Comparison of Introductory Zero-Knowledge Proof Examples

By Navid Roux, 2020-05-22.

	Sudoku	**Hamiltonian Cycle**	**Any "hard" Graph Property**	**Discrete Log (variant)**	**Discrete Log (Schnorr variant)**
Statement public or sent from P to V	Partial sudoku Ψ is solvable	Graph G is Hamiltonian[1]	Let $L \in \mathsf{NP}$ be any graph-isomorphism-invariant graph property believed to be hard.[3] Graph $G \in L$	Let $\mathbb{G}$ of order q and $y \in \mathbb{Z}_q$ be fixed. I know $x \in \mathbb{Z}_q$ such that $[x] = y$	Let $\mathbb{G}$ of order q and $y \in \mathbb{G}$ be fixed. I know $x \in \mathbb{Z}_q$ such that $[x] = y$
Witness only known to P	Solution $\overline{\Psi}$	Hamiltonian cycle v	Certificate w	x	x
Iteration					
1. Rerandomization by P of 1. Problem Statement 2. Solution	Pick set isomorphism i on $\{1, \ldots, 9\}$ 1. $\Psi' := i[\Psi]$ is solvable 2. $\overline{\Psi}' := i[\overline{\Psi}]$ is solution to Ψ'	Pick graph isomorphism $i\colon G \to G'$ (just relabel vertices) 1. $G' := i[G]$ is Hamiltonian 2. $v' := i[v]$ is Hamiltonian cycle for G'[2]	Pick graph isomorphism $i\colon G \to G'$ (just relabel vertices) 1. $G' := i[G] \in L$ 2. $w' := i[w]$ is certificate for G'	Pick $r \leftarrow \mathbb{Z}_q$ uniformly at random	Pick $r \leftarrow \mathbb{Z}_q$ uniformly at random
2. Commitment by P	Send all of • $(\mathrm{com}(\Psi_{i,j}))_{1 \le i,j \le 9}$ • $\mathrm{com}(\Psi')$	Send all of • G' • $\mathrm{com}(i)$ • $\mathrm{com}(v')$	Send all of • G' • $\mathrm{com}(i)$ • $\mathrm{com}(w')$	Send all of • $\hat{g} := [r]$ • $\mathrm{com}(r)$	Send $[r]$
3. Pose Challenge by V	Ask for one of • permuted row i • permuted column j • permuted square k • permuted statement In total, this gives $9 + 9 + 9 + 1 = 28$ challenge types	Ask for one of • isomorphism $i\colon G \to G'$ • Hamiltonian cycle in G'	Ask for one of • isomorphism $i\colon G \to G'$ • certificate for $G' \in L$	Ask for one of • r • $x + r$ and denote response by resp.	Pick $c \leftarrow \mathbb{Z}_q$ uniformly at random. Ask for $cx + r$ and denote response by resp.
4. Respond to challenge by P	canonical: respond exactly with what was asked				
5. Verify response by V	Check • that no numbers occur twice in row, column, or square, • or that the permuted statement is in fact a permutation	Check • conditions on isomorphism, • or check that cycle is indeed Hamiltonian	Check • conditions on isomorphism, • or check that certificate is valid	Check • that indeed $\hat{g} = [\text{resp.}]$ • that $[\text{resp.}] = y + \hat{g}$ namely if indeed $[x] = y$, then $y + \hat{g} = [x] + [r] = [x + r] = [\text{resp.}]$	Check that $[\text{resp.}] = cy + [r]$
Completeness P can convince V in case P actually had a solution	Since step 4 above is canonical, provers can convince with prob. of 1				
Soundness P cannot convince V without having a solution. Shown are the prob. of convincing w/o having a sol.	$\approx \left(\frac{1}{28}\right)^{\#\text{iter}}$	$\left(\frac{1}{2}\right)^{\#\text{iter}}$	$\left(\frac{1}{2}\right)^{\#\text{iter}}$	$\left(\frac{1}{2}\right)^{\#\text{iter}}$	todo
Zero Knowledge V doesn't learn anything about the witness	todo	In each round, V learns *either* a useless isomorphism *or* a Hamiltonian cycle in $G' \cong G$. Since the graph isomorphism problem is believed to be hard, learning about such a cycle in G' without learning the isomorphism is useless as well.	Same argument as in the cell to the left.	In each round, V learns *either* a useless random r *or* $x + r$. In the latter case, however, since $r \sim \mathcal{U}(\mathbb{Z}_q)$, we also have $(x + r) \sim \mathcal{U}(\mathbb{Z}_q)$[4]	In each round, V only learns $[r]$ and $cx + r$ for a c chosen by them. Due to DLOG assumed to be hard in $\mathbb{G}$, in the eyes of V we have $r \sim \mathcal{U}(\mathbb{Z}_q)$ and hence $(cx + r) \sim \mathcal{U}(\mathbb{Z}_q)$.[4]

1 This means it contains a so-called Hamiltonian cycle that is a path visiting every node exactly once. The problem of finding such a cycle is NP-complete.
2 Here, v is effectively a sequence of edges, on which the isomorphism is applied elementwise.
3 Take for example $\mathsf{HAMILTONIAN}$, $\mathsf{3\text{-}COL}$, or CLIQUE. From $L \in \mathsf{NP}$ it follows that for every $G \in L$ there is a certificate w for membership of length $\mathrm{poly}(|G|)$ that can be verified in $\mathrm{poly}(|G|)$ time.
By graph-isomorphism invariance we demand that for $G \cong G'$ witnessed by an isomorphim $i\colon G \to G'$, certificates w for $G \in L$ can be transformed to certificates w' for $G' \in L$. We denote the latter by $i[w]$.
4 This is a simple lemma holding for arbitrary groups. The security of the OTP is based on this,
usually phrased in the language of the group $(\{0,1\}^n, \oplus)$.

Useful Links

- Sudoku (slightly different challenges are given, though)
  - `https://manishearth.github.io/blog/2016/08/10/interactive-sudoku-zero-knowledge-proof/`
  - `https://manishearth.github.io/sudoku-zkp/zkp.html`
- Hamiltonian Cycles: [Wik20b]
- Discrete Log (variant): [Wik20a]
- Discrete Log (Schnott variant)
  - Lecture Notes by Prof. Schröder on "Privacy-Preserving Cryptocurrencies" (currently non-public; only accessible to students enrolled in their course)
  - [Sch90]

References

[Sch90] C. P. Schnorr. "Efficient Identification and Signatures for Smart Cards". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by Gilles Brassard. New York, NY: Springer New York, 1990, pp. 239–252. ISBN: 978-0-387-34805-6.

[Wik20a] Wikipedia contributors. *Zero-knowledge proofs (Discrete log of a given value) — Wikipedia, The Free Encyclopedia*. [Online; accessed 2020-05-21]. 2020. URL: `https://en.wikipedia.org/w/index.php?title=Zero-knowledge_proof&oldid=957331895#Discrete_log_of_a_given_value`.

[Wik20b] Wikipedia contributors. *Zero-knowledge proofs (Hamiltonian cycle for a large graph)— Wikipedia, The Free Encyclopedia*. [Online; accessed 2020-05-21]. 2020. URL: `https://en.wikipedia.org/w/index.php?title=Zero-knowledge_proof&oldid=957331895#Hamiltonian_cycle_for_a_large_graph`.