Introduction to Zero Knowledge Proofs

Paul Staadecker

supervised by:
Professor Douglas Stebila

Department of Combinatorics and Optimization
University of Waterloo

Canadian Undergraduate Mathematics Conference, 2022

Big Idea:

Convince someone that some statement is true without revealing any information to them other than the truth of the statement.

Outline

Why are ZK Proofs Important in Cryptography?

Example: Proving Graph Isomorphism in ZK

Mathematical Details

- Interactive Protocols
- Properties of ZK Proofs

Example: Schnorr's Identification Protocol

A Software Implementation

Conclusion

Section 1

Why are ZK Proofs Important in Cryptography?

Proving Things in Cryptography

- Prove that you are the sender of a message
- Prove that you are authorized to access some service
- Prove that you performed some computation correctly

Things to Prove in Zero Knowledge

Recall: Prove something without revealing any other information

- Prove that you know some secret key without revealing the key
- Prove that the balance in your bitcoin account is above some threshold without revealing the balance
- Prove that you are at least 18 years old without revealing your birthday
- Prove that an election was held correctly without revealing any votes

Section 2

Example: Proving Graph Isomorphism in ZK

Recall: Graph Isomorphisms

Definition

A graph is a pair $G = (V, E)$:

- V is the vertex set
- E is the edge set, consisting of unordered pairs of elements in V

Definition

A graph isomorphism between two graphs $G_0 = (V_0, E_0)$ and $G_1 = (V_1, E_1)$ is a bijection $\phi : V_0 \to V_1$ satisfying $\{\phi(v), \phi(w)\} \in E_1$ iff $\{v, w\} \in E_0$, for each $v, w \in V$.

Two graphs are isomorphic if there exists an isomorphism between them.

Fact

There is no known way to determine whether two graphs are isomorphic efficiently.

Proving Graph Isomorphism in ZK

Example

Peggy and Victor know graphs G_0 and G_1.
Peggy also knows isomorphism ϕ between them.
How can Peggy prove to Victor that G_0 and G_1 are isomorphic, without revealing ϕ?

Solution

See board.

Example from Smart, *Cryptography Made Simple*

Why is This a ZK Proof of Graph Isomorphism

Why it's a proof:

1. Suppose the two graphs are not isomorphic.
2. Then no graph can be isomorphic to both G_0 and G_1
3. So no matter what graph H is sent to Victor, Victor will reject for either $b = 0$ or $b = 1$
4. At least a 50% chance that Victor detects a lying Peggy
5. Repeat the process multiple times to get this probability close to zero

Why it's ZK:

1. Victor learns either $\phi' \circ \phi$ or ϕ'
2. This does not give him any information about ϕ

Section 3

Mathematical Details

Algorithms

Definition

An algorithm:

- A Turing Machine with an input tape, a work tape, an output tape and possibly a random tape

Definition

An interactive algorithm:

- A Turing Machine with an added communication tape and a common input tape

Definitions from Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*

Protocols

- Prover and Verifier are interactive algorithms

Definition

A protocol:

- The descriptions according to which two or more interactive algorithms communicate

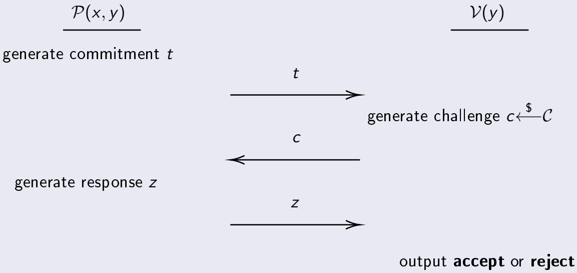
Definition from Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*

Sigma Protocols

Definition

A sigma protocol:

- y is public information
- Prover wants to prove some statement about y to Verifier
- x is a witness for y, known only by $\mathcal{P}$



$\mathcal{P}(x, y)$

$\mathcal{V}(y)$

generate commitment t

t

generate challenge $c \xleftarrow{\$} \mathcal{C}$

c

generate response z

z

output **accept** or **reject**

Definition from Boneh and Shoup, *A Graduate Course in Applied Cryptography*

Properties of ZK Proofs

- Completeness
- Soundness
- Zero Knowledge

Section 4

Example: Schnorr's Identification Protocol

Cryptography Based on Discrete Logarithms

The following assumption is used in public key cryptography and generally believe to be true:

Assumption

Given a group $\mathbb{G}$ of prime order q and $g, u \in G$ both different than the identity, it is computationally hard to find $\alpha \in \mathbb{Z}_{\shortparallel}$ such that:

$$g^{\alpha} = u.$$

We say that α is the discrete logarithm of u with respect to g.

Schnorr's Identification Protocol

Example

Let $\mathbb{G}$ be a group of prime order q and $g \in G$. Prover chooses $\alpha \in \mathbb{Z}_{||}$ and computes $u := g^{\alpha}$. Prover sends g and u to the Verifier.
How can P prove that they know the discrete logarithm of u with respect to g, without revealing it?

Solution

See board.

Example from Smart, *Cryptography Made Simple*

Remarks on Schnorr's Indentification Protocol

- Used for identification
- Verifier cannot convince anyone else that Prover knows the discrete logarithm
- Is complete, sound, and honest verifier zero knowledge

Section 5

A Software Implementation

Conclusion

- Zero Knowledge proofs allow a prover to convince a verifier of some statements
- ZK proofs are often interactive protocols
- ZK proofs are used in internet privacy

Boneh, D. and V. Shoup. *A Graduate Course in Applied Cryptography*. 2020. Chap. 19. URL: https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf.

Brands, S. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. The MIT Press. MIT Press, 2000. Chap. 2. ISBN: 9780262261661. URL: www.credentica.com/the_mit_pressbook.html.

Smart, Nigel P. *Cryptography Made Simple*. English. Information Security and Cryptography. Springer, 2016. Chap. 21. ISBN: 978-3-319-21935-6. DOI: 10.1007/978-3-319-21936-3.