

Proseminar Sicherheit in Computersystemen

Zero Knowledge Proofs

28.05.2019

Max Ostermann

Inhalt

- Einführung
- Grundlagen
- Protokolle
- Simulierbarkeit
- Nicht-interaktive Zero Knowledge Proofs
- Moderne Anwendung
- Angriffsvektoren

Einführung

- Historisch

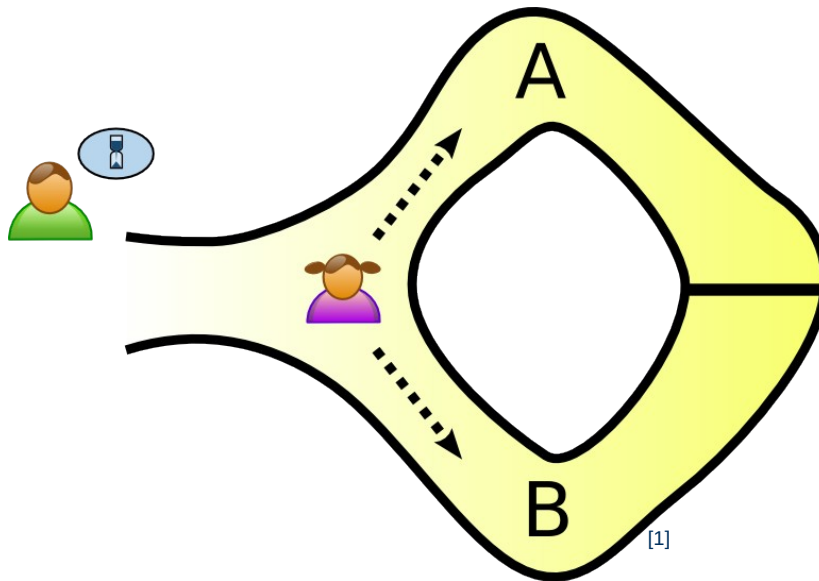
Niccolo Tartaglia fand 1535 eine Formel zum Lösen von Polynomen dritten Grades

Einführung

- Historisch

Niccolo Tartaglia fand 1535 eine Formel zum Lösen von Polynomen dritten Grades

- Alibabas Höhle



Grundlegende Definitionen

- Korrektheit/Soundness

Wahrscheinlichkeit eine Aussage ohne Kenntnis des Geheimnisses zu beweisen ist vernachlässigbar gering

Wahrscheinlichkeit: $1 / 2^n$

- Vollständigkeit/Completeness

Protokoll führt mit überwältigender Wahrscheinlichkeit zum Erfolg

Wahrscheinlichkeit: $1 - (1/2^n)$

Grundlegende Definitionen

- Korrektheit/Soundness

Wahrscheinlichkeit eine Aussage ohne Kenntnis des Geheimnisses zu beweisen ist vernachlässigbar gering

Wahrscheinlichkeit: $1 / 2^n$

- Vollständigkeit/Completeness

Protokoll führt mit überwältigender Wahrscheinlichkeit zum Erfolg

Wahrscheinlichkeit: $1 - (1/2^n)$

- Genereller Ablauf:

Schritt 1: $P \rightarrow V$ Commitment a

Schritt 2: $P \leftarrow V$ Challenge c

Schritt 3: $P \rightarrow V$ Reponse z

Protokollübersicht

- Graphisomorphismus
- Hamiltonsche Graphen
- Diskrete Logarithmen
- Quadratische Reste

Protokoll: Quadratische Reste

Schlüsselgenerierung

Sei $n = p \cdot q$ das Produkt zweier zufälliger, verschiedener Primzahlen.

Der Beweiser \mathcal{P} wählt $w \in_R \mathbb{Z}_n^*$ und berechnet $x = w^2 \bmod n$. Die Werte (n, x) werden als öffentlicher Schlüssel veröffentlicht, w bildet das Geheimnis von \mathcal{P} .

