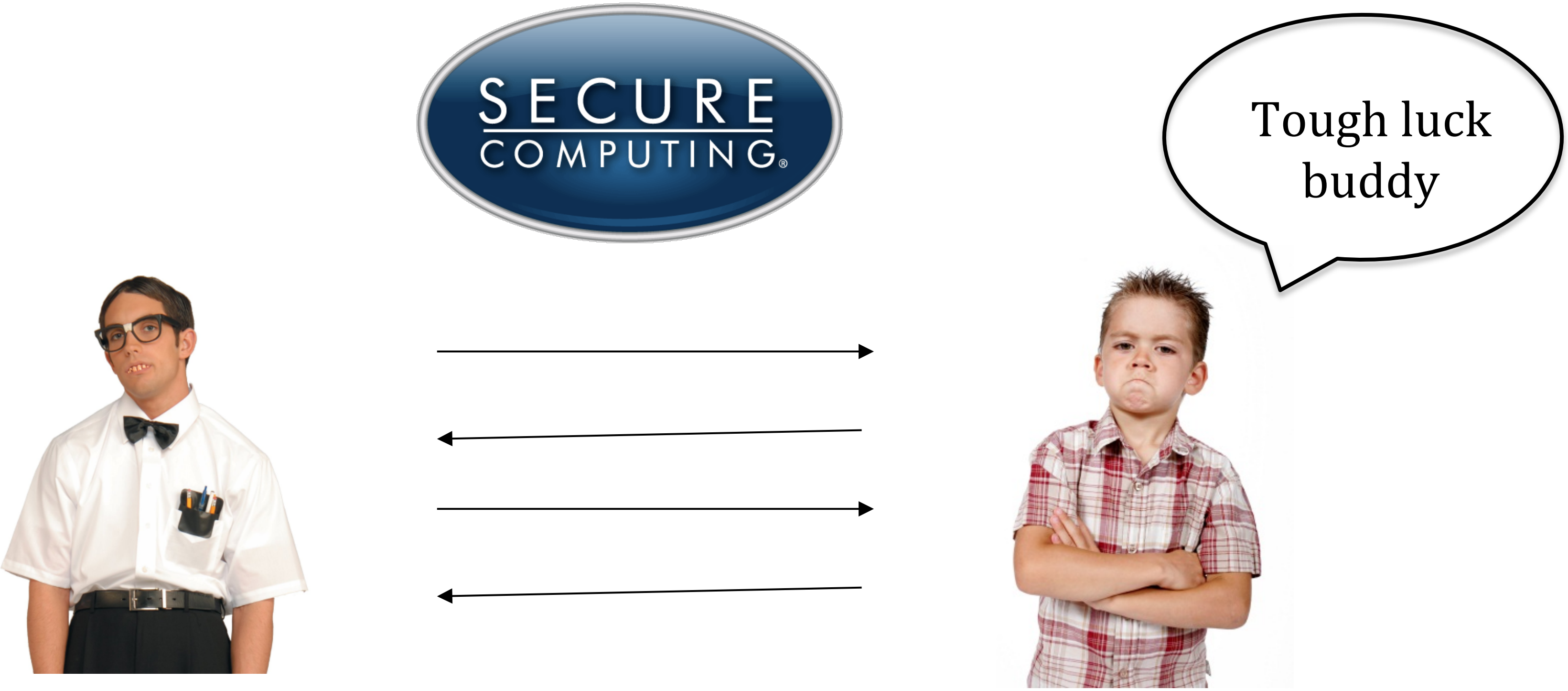
How to Use Bitcoin to Design Fair Protocols

Iddo Bentov (Technion)

Ranjit Kumaresan (Technion)

