Secure Mobile Gambling

RSA Conference ‘ 2001

San Francisco, California, April 2001

Markus Jakobsson
Bell Laboratories
Lucent Technologies

David Pointcheval
Dept d’Informatique
ENS-CNRS

Adam Young
Lockheed Martin

David.Pointcheval@ens.fr
http://www.di.ens.fr/users/pointche

Overview

- Introduction
- Constraints
  - device
  - communication
  - adversary
- Our solution
- Conclusion

Introduction

Want ! Gambling & gaming using handheld computers and cellular phones

Problems!

- trust between users and casino
- accidental/malicious disconnections
- computational limitations

Requirements:

- use only computationally inexpensive operations
- always allow recovery of state and conflict resolution

Structure

1. Do a setup of many games
2. Play an individual game
3. The revealed parameters of the game automatically “turn into” an electronic payment to the winner
4. Allow restart at same point if disconnected

Definitions

Metagame

game + disconnection strategies

Robustness

the disconnection strategy cannot increase the payoff for a cheater

Constraints

Typical devices:

- limited memory
- limited computational power

Possible attackers:

- lots of storage & computational power

Basic Assumptions

Casino:

May want to cheat

but won’t systematically deny a player access

Bank:

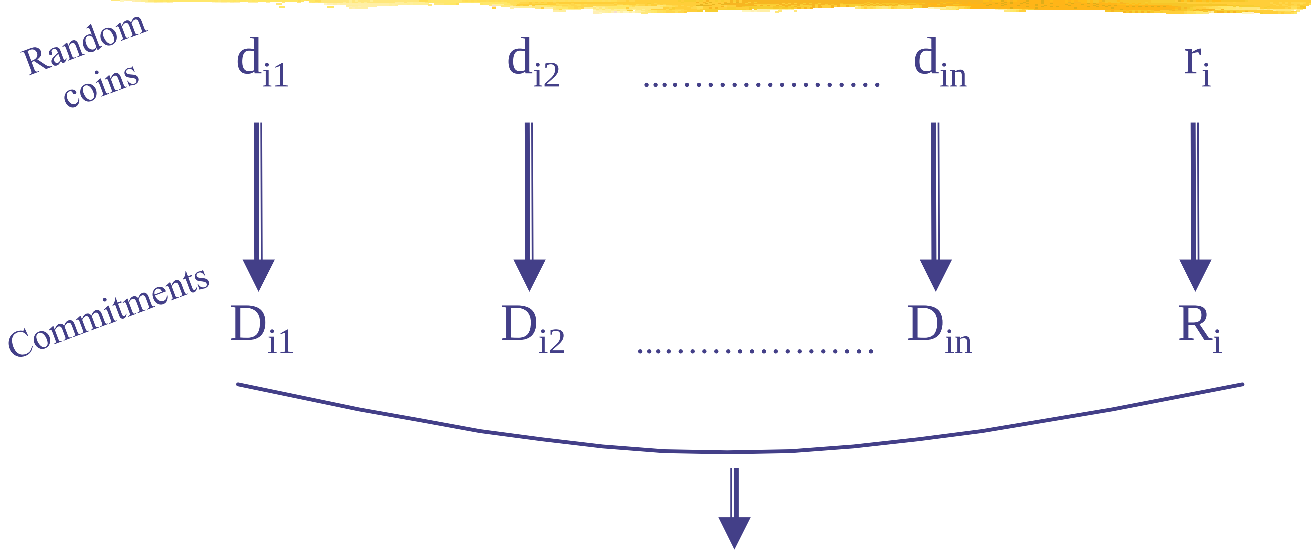
Will not collude with players or casino

Will not steal money

Game:

Focus on open card games

Game Node



Random coins d_{i1} d_{i2} ………………… d_{in} r_i

Commitments D_{i1} D_{i2} ………………… D_{in} R_i

Game$_i$ $= (D_{i1}, D_{i2}, \ldots, D_{in}, R_i)$

Game:

Defined by $game_{i,casino}$ and $game_{i,player}$ + strategy

Play One Game

0. Player & Casino have already exchanged
   $\text{game}_{i,\text{player}}$ and $\text{game}_{i,\text{casino}}$
1. Player sends $r_{i,\text{player}}$, casino checks it
2. Strategies:

   Casino reveals decision preimages, player checks

   Player reveals decision preimages, casino checks

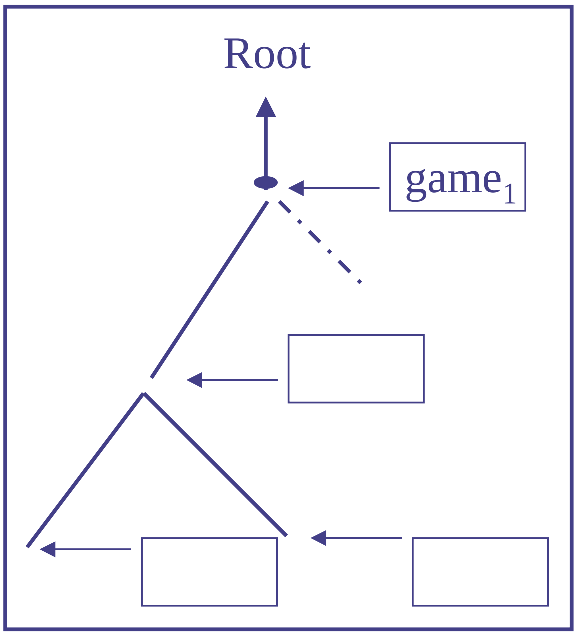
   (repeated one or more times)
3. Casino sends $r_{i,\text{casino}}$, player checks.
4. Evaluate game function on all known preimages
   and obtain result (= an electronic coin)

Example: Roulette

1. Player makes a bet by selecting
   a position and amount
2. Bet translated into choice of (decision) preimages
   $\Rightarrow$ Player reveals preimages
3. Casino reveals a fix preimage (no strategy)
4. Determine outcome as a deterministic,
   but one-way function, of all known preimages

Intuition: why no cheating?

Game Trees



- All randomness can be generated from one seed
- in setup, player and casino sign the pair

  $(\text{root}_{\text{casino}}, \text{root}_{\text{player}})$
- preimages + above signature become “payment orders”.

Disconnection

- Because of the signed trees,
  after a disconnection, they start again
  at the same point (where the game stopped)
- With a new strategy?
  If the casino/player uses a different strategy,
  the player/casino can choose the worst strategy
  of his adversary by selecting among
  all the revealed preimages

$\Rightarrow$ bad idea to change anything

Conflict Resolution

- If two equal “deposits” of same game,
  bank pays first one only
- If several inconsistent deposits of same game,
  bank locates inconsistencies,
  and lets other party win
- Other cases … see in the paper

Conclusion

- Low computation & storage
- can recover state
- disconnection strategies useless
- conflict resolution
- secure gambling for handheld devices