Secure Trick-Taking Game Protocols
How to Play Online Spades with Cheaters

Xavier Bultel and **Pascal Lafourcade**

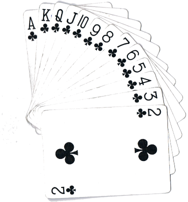
UNIVERSITÉ Clermont Auvergne

LIMOS

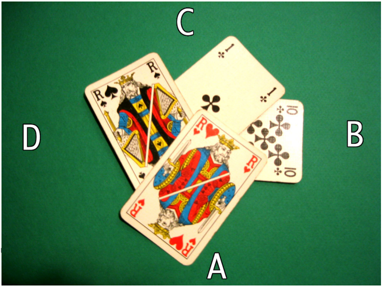
Financial Cryptography 2019
St. Kitts

Rules of SPADES

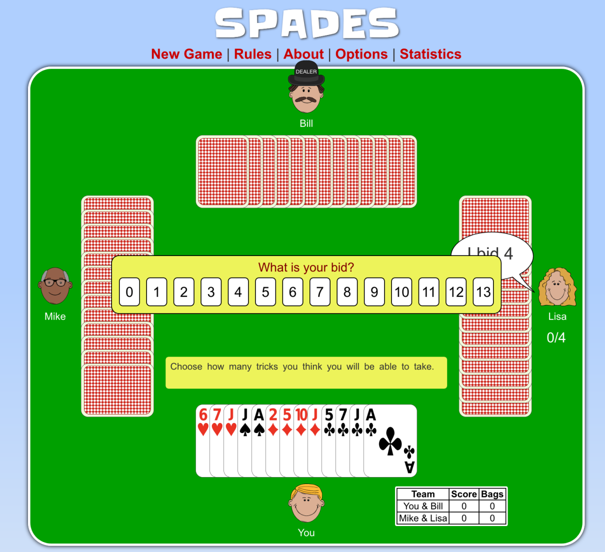
- The 52 cards are shuffled and then dealt 13 by players



- Trump is ♠
- If unable to follow suit, the player may play any card



SPADES https://cardgames.io/spades



What is your bid?

0 1 2 3 4 5 6 7 8 9 10 11 12 13

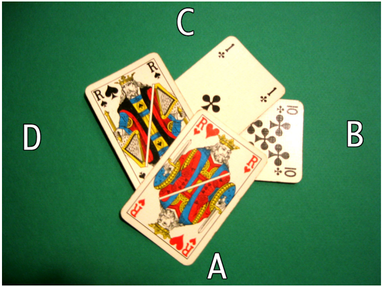
Choose how many tricks you think you will be able to take.

Team	Score	Bags
You & Bill	0	0
Mike & Lisa	0	0

Trick Taking Games

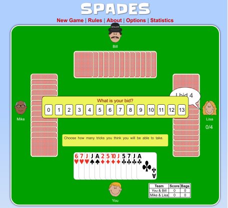
Principles

- Every player plays one card at each trun
- There is one winner of the trick



Belotte, Bridge, Whist, Napoleon, etc ...

Online Implicit Assumption



Choose how many tricks you think you will be able to take.

Team	Score	Bags
You & Bill	0	0
Mike & Lisa	0	0

Trust Sever

Related Work

- *Mental poker* Protocols, without relying on a trusted third party.
- Royale (tomorrow): UC framework for securely playing general card games with financial rewards/penalties enforcement

Our Contributions

The server is not trust

Security Models for Trick Taking Games

- Unpredictability
- Players are convinced that nobody cheats : Theft-resistance and Cheating-resistance.
- Hand-privacy
- Game-privacy

Proof of concept: Secure Spades

Introduction

Security Models for TTG

Secure Spades

Conclusion

Outline

Introduction

Security Models for TTG

Secure Spades

Conclusion

Unpredictability

Cards are dealt at random

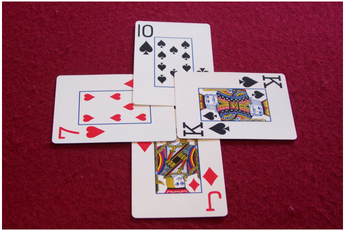
No Cheat: Theft-resistance

A player cannot play

- a card that is not in his hand
- cards from the hand of his partner

No Cheat: Cheating-resistance

A player cannot play a card that does not follow the rules



Hand-privacy

Players do not know the hidden cards of the other players

Game-privacy

At each round, the protocol does not leak any information except for the played cards