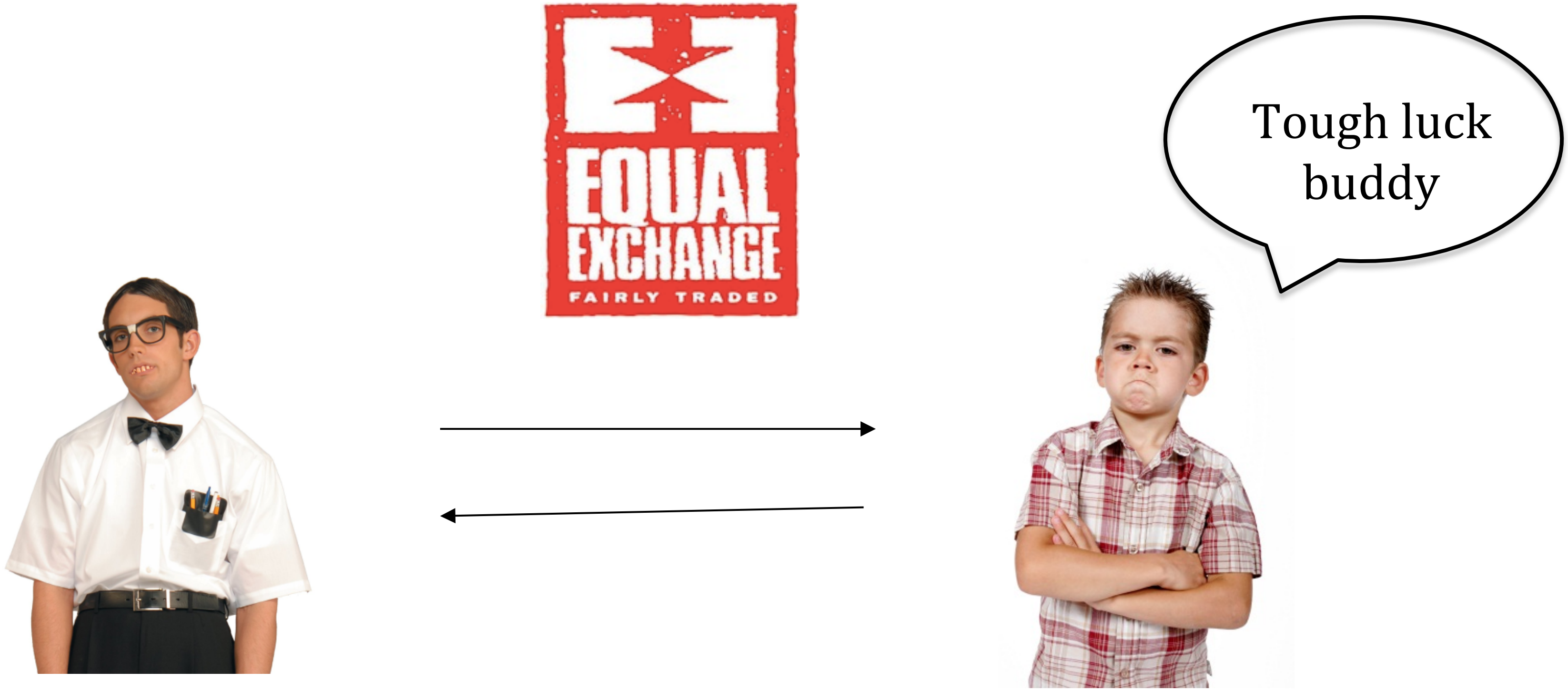
ePrint 2014/129

Fairness in Secure Computation



Fair coin tossing is impossible
[Cle86]

