CONSTANT-ROUND CZK PROOFS for NP

ALON ROSEN

IDC HERZLIYA
Goal: construct proof for every $L \in \text{NP}$

- in computational $\text{ZK}$
- with negligible soundness
- and a constant number of rounds

Need to address:

- malleability
- aborts in simulation
Recall: CZK proof for $HAM$

- $G_0 = \pi(w)$
- $G_1 = \pi, \pi(G)$

- **Prover**: commit to $G_0, G_1$
- **Verifier**: send $b \in \mathbb{R} \{0, 1\}$
- **Prover**: decommit to $G_b$

- **Completeness**: can always make sure that $G_0, G_1$ are valid
- **Soundness**: either $G_0$ or $G_1$ is invalid
- **Zero-Knowledge**: given $b$ can always ensure that $G_b$ is valid
Zero-Knowledge

- $G_0 = \pi(w)$
- $G_1 = \pi, \pi(G)$

**Simulator**: sample $b \in_R \{0,1\}$

**Simulator**: commit to $G_0, G_1$ so that $G_b$ is valid

**Verifier***: send $b' = V^*(c)$

**Simulator**: if $b' = b$ decommit to $G_b$, otherwise repeat
Parallel repetition

- To reduce soundness error – repeat $k$ times in parallel
- **Problem**: $V^*$’s challenge is now a string $b \in_R \{0,1\}^k$
- Simulator’s expected number of guessing attempts is $2^k$
- **Solution**: Let verifier commit to $b$ in advance
Parallel $HAM$

- $G_0 = \pi_1(w), ..., \pi_k(w)$
- $G_1 = \pi_1, \pi_1(G), ..., \pi_k, \pi_k(G)$

- **Verifier**: commit to $b \in_R \{0,1\}^k$
- **Prover**: commit to $G_0, G_1$
- **Verifier**: decommit to $b$
- **Prover**: decommit to $G_{b_1}, ..., G_{b_k}$

**Soundness**:
- Relies on hiding of $Com$
- Probability that $G_{b_1}, ..., G_{b_k}$ are all valid is at most $2^{-k}$

**Zero-Knowledge**: given $b_i$ can ensure that $G_{b_i}$ is valid
Malleability of Prover Commitment

- *Com* must be statistically hiding

- Otherwise $P$ can generate $c = \text{Com}(G_0, G_1)$ that depends on $d = \text{Com}(b)$ so that upon seeing $b = \text{Dec}(d)$ he can generate valid $\text{Dec}(G_{b_1}, \ldots, G_{b_k})$

- Succeeding in doing so would not necessitate $P$ to violate the (computational) hiding property of *Com*

- “Man-in-the-middle” attacks are feasible and devastating

- This “malleability” issue is averted by using *Com* that is statistically hiding
**Statistically-hiding Commitments**

**Definition:** A statistically-hiding \((Com, Dec)\) satisfies:

**Statistical hiding:** \(\forall R^* \ \forall m_1, m_2\)
\[Com(m_1) \cong_s Com(m_2)\]

**Computational binding:** \(\forall PPT C^* \ \forall m_1 \neq m_2\)
\[Pr[C^* \text{ wins the binding game}] \leq neg(n)\]

- Can also consider commitments that are simultaneously computationally hiding and binding
- **Exercise:** There do not exist commitments that are simultaneously statistically hiding and binding
- **Instance-dependent:** hiding for \(x \in L\), binding for \(x \notin L\)
Examples (statistically-hiding)

- Pedersen (assuming DL):
  \[ \text{Com}_{g,h}(m, r) = h^r \cdot g^m \]

- Any CRH \( H: \{0,1\}^* \rightarrow \{0,1\}^n \):
  \[ \text{Com}_H(m, r) = (H(r), h(r) \oplus m) \]

- “Random oracle” \( H: \{0,1\}^* \rightarrow \{0,1\}^n \):
  \[ \text{Com}(m) = H(m) \]

- Any OWF: \( \text{poly}(n) \) rounds of interaction
(garbage: all 0’s string)

- **Verifier**: commit to $b \in_R \{0,1\}^k$
- **Simulator**: commit to garbage
- **Verifier\(^*\)**: decommit to $b$
- **Simulator**: rewind and adjust garbage to be valid
- **Com** is comp. binding so $V^*$ cannot decommit to $b' \neq b$
- But what if $V^*$ refuses to decommit altogether?
  - $V^*$ might ABORT w/ unknown probability $0 \leq p \leq 1$
  - Simulator needs to generate the correct distribution
A Naïve Simulator

(garbage: all 0’s string)

Naïve simulator:
• commit to garbage
• If $V^*(c) = \text{ABORT}$, halt
• If $V^*(c) \neq \text{ABORT}$,
  a) rewind and adjust garbage to be valid
  b) obtain decommitment to $b$ from $V^*$
  c) Repeat (a),(b) until $V^*(c) \neq \text{ABORT}$ again

