TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Proseminar Sicherheit in Computersystemen

Zero-Knowledge Proofs

28.05.2019

Max Ostermann

Inhalt

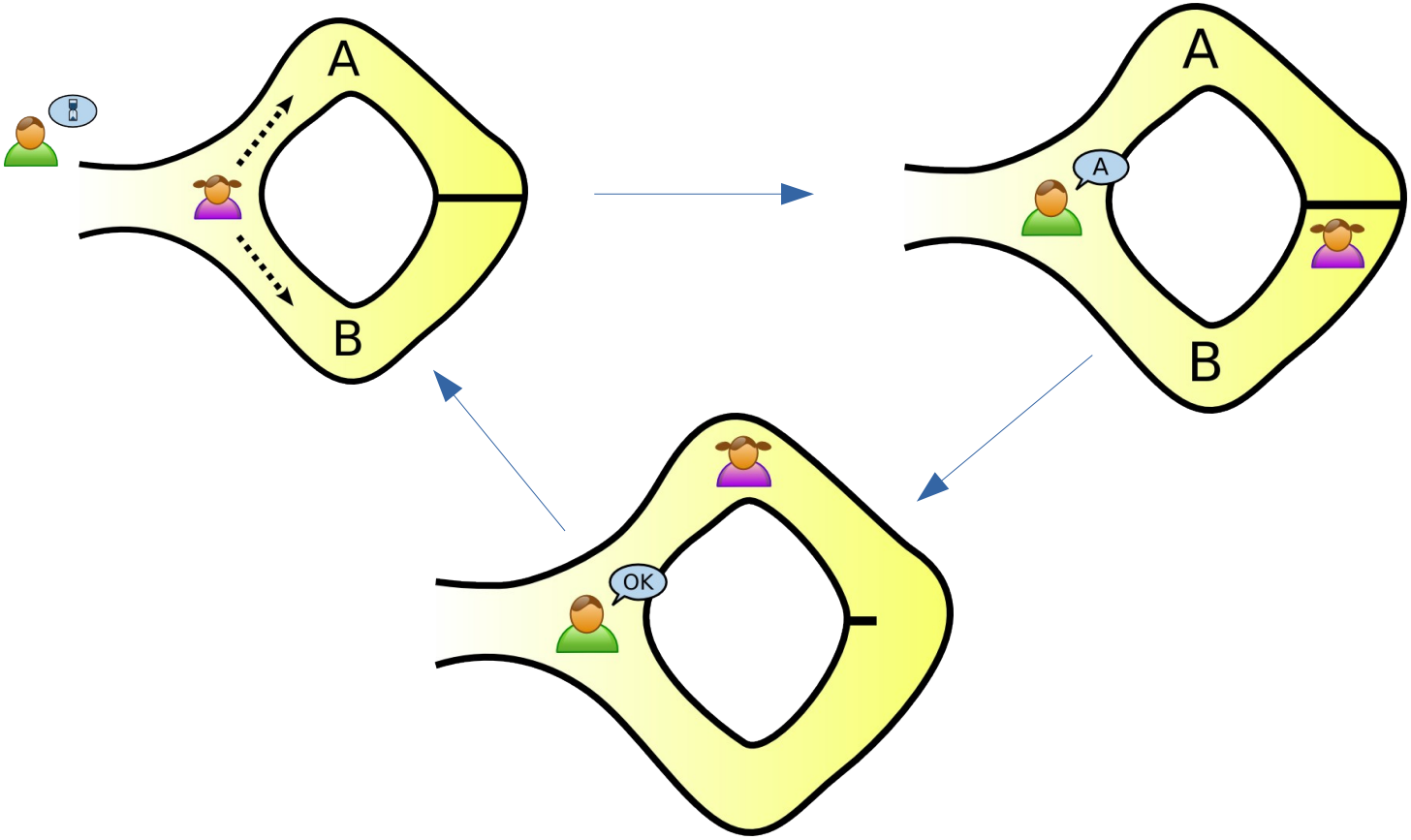
- Einführung
- Grundlagen
- Simulierbarkeit
- Protokolle
- Nicht-interaktive Zero-Knowledge Proofs
- Moderne Anwendung
- Angriffsvektoren
- Fazit

