TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Proseminar Sicherheit in Computersystemen

Zero Knowledge Proofs

28.05.2019

Max Ostermann

Inhalt

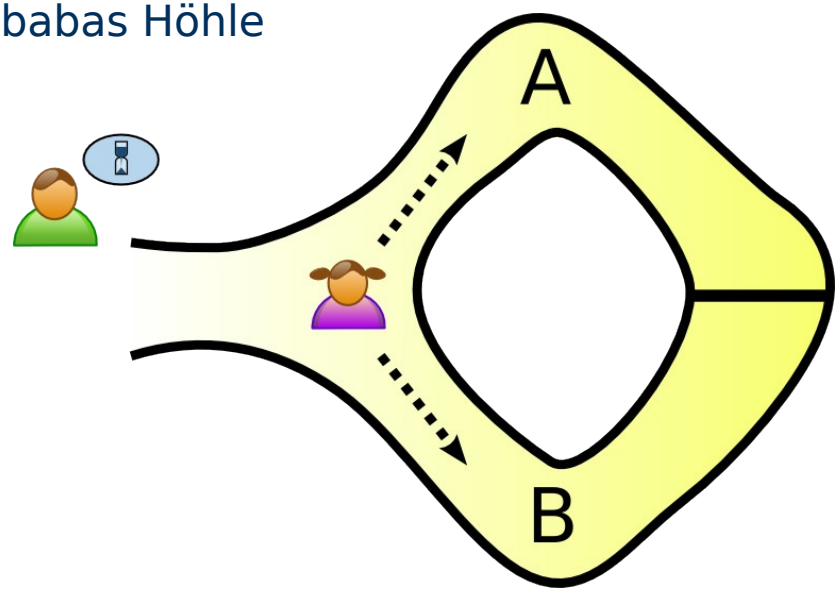
- Einführung
- Grundlagen
- Protokolle
- Simulierbarkeit
- Nicht-interaktive Zero Knowledge Proofs
- Moderne Anwendung
- Angriffsvektoren

Einführung

- Historisch

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

- Alibabas Höhle



Grundlegende Definitionen

- Korrektheit/Soudness

  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 → V Commitment a

  Schritt 2: P ← V Challenge c

  Schritt 3: P → 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.

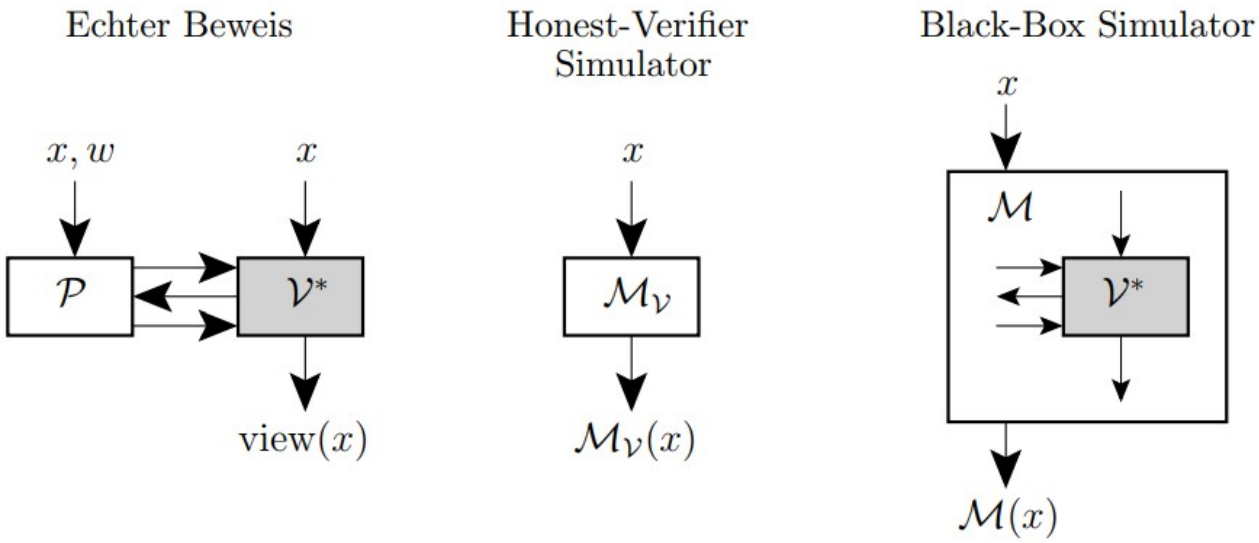
Der Beweiser $\mathcal{P}$ wählt $w \in_R \mathbb{Z}_n^*$ und berechnet $x = w^2 \bmod n$. Die Werte (n, x) werden als öffentlicher Schlüssel veröffentlicht, w bildet das Geheimnis von $\mathcal{P}$.

Protokoll

Beweiser		**Verifizierer**
geg.: $(n, x)w$		geg.: (n, x)
wählt s zufällig in $\mathbb{Z}_n^*$ berechnet $a = s^2 \bmod n$	$\xrightarrow{a}$	
		wählt $c \in_R \{0, 1\}$
	$\xleftarrow{c}$	
berechnet $z = s \cdot w^c \bmod n$	$\xrightarrow{z}$	
		überprüft ob $z^2 \stackrel{?}{=} a \cdot x^c \bmod n$

Simulierbarkeit

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



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

- Große, koordinierte Angreifernetzwerke