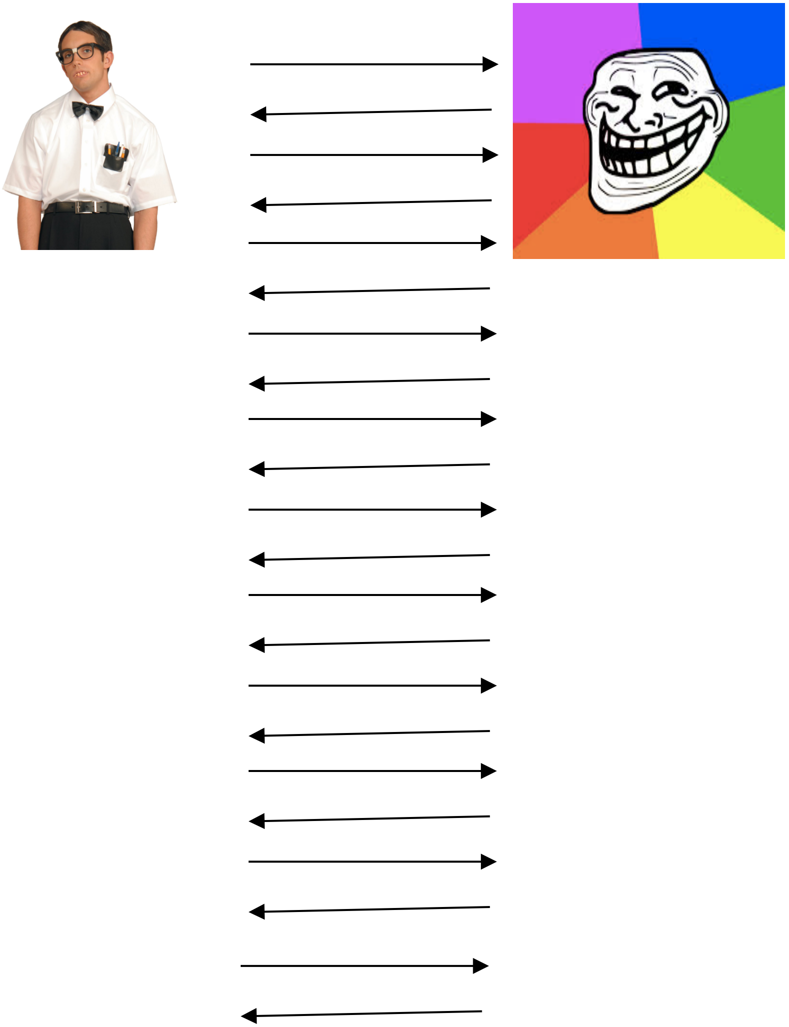
Fair Exchange

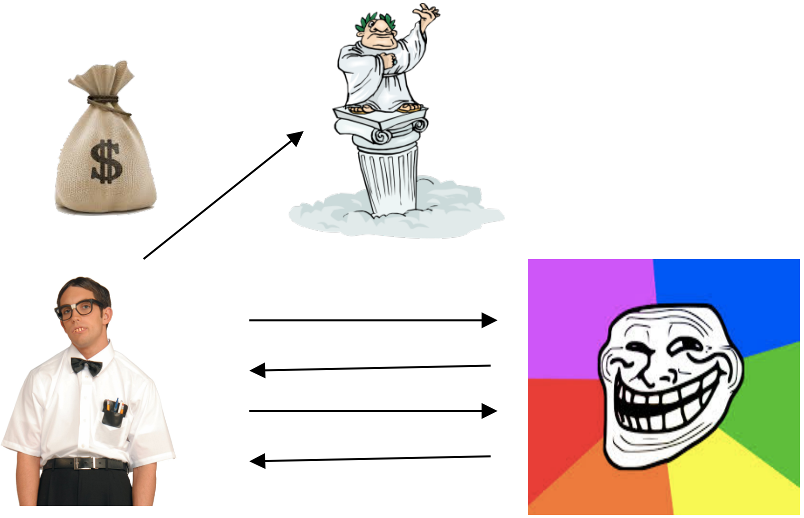


Fair exchange is impossible [Cle86,BN00]

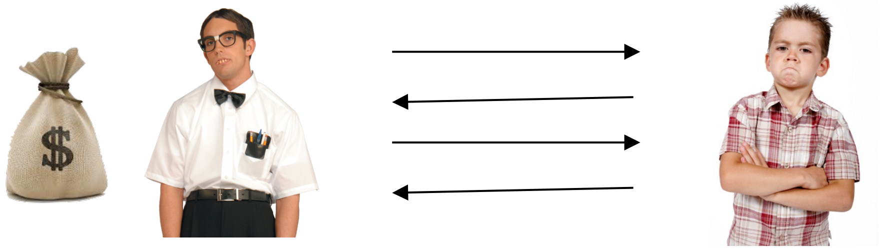
Workarounds

- Let’s release output gradually…
- Let’s do partial fairness?
- Let’s be optimistic!

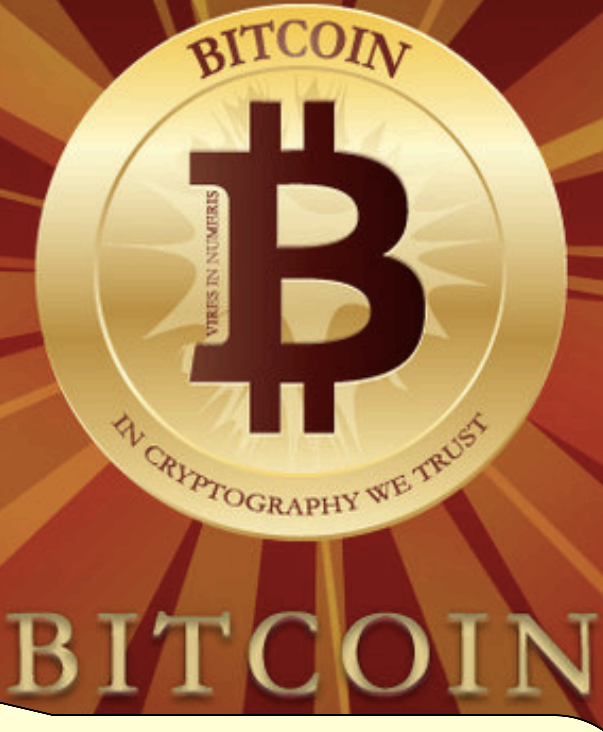




Let’s compensate the poor guy with some money!



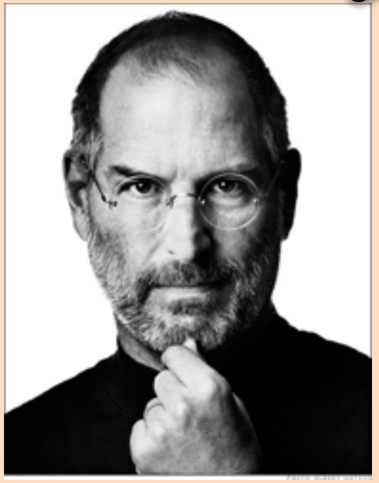
If only there was a better middle ground...



Defn.1: A cryptosystem is secure if my bank uses it and I’m not losing money

SECURE COMPUTING
EQUAL EXCHANGE
FAIRLY TRADED
AEQUITAS
VERITAS
LIBERTAS
2009
IN CRYPTOGRAPHY WE TRUST

Get it??