Einführung

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

[1]

Alibabas Höhle



[2]

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 → V Commitment a

  Schritt 2: P ← V Challenge c

  Schritt 3: P → V Reponse z

Grundlegende Definitionen

- Zero-Knowledge Eigenschaft

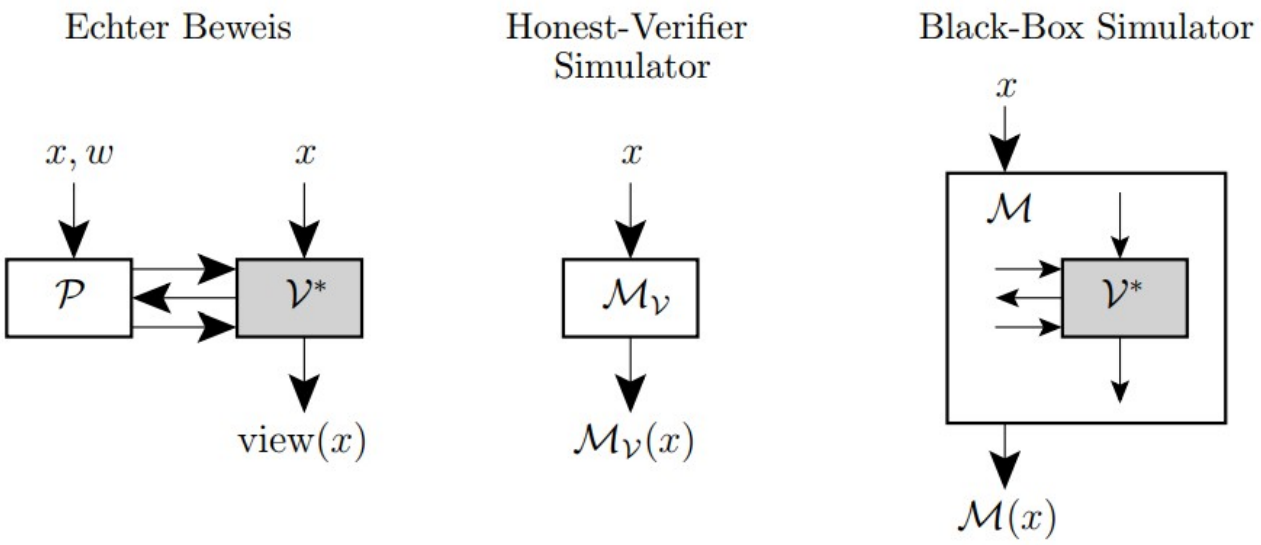
  - Verifizierer erlangt kein Wissen vom Geheimnis

  → Verlauf eines Beweises für Dritte ununterscheidbar von falschem Beweis

  ➡ Bobs Aufnahme == Malice‘ Aufnahme?

Simulierbarkeit

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



[3]

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

[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

- Signaturen
- Blockchain
- Authentifizierung
- Nachweis privater Angelegenheiten

Angriffsvektoren

- Große, koordinierte Angreifernetzwerke
- Man in the middle

[4]

Fazit

Pro:

- Zero-Knowledge Eigenschaft
- Vielfältig anwendbar
- Hervorragendes Subprotokoll
- Einfache, schnelle Berechnungen

Con:

- P != NP
- Angriffsvektoren
- Teils hohe Anzahl an Interaktionen

Danke für eure Aufmerksamkeit

Fragen?

Quellen

- Bildquellen:

  [1]: https://de.wikipedia.org/wiki/Niccol%C3%B2_Tartaglia#/media/File:Niccol%C3%B2_Tartaglia.jpg

  [2]:https://en.wikipedia.org/wiki/Zero-knowledge_proof

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

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

  [5]: 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