, check whether it is equal to $qm \cdot e(G,G)$ for each $m \in \{0, \dots, B-1\}$.

- The output of Setup_{hiding} is computationally indistinguishable from $\text{Setup}_{binding}$ under subgroup hiding, so Setup_{hiding} gives *computational* binding.

Agenda

- Non-interactive zero-knowledge (NIZK) definitions ✓

Pairing-based constructions of NIZK

- From reasonable cryptographic assumptions
  - The BGN cryptosystem ✓
  - **BGN bit proofs**
  - BGN proofs for CSAT

$O(N)$ proof size for Boolean circuits

- From strong cryptographic assumptions

$O(1)$ proof size for Arithmetic circuits

Proof for committed bits

Setup choice didn't matter

- $\mathcal{R} := \{((\sigma, C), (m, r)) : C \in \mathbb{G},\ m \in \{0,1\}, r \in \mathbb{Z}_n, C = m \cdot G + r \cdot H\}$.

$K(1^\lambda)$ Hiding or binding

Output $\sigma = (e, \mathbb{G}, \mathbb{G}_T, G, H, n)$ from BGN setup.

$P(\sigma, C, m, r)$

Compute $\pi := r(2m-1) \cdot G + r^2 \cdot H \in \mathbb{G}$.

$V(\sigma, C, \pi)$

Output $(e(C, C - G) == e(\pi, H))$.

Proof idea: C commits to m

$C - G$ commits to $m - 1$

$m \in \{0,1\}$

$\Updownarrow$

$m(m-1) = 0$

Pairing 'multiplies' committed values.

π is the leftover terms.

Completeness:

Suppose $m \in \{0,1\}, r \in \mathbb{Z}_n$,

$C = m \cdot G + r \cdot H$, and

$\pi = r(2m-1) \cdot G + r^2 \cdot H$.

We have $e(C, C - G)$

$= e(m \cdot G + r \cdot H, (m-1) \cdot G + r \cdot H)$

$= m(m-1) \cdot e(G, G)$ Bilinearity

$+ mr \cdot e(G, H) + (m-1)r \cdot e(H, G)$

$m(m-1) = 0$ $\quad + r^2 \cdot e(H, H)$ Symmetry and bilinearity

$= r(2m-1) \cdot e(G, H) + r^2 \cdot e(H, H)$

$= e(r(2m-1) \cdot G + r^2 H) = e(\pi, H)$

So V always accepts.

m is uniquely determined

Soundness analysis

$C = m \cdot G + r \cdot H$
$= m \cdot G + \frac{m_* - m}{ps} ps \cdot G$
$= m_* \cdot G$

- Using $\text{Setup}_{binding}$: $G \leftarrow_\$ \mathbb{G},\ s \leftarrow_\$ \mathbb{Z}_n^*,\ H = ps \cdot G$.
- $\mathbb{G} = \langle G \rangle$ so $\exists m_* \in \mathbb{Z}_n$ with $C = m_* \cdot G$.
- Let $m \coloneqq m_* mod\ p$ and $r \coloneqq \frac{m_* - m}{ps} mod\ n$. Then $C = m \cdot G + r \cdot H$.
- $\forall G' \in \mathbb{G}, q \cdot e(G', H) = spq \cdot e(G', G) = 0$. Group has order $n = pq$.

- If $e(C, C - G) = e(\pi, H)$ then expanding $e(C, C - G)$ gives

$m(m-1) \cdot e(G, G) + e\big(r(2m-1) \cdot G + r^2 \cdot H, H\big) = e(\pi, H)$.

- $qm(m-1) \cdot e(G, G) + q \cdot e\big(r(2m-1) \cdot G + r^2 \cdot H, H\big) = q \cdot e(\pi, H)$.
- $\Rightarrow qm(m-1) \cdot e(G, G) = 0$. $e(G, G)$ has order n by non-degeneracy
- $\Rightarrow qm(m-1) = kn$ for some $k \in \mathbb{Z}$. Hence $m(m-1) = kp$.
- $m(m-1) = 0\ mod\ p$. $m < p$ so $m \in \{0,1\}$

'Almost' knowledge soundness analysis

$E_1(1^\lambda) \to (\sigma, \xi := q \cdot G)$
Using BGN binding setup.

$E_2(\sigma, C, \pi) \to m \in \{0,1\}$
Using commitment extraction.

'almost' knowledge soundness because we only get m and not r satisfying $C = m \cdot G + r \cdot H$.