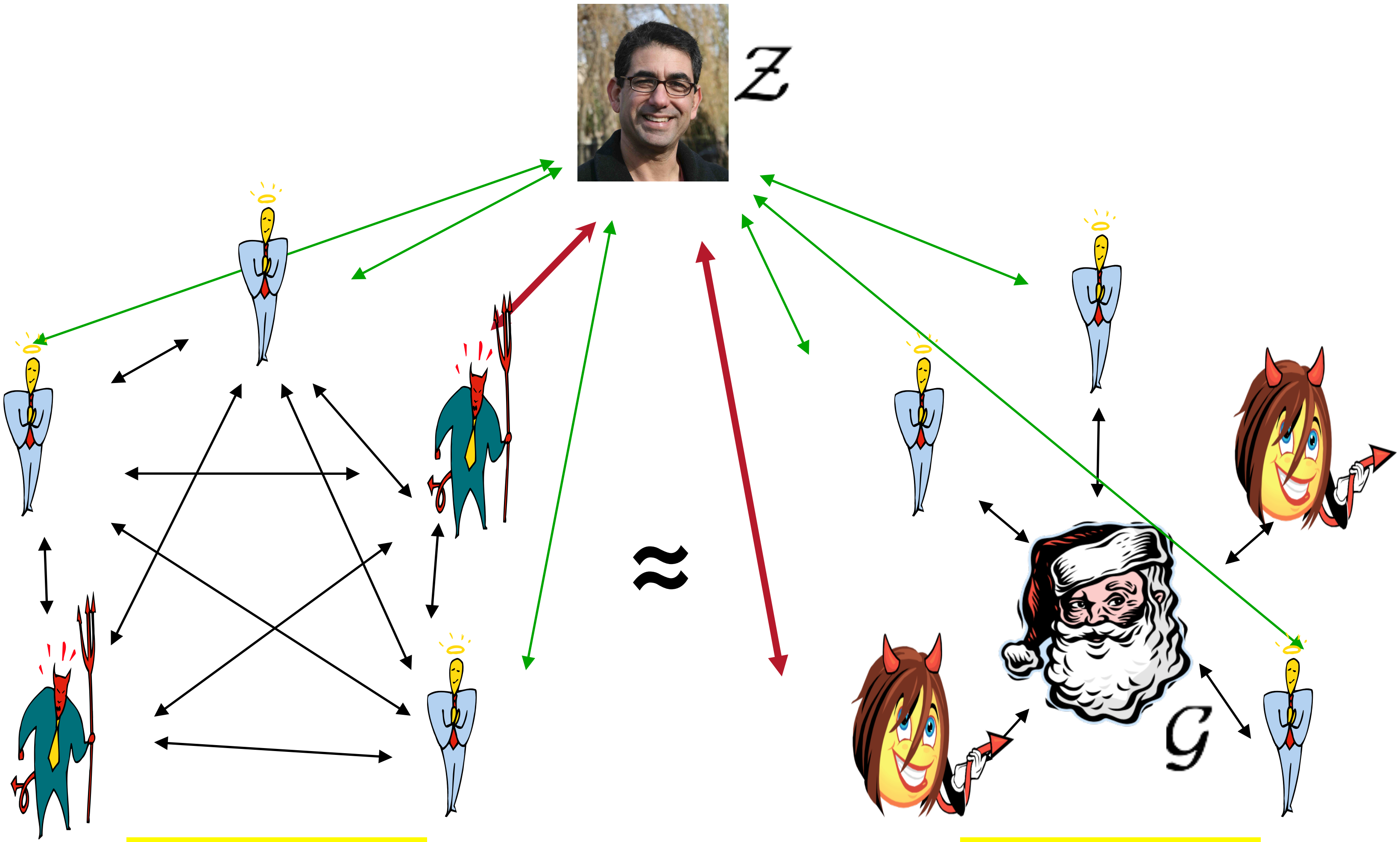


Missing Pieces

Security definition??

Abstraction of what you want from Bitcoin??