Outline

Introduction

Security Models for TTG

Secure Spades

Conclusion

Game Phases

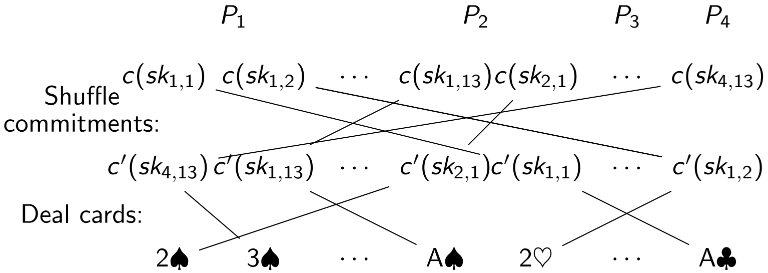
- **Initialisation phase:** One player publishes the public setup
- **Keys generation phase:**
  - each player generates 13 pairs $(pk_i = g^{sk_{i,j}}, sk_{i,j})$ and $c(sk_{i,j}) = pk_{i,j}$
  - all players generate the game key $PK = \{pk_{i,j}\}i, j \in [1, 52]$ together
- **Shuffle phase:** Players together
  - choose a deck,
  - compute their own hand
- **Game phase:**
  - play in turn
  - each time proving the validity of the cards

Deal the Cards

1. Each player generates commitments on his 13 secret keys,
2. Each player shuffles and randomizes the commitments in turn

3. Jointly randomly associate commitments to cards of the deck

Example



P_1 P_2 P_3 P_4

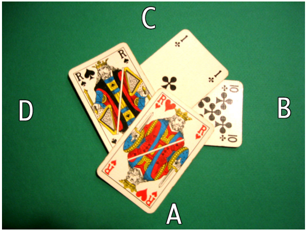
Shuffle commitments: $c(sk_{1,1})$ $c(sk_{1,2})$ $\cdots$ $c(sk_{1,13})$ $c(sk_{2,1})$ $\cdots$ $c(sk_{4,13})$

$c'(sk_{4,13})$ $c'(sk_{1,13})$ $\cdots$ $c'(sk_{2,1})$ $c'(sk_{1,1})$ $\cdots$ $c'(sk_{1,2})$

Deal cards: 2♠ 3♠ $\cdots$ A♠ 2♡ $\cdots$ A♣

where $c(sk)$ is the commitment of sk and $c'(sk)$ its randomization.

Play a Card using ZKP



1. Proves that the played card (A♣ $c'(sk_{1,1})$) corresponds to his secret keys ($sk_{1,1}$).
2. If do not follow the suit, then prove that none of his cards are of different color:
   - Poves that each commitment that matches a card of a non-leading suit commits one of his (not yet used) keys.

LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Security

Theorem

Secure Spades is theft-resistant, cheating-resistant, hand-private, unpredictable, and game-private under the DDH assumption.

Security

Theorem

Secure Spades is theft-resistant, cheating-resistant, hand-private, unpredictable, and game-private under the DDH assumption.

- Theft-resistant: Ownership by ZKP of EqLog
- Cheating-resistant: EqLogs for all his cards respect the rules
- Unpredictable: Shuffle committments and deal cards phases
- Hand-private: Shuffle and ZKP
- Game-private: ZKP

Outline

Introduction

Security Models for TTG

Secure Spades

Conclusion

Contributions

- Secure online trick-taking games
- No need to trust the server

Security Properties:

- Players are convinced that nobody cheats :
  - Theft-resistance
  - Cheating-resistance
- Unpredictability
- Hand-privacy
- Game-privacy

Allow new fancy games, that cannot be done physically

Future Works

- Prototype, it seems to be acceptable
- More games
- Bidding phase
- Score Counting

Thanks for your attention

pascal.lafourcade@uca.fr