We want $\{\sigma : (\sigma, \xi) \leftarrow E_1(1^\lambda)\} \approx \{\sigma : \sigma \leftarrow K(1^\lambda)\}$, and $\Pr\left[\begin{array}{c} V(\sigma, x, \pi) = 0 \\ \vee\ (x, w) \in \mathcal{R} \end{array} : \begin{array}{c} (\sigma, \xi) \leftarrow E_1(1^\lambda), (x, \pi) \leftarrow P^*(\sigma) \\ w \leftarrow E_2(\sigma, \xi, x, pi) \end{array}\right] \approx 1.$

Why are $\boldsymbol{\sigma}$ from $\boldsymbol{K}$, $\boldsymbol{E_1}$ indistinguishable?

- Trivially if K uses binding setup. Computationally if K uses hiding setup.

Why is the output of $\boldsymbol{E_2}$ a witness?

- E_2 extracts the unique m from the previous slide.
- The soundness analysis shows that $m \in \{0,1\}$.

Proof uniqueness (witness indistinguishabilility)

- Using Setup_{hiding}: $G \leftarrow_\$ \mathbb{G},\ s \leftarrow_\$ \mathbb{Z}_n^*,\ H = s \cdot G$.

- Suppose $\pi_1, \pi_2 \in \mathbb{G}$ satisfy $e(\pi_1, H) = e(\pi_2, H) = e(C, C - G)$.
- Writing $\pi_i = a_i \cdot G$, we have $a_1 \cdot e(G, H) = a_2 \cdot e(G, H)$.
- Hence $(a_1 - a_2) \cdot e(G, H) = 0$.
- Hence $a_1 - a_2 \equiv 0 \mod n$, so $a_1 = a_2$ and $\pi_1 = \pi_2$.

Non-degeneracy ⇒ $e(G, H)$ has order n since both G, H are generators.

- Therefore, $\forall C \in \mathbb{G}$, there is at most one accepting proof $\pi \in \mathbb{G}$.

With Setup_{hiding}, BGN is *equivocable* with equivocation key s.
$\mathbb{G} = \langle G \rangle$ so $\exists m \in \mathbb{Z}_n$ with $C = m \cdot G$.
$C = m \cdot G = 0 \cdot G + r' \cdot H$ where $r' = \frac{m - m'}{s} \mod n$.

⇒ a valid proof exists based on $C = 0 \cdot G + r' \cdot H$

Agenda

- Non-interactive zero-knowledge (NIZK) definitions ✓

Pairing-based constructions of NIZK

- From reasonable cryptographic assumptions
  - The BGN cryptosystem ✓
  - BGN bit proofs ✓
  - **BGN proofs for CSAT**

$O(N)$ proof size for Boolean circuits

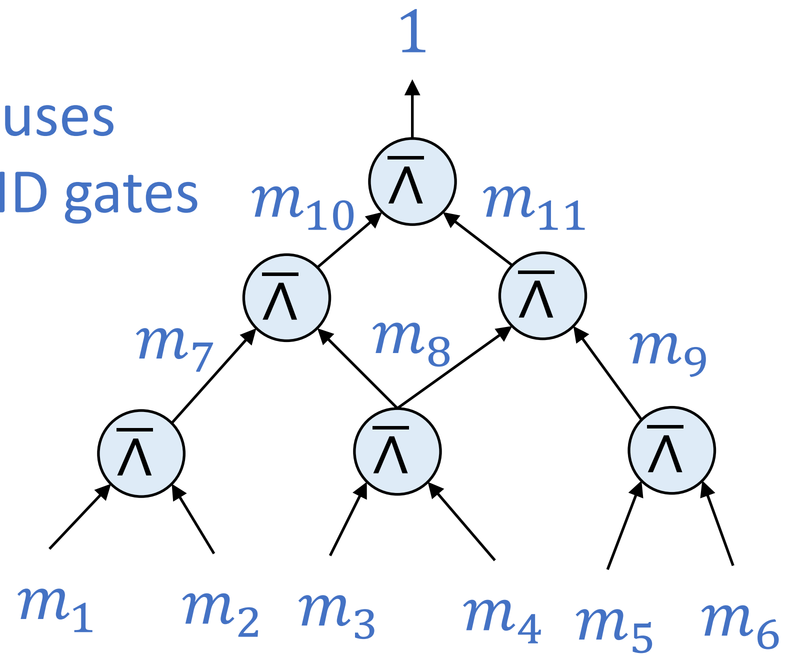
- From strong cryptographic assumptions

$O(1)$ proof size for Arithmetic circuits

$\mathbb{x}$ = circuit description
$\mathbb{w}$ = satisfying wire values

Boolean circuit NIZK idea

W.L.O.G. uses only NAND gates



Instance: circuit over $\mathbb{Z}_2$ with output.