Protokoll

Beweiser

geg.: $(n, x)w$

wählt s zufällig in \mathbb{Z}_n^*

berechnet $a = s^2 \bmod n$

berechnet $z = s \cdot w^c \bmod n$

Verifizierer

geg.: (n, x)

wählt $c \in_R \{0, 1\}$

überprüft ob $z^2 \stackrel{?}{=} a \cdot x^c \bmod n$

\xrightarrow{a}

\xleftarrow{c}

\xrightarrow{z}

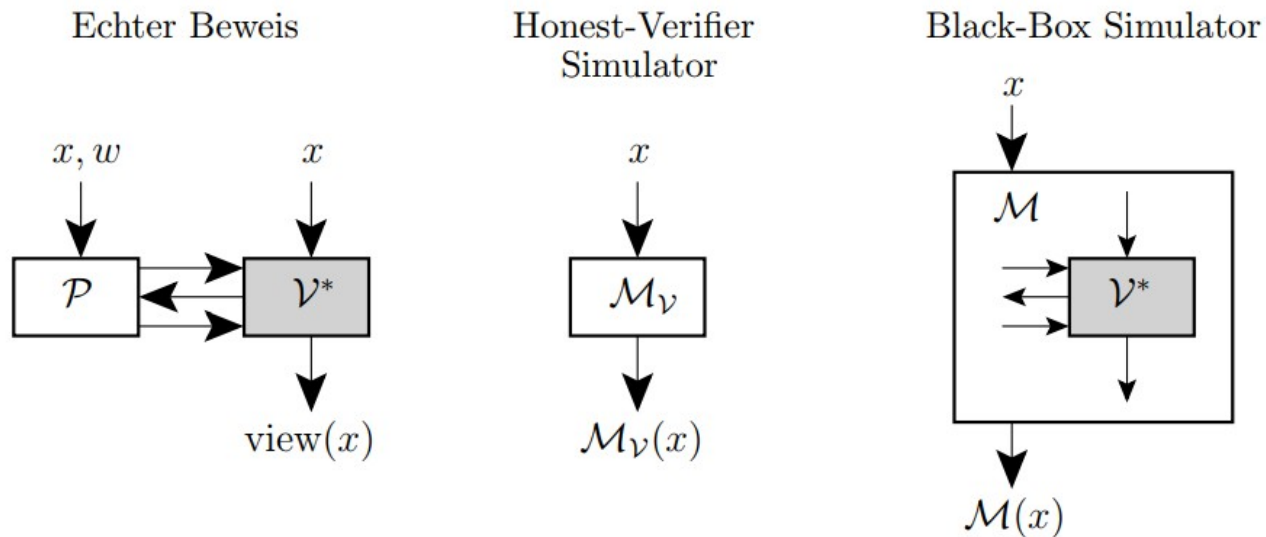
[2]

Simulierbarkeit

- Simulation der Wahrscheinlichkeitsverteilung ohne Kenntnis des Geheimnisses
- Ununterscheidbarkeit simulierter und echter Abläufe

Simulierbarkeit

- Simulation der Wahrscheinlichkeitsverteilung ohne Kenntnis des Geheimnisses
- Ununterscheidbarkeit simulierter und echter Abläufe



[3]

Nicht-interaktive Zero Knowledge Proofs

- Zero Knowledge Proof in „einer Postkarte“
- Fiat-Shamir Heuristik
 - Challenges über Hashfunktion
 - Rundenzahl von >64
- Beweis über das ‚Random Oracle Model‘
- Zero-Knowledge Eigenschaft nicht in der „realen“ Welt beweisbar

Moderne Anwendung

- Authentifizierung
- Blockchain
- Signaturen
- Nachweis privater Angelegenheiten

Angriffsvektoren

- Man in the middle



[4]

- Große, koordinierte Angreifernetzwerke

Danke für eure Aufmerksamkeit

Fragen?

Quellen

- Bildquellen:

[1]: https://en.wikipedia.org/wiki/Zero-knowledge_proof#/media/File:Zkip_alibaba1.png

[2]: https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_kp_datensicherheit/v11_doku.pdf?lang=de Abbildung 9

[3]: https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_kp_datensicherheit/v11_doku.pdf?lang=de Abbildung 6

[4]: https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_kp_datensicherheit/v11_doku.pdf?lang=de Abbildung 12

- Hauptquellen

- https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_kp_datensicherheit/v11_doku.pdf?lang=de

- “How to explain Zero-Knowledge Protocols to your children“ Quisquater et al. Advances in Cryptology – Crypto ‘89 p.628 - 631