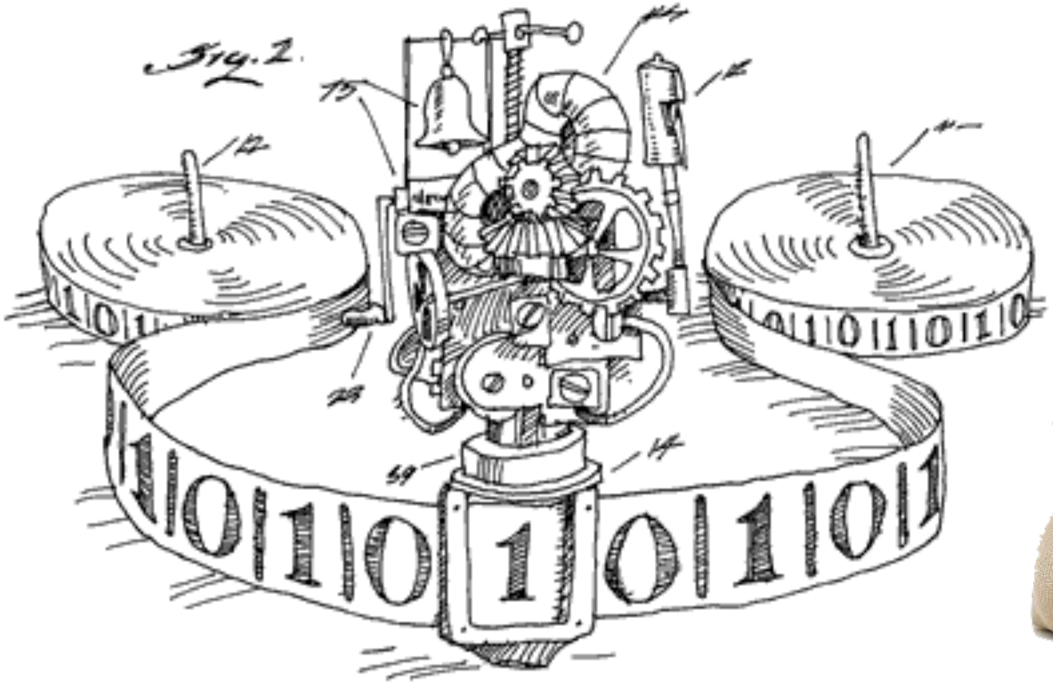
Standard Security Definitions

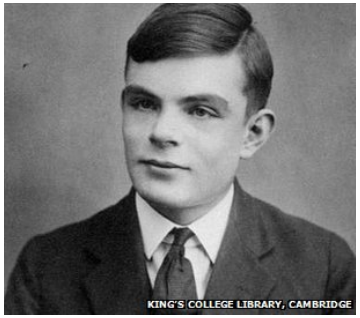


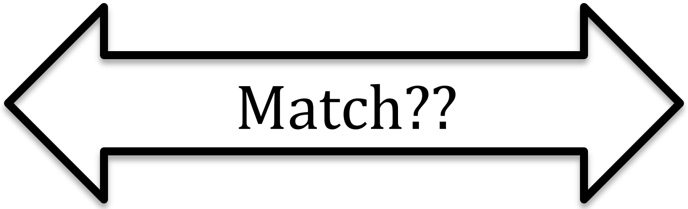
REAL

IDEAL

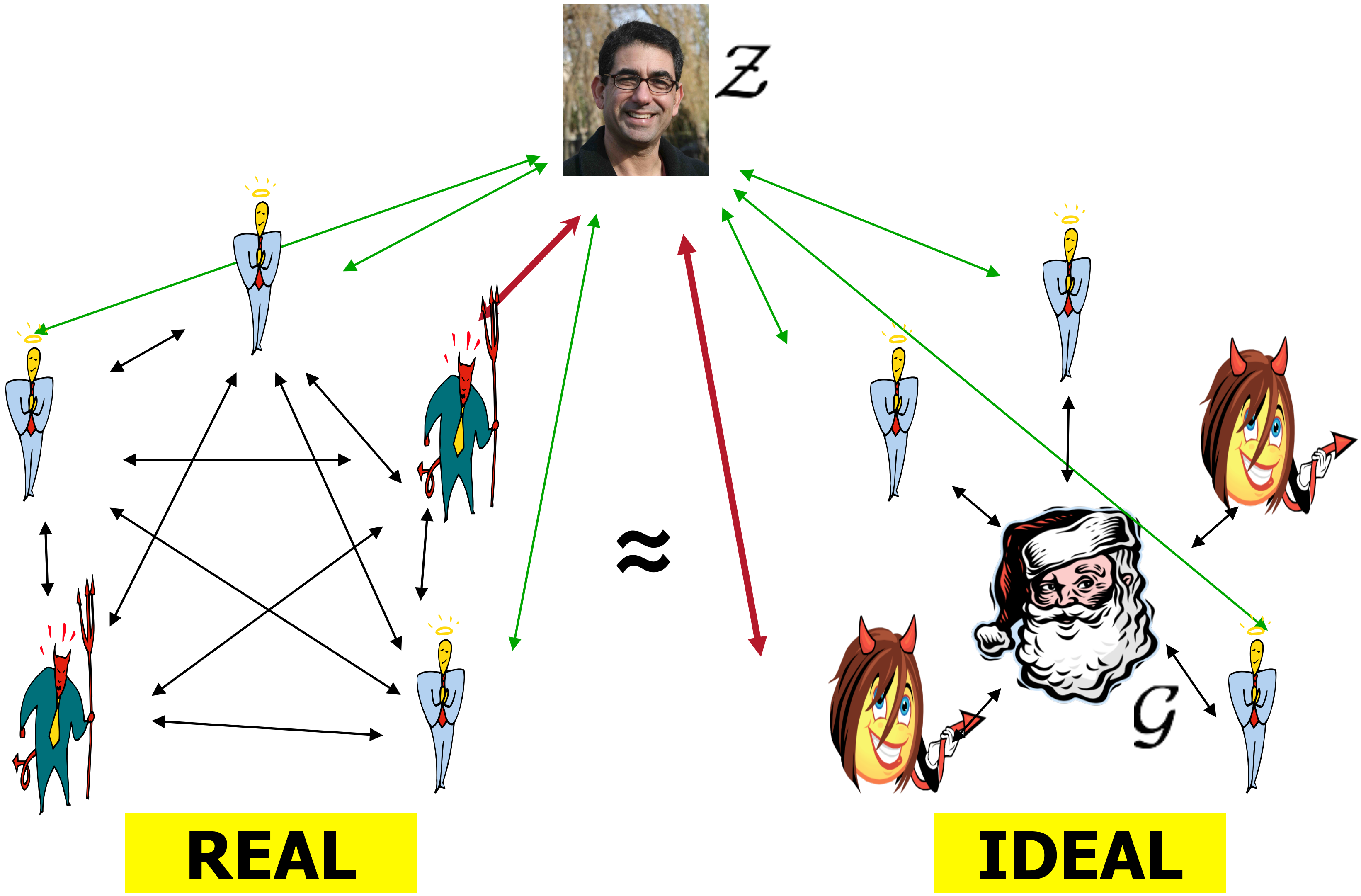
Where is the money???