Witness: input wire values giving correct output.

a	b	c	$\overline{a \wedge b} == c$	$a + b + 2c - 2$
0	0	0	0	-2
0	0	1	1	0
0	1	0	0	-1
0	1	1	1	1
1	0	0	0	-1
1	0	1	1	1
1	1	0	1	0
1	1	1	0	2

$$\overline{a \wedge b} = c \Leftrightarrow a + b + 2c - 2 \in \{0,1\}$$

Proof idea:

- Commit to each wire value.
- Prove each wire value $\in \{0,1\}$.
- Prove $\mathrm{a} + \mathrm{b} + 2\mathrm{c} - 2 \in \{0,1\}$ for wires around each gate.

Need a commitment scheme with NI bit proofs

$O(N)$ proof size and verification time

NIZK for Boolean satisfiability

$K(1^\lambda)$ Hiding or binding

Output $\sigma = (e, \mathbb{G}, \mathbb{G}_T, G, H, n)$ from BGN setup.

$P(\sigma, \mathbb{x}, \mathbb{w})$: For each m_i

- Sample $r_i \leftarrow_\$ \mathbb{Z}_n$. Compute $C_i = m_i \cdot G + r_i \cdot H \in \mathbb{G}$.
- Compute $\pi_i := r_i(2m_i - 1) \cdot G + r_i^2 \cdot H \in \mathbb{G}$.
- Compute $C_{out} = 1 \cdot G + 0 \cdot H \in \mathbb{G}$.
- For each gate $\overline{m_i \wedge m_j} = m_k$, compute

$C_{ijk} = m_{ijk} \cdot G + r_{ijk} \cdot H := C_i + C_j + 2 \cdot C_k - 2 \cdot G$.

- Compute $\pi_{ijk} := r_{ijk}(2m_{ijk} - 1) \cdot G + r_{ijk}^2 \cdot H \in \mathbb{G}$.
- Output $((C_i)_i, (\pi_i)_i, (\pi_{ijk})_{ijk})$.

$V(\sigma, C, \pi)$: Output 1 if and only if

$e(C_i, C_i - G) = e(\pi_i, H)$ for each i and similarly for each gate.

Completeness, soundness:

Immediate from the properties of the bit proofs.

Knowledge soundness:

- E_1 is the same as in the bit proofs (binding setup).
- For E_2, we use the bit proof extractor to extract each wire value.
- Bit proof soundness implies that each gate is satisfied.

No need to extract commitment randomness. 'Almost' knowledge soundness of bit proofs suffices.

Use equivocation key s to cheat openings and satisfy NANDs

Zero-knowledge analysis

$S_1(1^\lambda) \to (\sigma, \tau \coloneqq s)$
Using BGN hiding setup.

Using Setup_{hiding}: $G \leftarrow_\$ \mathbb{G}$, $s \leftarrow_\$ \mathbb{Z}_n^*$, $H = s \cdot G$.

What is the verifier's view?

$((C_i)_i, (\pi_i)_i, (\pi_{ijk})_{ijk})$

- Each C_i is uniformly random in $\mathbb{G}$.
- Each π_i and π_{ijk} is uniquely determined by the C_i.

Why is the simulator valid?

- The distributions of σ and C_i are identical and the bit proofs uniquely determined from these.

$S_2(\sigma, \mathbb{x}, \tau)$: For each wire, set $m_i \coloneqq 0$.

- Sample $r_i \leftarrow_\$ \mathbb{Z}_n$. Compute $C_i = m_i \cdot G + r_i \cdot H \in \mathbb{G}$.
- Compute $\pi_i \coloneqq r_i(2m_i - 1) \cdot G + r_i^2 \cdot H \in \mathbb{G}$.
- Compute $C_{out} = 1 \cdot G + 0 \cdot H \in \mathbb{G}$.
- For each gate $\overline{m_i \wedge m_j} = m_k$, use the trapdoor s to open C_k as $1 \cdot G + r_i' \cdot H$.
- Compute $C_{ijk} = m_{ijk} \cdot G + r_{ijk} \cdot H \coloneqq C_i + C_j + 2 \cdot C_k - 2 \cdot G$.
- Compute $\pi_{ijk} \coloneqq r_{ijk}(2m_{ijk} - 1) \cdot G + r_{ijk}^2 \cdot H \in \mathbb{G}$. Use $m_i = m_j = 0, m_k' = 1$.
- Output $((C_i)_i, (\pi_i)_i, (\pi_{ijk})_{ijk})$.

Summary of BGN-based NIZK

- $O(N)$ proof size and verification time for CSAT (hence all NP).

	Binding setup	Hiding setup
Knowledge soundness	Perfect	Computational
Zero-knowledge	Computational	Perfect

- Composite order symmetric pairings $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, order $n = pq$.

- Subgroup hiding assumption $\{G, ps \cdot G\} \approx_c \{G, s \cdot G\}$.

