

# Elektronische Kartenspiele

Effiziente Realisierung elektronischer Kartenspiele  
in Netzwerken ohne vertrauenswürdige Zentrale

Heiko Stamer

Universität Kassel  
Fachbereich Mathematik/ Informatik  
Heinrich-Plett-Straße 40, D-34132 Kassel

stamer@theory.informatik.uni-kassel.de

76F7 3011 329D 27DB 8D7C 3F97 4F58 4EB8 FB2B E14F

MetaRheinMain ChaosDays 11b

- 1 Motivation: Sichere elektronische Kartenspiele
- 2 Historischer Überblick: „Mental Poker“ Problem
- 3 LibTMCG: Entwicklung einer freien C++ Bibliothek
- 4 SecureSkat: Eine Referenzimplementierung
- 5 Weitere Anwendungen und Ausblick

## Aufgabe: Bereitstellung einer Plattform für „sichere“ elektronische Kartenspiele in einem Kommunikationsnetzwerk

Häufige Lösung: Vertrauenswürdige Zentrale (Trusted Third Party)

### Nachteile:

- Nicht immer verfügbar (on demand)
- Wer hat Kontrolle? (Internet-Casinos)
- Zentraler Angriffspunkt (DoS)

Oft bessere Lösung: Verteile das „Vertrauen“ auf die Teilnehmer

Motto (Hackerethik): Misstraue Autorität – fördere  
Dezentralisierung!

### Bekannte Beispiele:

- Web of Trust (OpenPGP)
- (Verifizierbare) Geheimnisteilung
- Peer-to-Peer Netzwerke
- ...

**Aufgabe:** Bereitstellung einer Plattform für „sichere“ elektronische Kartenspiele in einem Kommunikationsnetzwerk

**Häufige Lösung:** Vertrauenswürdige Zentrale (Trusted Third Party)

**Nachteile:**

- Nicht immer verfügbar (on demand)
- Wer hat Kontrolle? (Internet-Casinos)
- Zentraler Angriffspunkt (DoS)

**Oft bessere Lösung:** Verteile das „Vertrauen“ auf die Teilnehmer

**Motto (Hackerethik):** Misstraue Autorität – fördere Dezentralisierung!

**Bekannte Beispiele:**

- Web of Trust (OpenPGP)
- (Verifizierbare) Geheimnisteilung
- Peer-to-Peer Netzwerke
- ...

**Aufgabe:** Bereitstellung einer Plattform für „sichere“ elektronische Kartenspiele in einem Kommunikationsnetzwerk

**Häufige Lösung:** Vertrauenswürdige Zentrale (Trusted Third Party)

**Nachteile:**

- Nicht immer verfügbar (on demand)
- Wer hat Kontrolle? (Internet-Casinos)
- Zentraler Angriffspunkt (DoS)

**Oft bessere Lösung:** Verteile das „Vertrauen“ auf die Teilnehmer

**Motto (Hackerethik):** Misstraue Autorität – fördere Dezentralisierung!

**Bekannte Beispiele:**

- Web of Trust (OpenPGP)
- (Verifizierbare) Geheimnisteilung
- Peer-to-Peer Netzwerke
- ...

- Kodierung der virtuellen Spielkarten
  - Verschlüsselung/ Maskierung
- Korrektheit der Spieloperationen (Mischen, Geben, etc.)
  - Zero-Knowledge Beweise/ Protokolle
- Absicherung der Kommunikationsverbindungen
  - Vertraulichkeit, Authentizität, Reliable Broadcast, etc.
- Angriffsmodell
  - passiver/ aktiver Angreifer, statische/ adaptive Wahl der korrupten Teilnehmer, etc.

siehe [SPWK\\_ZNP.pdf](#) (Folien 1 bis 40)

siehe [SPWK\\_ZNP.pdf](#) (Folie 53)

- Kodierung der virtuellen Spielkarten
  - Verschlüsselung/ Maskierung
- Korrektheit der Spieloperationen (Mischen, Geben, etc.)
  - Zero-Knowledge Beweise/ Protokolle
- Absicherung der Kommunikationsverbindungen
  - Vertraulichkeit, Authentizität, Reliable Broadcast, etc.
- Angriffsmodell
  - passiver/ aktiver Angreifer, statische/ adaptive Wahl der korrupten Teilnehmer, etc.

siehe [SPWK\\_ZNP.pdf](#) (Folien 1 bis 40)

siehe [SPWK\\_ZNP.pdf](#) (Folie 53)

- Kodierung der virtuellen Spielkarten
  - Verschlüsselung/ Maskierung
- Korrektheit der Spieloperationen (Mischen, Geben, etc.)
  - Zero-Knowledge Beweise/ Protokolle
- Absicherung der Kommunikationsverbindungen
  - Vertraulichkeit, Authentizität, Reliable Broadcast, etc.
- Angriffsmodell
  - passiver/ aktiver Angreifer, statische/ adaptive Wahl der korrupten Teilnehmer, etc.

siehe [SPWK\\_ZNP.pdf](#) (Folien 1 bis 40)

siehe [SPWK\\_ZNP.pdf](#) (Folie 53)

- Kodierung der virtuellen Spielkarten
  - Verschlüsselung/ Maskierung
- Korrektheit der Spieloperationen (Mischen, Geben, etc.)
  - Zero-Knowledge Beweise/ Protokolle
- Absicherung der Kommunikationsverbindungen
  - Vertraulichkeit, Authentizität, Reliable Broadcast, etc.
- Angriffsmodell
  - passiver/ aktiver Angreifer, statische/ adaptive Wahl der korrupten Teilnehmer, etc.

siehe [SPWK\\_ZNP.pdf](#) (Folien 1 bis 40)

siehe [SPWK\\_ZNP.pdf](#) (Folie 53)

„Mental Poker“ Problem: Kann man ein faires Kartenspiel (Poker) ohne physisches Spielmaterial (Karten) durchführen, wobei keine vertrauenswürdige dritte Partei (Schiedsrichter) zur Verfügung steht?

Das Problem wird im Bereich der Kryptographie seit 1979 betrachtet und hatte einen großen Einfluß auf die entwickelten Techniken.

siehe [KryptoTag\\_Ulm.pdf](#) (Folien 3 bis 10)

siehe [WEWoRC2005.pdf](#) (Folien 9 bis 11)

- Ehemaliger Name: OpenSkat, Jetzt: SecureSkat
- <http://savannah.nongnu.org/projects/securekat>

siehe [WEWoRC2005.pdf](#) (Folie 12)

siehe [Folien-Skat.pdf](#) (Folien 18 bis 20)

siehe [README \(Requirements\)](#)

siehe WEWoRC2005.pdf (Folie 13)

Vielen Dank für Ihre Aufmerksamkeit! Fragen?

siehe [WEWoRC2005.pdf](#) (Folie 13)

Vielen Dank für Ihre Aufmerksamkeit! Fragen?

- [Sch98] Christian Schindelhauer.  
A Toolbox for Mental Card Games.  
Technical Report A-98-14, University of Lübeck, 1998.  
<http://citeseer.ist.psu.edu/schindelhauer98toolbox.html>
- [BSm03] Adam Barnett, Nigel P. Smart.  
Mental Poker Revisited.  
9th IMA International Conference, LNCS 2898, pp. 370–383, 2003.
- [St04] Heiko Stamer.  
Kryptographische Skatrunde.  
Offene Systeme 4 (2004), pp. 10–30, 2004.
- [1] LibTMCG: <http://savannah.nongnu.org/projects/libtmcg>
- [2] SecureSkat: <http://savannah.nongnu.org/projects/secureskat>