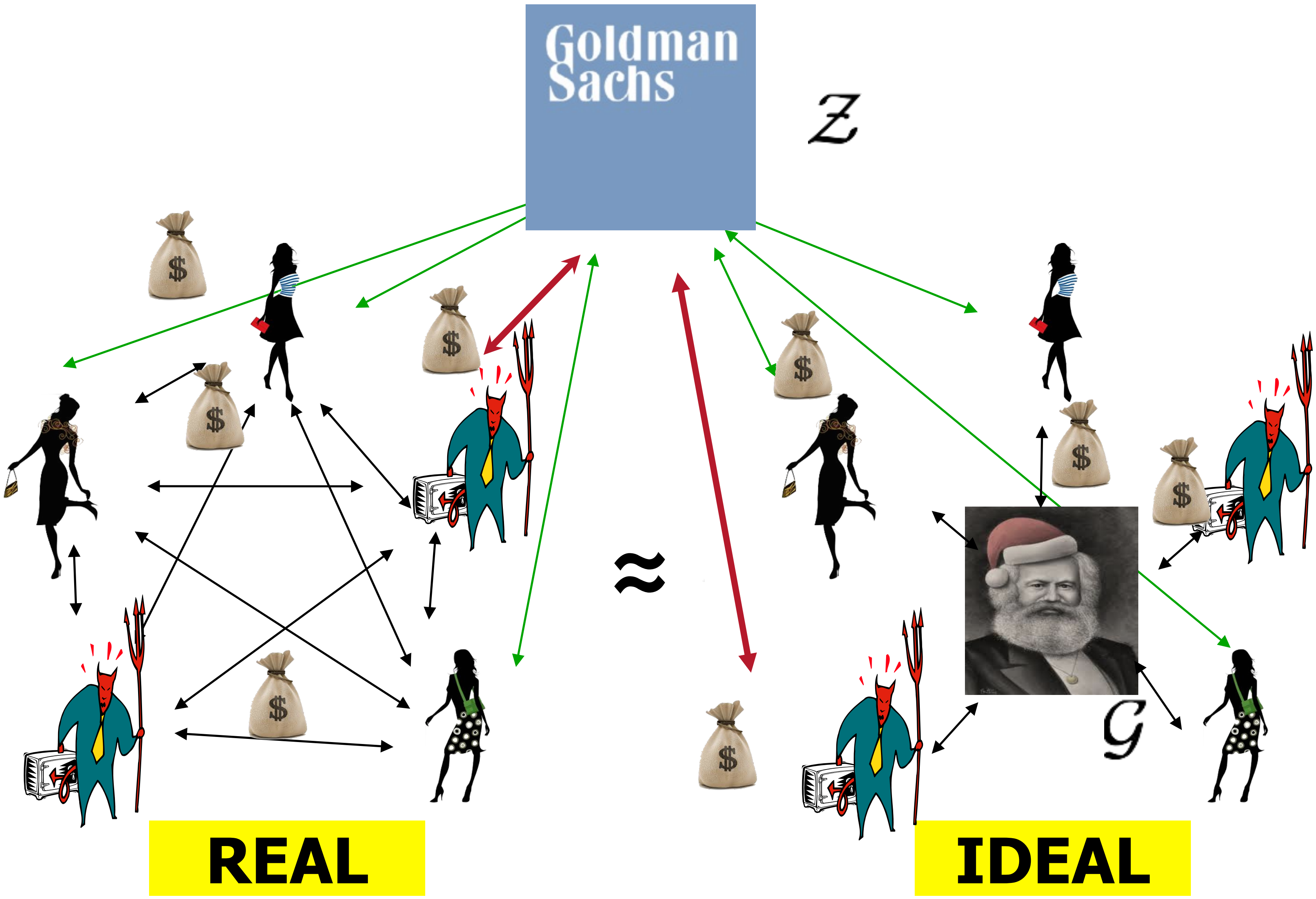

KING'S COLLEGE LIBRARY, CAMBRIDGE


Match??

