Superposition Attacks on Cryptographic Protocols

Jakob Funder[1]

Joint work with
Ivan Damgård[1], Jesper Buus Nielsen[1], Louis Salvail[2]

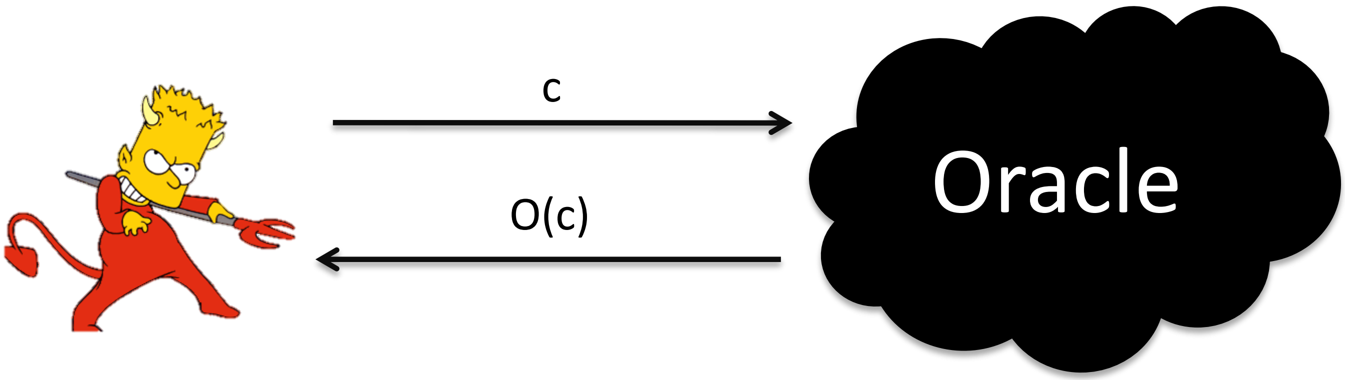
[1]Aarhus University, [2]Université de Montréal

Rough Outline

- Introduce our model
- Discuss several schemes in this model
  - ZK proofs, Secret Sharing
- Justification and Conclusion

The Model: Superposition attacks

Modeling cryptographic attacks

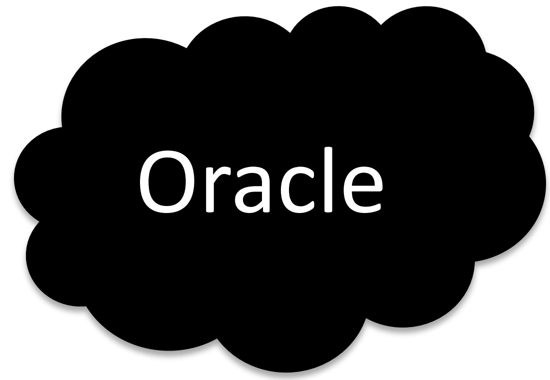


- Given the access to the oracle, there is some task the adversary cannot accomplish
- Eg. Secret Sharing, ZK proofs

Modeling cryptographic attacks

c

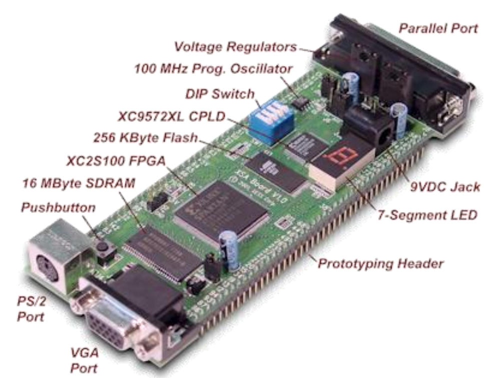
O(c)



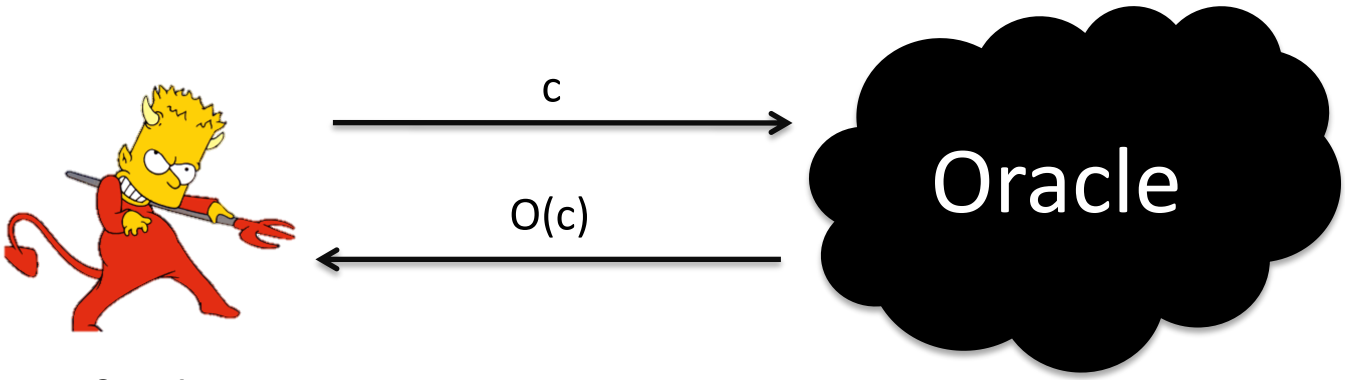
How do we make sure our model matches implementation?
This is notoriously hard! (eg. Leakage).
Hardware countermeasures or better models.