Agenda

- Non-interactive zero-knowledge (NIZK) definitions ✓

Pairing-based constructions of NIZK

- From reasonable cryptographic assumptions
  - The BGN cryptosystem ✓
  - BGN bit proofs ✓
  - BGN proofs for CSAT ✓
- **From strong cryptographic assumptions**
  - Arithmetisation of R1CS into QAP
  - Polynomial IOP and pairing-based compiler

$O(N)$ proof size for Boolean circuits

$O(1)$ proof size for Arithmetic circuits

From R1CS to strong R1CS

$$\mathcal{R}_{R1CS} = \left\{ \left((\mathbb{F}, A, B, C, \vec{x}), \vec{w} \right) : \begin{array}{c} A, B, C \in \mathbb{F}^{N_r \times N_c}, \vec{x} \in \mathbb{F}^k \\ \vec{w} \in \mathbb{F}^{N_c - k}, \vec{z} := \vec{x} || \vec{w} \\ A\vec{z} \circ B\vec{z} = C\vec{z} \end{array} \right\}.$$

entry-wise product

$\vec{x}$ makes the problem non-trivial. W.L.O.G first entry is 1.

Definition: *strong* R1CS instances are as above, and additionally, if $\vec{z}_i := \vec{x} || \vec{w}_i$ for $i \in [3]$, $A\vec{z}_1 \circ B\vec{z}_2 = C\vec{z}_3$ implies that $\vec{z}_1 = \vec{z}_2 = \vec{z}_3$.

Lemma: for each R1CS instance, there is a *strong* R1CS instance with exactly the same witnesses and dimensions $N_r + 2N_c, N_c$.

Proof:

$$\begin{pmatrix} & A \\ & I_{N_c} \\ 1^{N_C} & 0_{N_c \times (N_c - 1)} \end{pmatrix} \vec{z}_1 \circ \begin{pmatrix} & B \\ 1^{N_C} & 0_{N_c \times (N_c - 1)} \\ & I_{N_c} \end{pmatrix} \vec{z}_2 = \begin{pmatrix} C \\ I_{N_c} \\ I_{N_c} \end{pmatrix} \vec{z}_3$$

$$\begin{pmatrix} A\vec{z}_1 \\ 1^{N_C} \\ \vec{z}_1 \end{pmatrix} \circ \begin{pmatrix} B\vec{z}_2 \\ \vec{z}_2 \\ 1^{N_C} \end{pmatrix} = \begin{pmatrix} C\vec{z}_3 \\ \vec{z}_3 \\ \vec{z}_3 \end{pmatrix}$$

Polynomial definitions and facts

- Let $H \subseteq \mathbb{F}$ with $|H| = N$.

$L_{h,H}(\omega) = (\omega == h)$

Definition:

- The *Lagrange polynomials* on H are defined, for $h \in H$, by

$$L_{h,H}(X) \coloneqq \prod_{h' \in H \setminus \{h\}} \frac{X - h'}{h - h'}$$

Degree $|H| - 1$.

- The *vanishing polynomial* on H is defined as $v_H(X) \coloneqq \prod_{h \in H}(X - h)$.

Fact:

Degree $|H|$.

For $f \in \mathbb{F}[X]$, we have $f(h) = 0\ \forall h \in H \Leftrightarrow v_H(X) \mid f(X)$.

R1CS as polynomial divisibility

- Choose $H = \{1, \dots, N_r\} \subseteq \mathbb{F}$ (there are better choices).
- For each $j \in [N_c]$, define $a_j(X) := \sum_{i \in [N_r]} a_{ij} L_{i,H}(X)$.
- Define $b_j(X)$, $c_j(X)$ similarly.
- Let $\vec{z} = (z_1, \dots, z_{N_c})$ be an R1CS witness.
- Define $A(X) := \sum_{j \in [N_c]} z_j a_j(X)$ and $B(X), C(X)$ similarly.

$A = (a_{i,j})$

Note that $a_j(i) = a_{i,j}$.

Lemma: $v_H(X) \mid A(X) \cdot B(X) - C(X) \iff A\vec{z} \circ B\vec{z} = C\vec{z}$.

Proof: $v_H(X) \mid A(X) \cdot B(X) - C(X) \Leftrightarrow A(X) \cdot B(X) - C(X)$ vanishes on H.

For each $i \in H = [N_r]$,

$$A(i)B(i) - C(i) = \left(\sum_{j \in [N_c]} z_j a_j(i)\right)\left(\sum_{j \in [N_c]} z_j b_j(i)\right) - \left(\sum_{j \in [N_c]} z_j c_j(i)\right)$$

$$= \left(\sum_{j \in [N_c]} z_j a_{ij}\right)\left(\sum_{j \in [N_c]} z_j b_{ij}\right) - \left(\sum_{j \in [N_c]} z_j c_{ij}\right) = (A\vec{z})_i (B\vec{z})_i = (C\vec{z})_i.$$