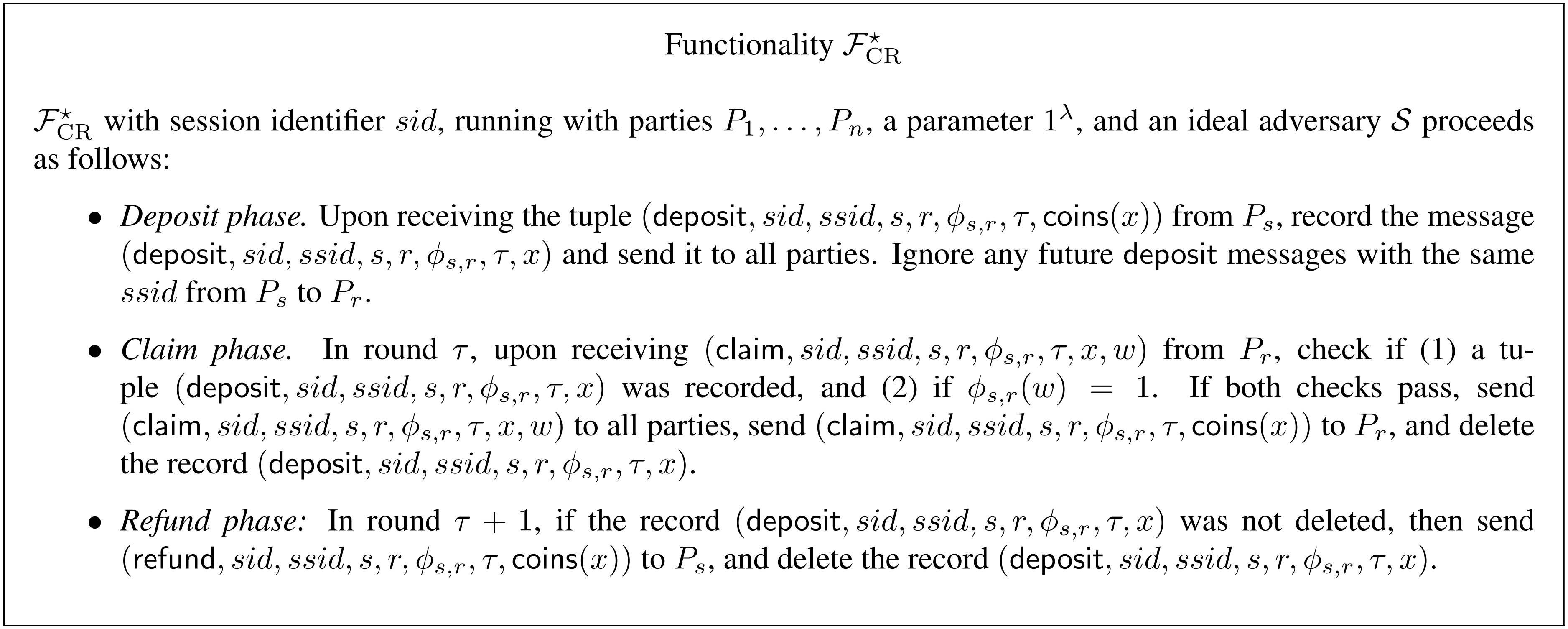
Standard Security Definitions



Security with “coins”