The problem: $Pr[V^* \neq \text{ABORT}]$ may change depending on whether simulator committed to garbage or to valid
Let
\[ s(n) = Pr[V^* \neq \text{ABORT} | \text{garbage}] \]
\[ t(n) = Pr[V^* \neq \text{ABORT} | \text{valid}] \]

then
\[ \mathbb{E}[\#\text{repetitions of (a), (b)}] = s(n)/t(n) \]

Suppose that for infinitely many n’s
\[ s(n) = 2^{-n} \]
\[ t(n) = 2^{-2n} \]

Then for these n’s, \( s(n)/t(n) \) is too large!
Theorem [GK’91]: If statistically-hiding commitments exist then every $L \in \text{NP}$ has a ZK proof with soundness error $2^{-k}$

Round-optimal [K’12]: if a language $L$ has a four-round zero-knowledge proof then $L \in \text{coMA}$

The GK solution:

- have the simulator first obtain an estimate $\tilde{t}(n)$ on $t(n)$
- achieved by rewinding with valid commitment until $m(n)$ successful decommits occur for some $m(n) = \text{poly}(n)$
- In step (c), the simulator then repeats (a),(b) up to some $\text{poly}(n)/\tilde{t}(n)$ repetitions, unless $V^*(c) \neq \text{ABORT}$ again
The idea [R’04]: $V^*$ commits to challenge $b$ in a way that allows extraction of $b$ before $c$ is even sent

Stage I:

- **Verifier**: commit to $b \in R \{0,1\}^k$ and to
  
  \[
  \begin{pmatrix}
  b_1^0, b_2^0, \ldots, b_n^0 \\
  b_1^1, b_2^1, \ldots, b_n^1
  \end{pmatrix}
  \]
  
so that $\forall i \in [n]$, $b_i^0 \oplus b_i^1 = b$

- **Prover**: send $n$ random bits $r_1, \ldots, r_n \in R \{0,1\}^n$

- **Verifier**: decommit to $b_1^{r_1}, b_2^{r_2}, \ldots, b_n^{r_n}$

Stage II:

- Run 3-round protocol for $HAM$ (parallel version) with $b$ as challenge ($V$ decommits to $b$ and $b_1^{1-r_1}, \ldots, b_n^{1-r_n}$)
Simulating the protocol

Simulator:

• Learn $b$ using naïve rewinding by learning $b_i^0, b_i^1$ for some $i \in [n]$

$$\bigg( b_1^0, b_2^0, \ldots, b_n^0 \bigg) \rightarrow b_2^0 \oplus b_2^1 = b$$

• Given $b$ can simulate 3-round protocol

The point:

• rewinding s are non adaptive ($r_1, \ldots, r_k$ are random)
• $s(n) = t(n)$ by definition
The 5-round protocol seems to not be a POK:

- In order to extract, one must obtain different responses from the prover relative to the same first message $c$.
- However, $V$ (and thus extractor) is bound to $b$ before $P$ commits to $c$, and the value of $c$ may depend on $V$’s commitment to $b$.
- Thus the extractor cannot change the query $b$ without $P$ changing $c$.
The Solution

- $G_0, G_1$ as before

- **Prover**: commit to $G_0, G_1$

- **Verifier**: commit to $b_1 \in_R \{0,1\}^k$

- **Prover**: commit to $b_2 \in_R \{0,1\}^k$

- **Verifier**: decommit to $b_1$

- **Prover**: decommit to $b_2$ and $G_{c_1}, ..., G_{c_k}$ where $c = b_1 \oplus b_2$

---

**Theorem [L’12]**: If statistically-hiding commitments exist then every $L \in \text{NP}$ has a ZKPOK with soundness error $2^{-k}$
### ZK and POK

**Zero-knowledge:**
- Simulator guesses ahead of time a string \( c \)
- It then obtains \( b_1 \), and rewinds \( V \) in order to set \( b_2 \) such that \( b_1 \oplus b_2 = c \)

**Proof of knowledge:**
- Extractor rewinds \( P \) multiple times relative to the same first message
- It obtains multiple openings with different strings \( c = b_1 \oplus b_2 \)
- This enables extraction from the *HAM* protocol, albeit with some complications
Summary

Saw:
• CZK proof of knowledge $\forall L \in \mathsf{NP}$
• with negligible soundness
• and a constant number of rounds

Issues addressed:
• malleability
• aborts in simulation

Issues still to be addressed:
• public-coin
• Strict polynomial-time simulation
History

Ariel Kahan  Jonathan Katz  Yehuda Lindell  Alon Rosen

Ivan Damgård  Torben Pryds Pedersen  Birgit Pfitzmann

Ramarathnam Venkatesan  Moti Yung  Iftach Haitner  Omer Reingold
The End

Questions?