Abstraction of Bitcoin Functionality



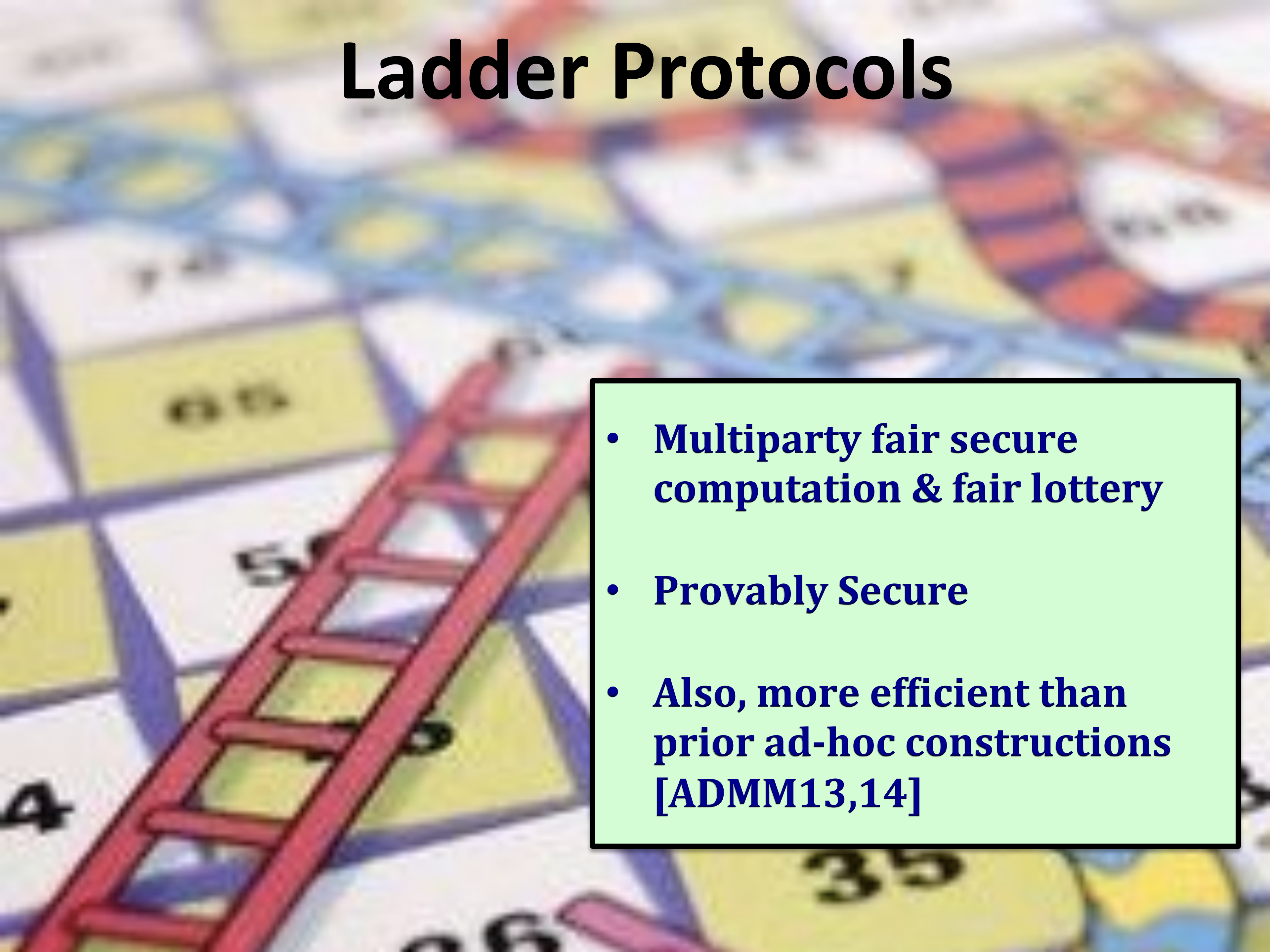
Functionality $\mathcal{F}^{\star}_{\mathrm{CR}}$

$\mathcal{F}^{\star}_{\mathrm{CR}}$ with session identifier sid, running with parties $P_1, \ldots, P_n$, a parameter 1^{λ}, and an ideal adversary $\mathcal{S}$ proceeds as follows:

- *Deposit phase.* Upon receiving the tuple $(\mathsf{deposit}, sid, ssid, s, r, \phi_{s,r}, \tau, \mathsf{coins}(x))$ from P_s, record the message $(\mathsf{deposit}, sid, ssid, s, r, \phi_{s,r}, \tau, x)$ and send it to all parties. Ignore any future deposit messages with the same $ssid$ from P_s to P_r.
- *Claim phase.* In round τ, upon receiving $(\mathsf{claim}, sid, ssid, s, r, \phi_{s,r}, \tau, x, w)$ from P_r, check if (1) a tuple $(\mathsf{deposit}, sid, ssid, s, r, \phi_{s,r}, \tau, x)$ was recorded, and (2) if $\phi_{s,r}(w) = 1$. If both checks pass, send $(\mathsf{claim}, sid, ssid, s, r, \phi_{s,r}, \tau, x, w)$ to all parties, send $(\mathsf{claim}, sid, ssid, s, r, \phi_{s,r}, \tau, \mathsf{coins}(x))$ to P_r, and delete the record $(\mathsf{deposit}, sid, ssid, s, r, \phi_{s,r}, \tau, x)$.
- *Refund phase:* In round $\tau + 1$, if the record $(\mathsf{deposit}, sid, ssid, s, r, \phi_{s,r}, \tau, x)$ was not deleted, then send $(\mathsf{refund}, sid, ssid, s, r, \phi_{s,r}, \tau, \mathsf{coins}(x))$ to P_s, and delete the record $(\mathsf{deposit}, sid, ssid, s, r, \phi_{s,r}, \tau, x)$.

Figure 1: The special ideal functionality $\mathcal{F}^{\star}_{\mathrm{CR}}$.

Ladder Protocols



- Multiparty fair secure computation & fair lottery
- Provably Secure
- Also, more efficient than prior ad-hoc constructions [ADMM13,14]

Killer App for MPC?

People don’t seem to care much about privacy… MPC has to provide something that people really need right now…

- **Fair exchange?**
- **Fair lottery?**
- **REAL poker over the internet?**

Thank You!!
ePrint 2014/129

Thank You!

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 259426 – ERC – Cryptography and Complexity