?

?

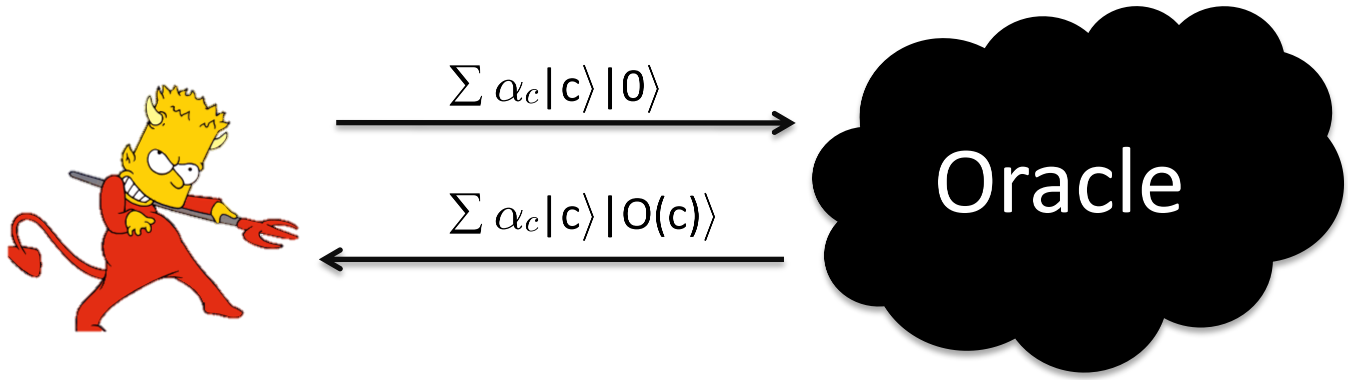


Modeling cryptographic attacks in a quantum world



- What if adversary is quantum?
  - Eg. RSA, ZK ([Wat06])

Modeling cryptographic attacks in a quantum world



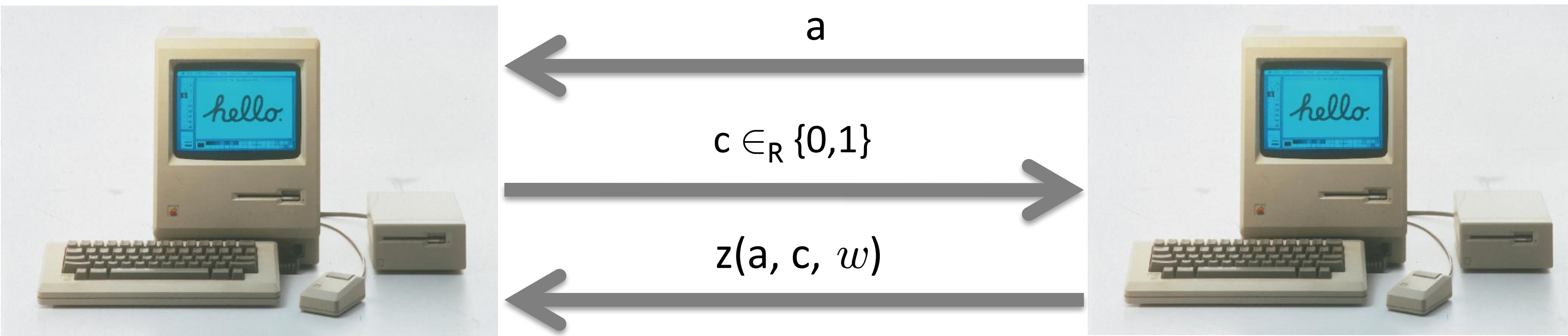
- What if adversary is quantum?
  - Eg. RSA, ZK ([Wat06])
- We ask: What if oracle access is quantum?
  - Eg. Superposition of shares in SS, challenges in ZK proofs.
  - Note that essentially all security proofs need to be reconsidered in this model.
- Justification: Later!

Example:
Σ-protocol

Σ-protocol – in classical setting

(x) w

V P



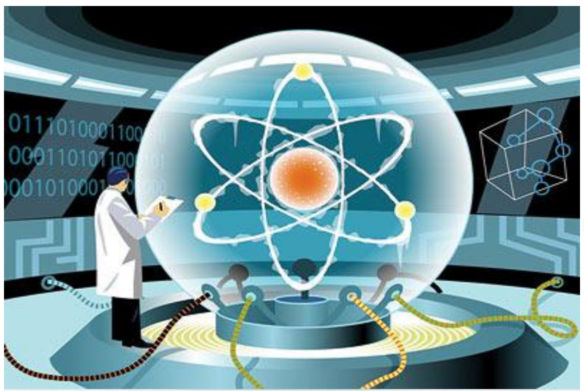
- Accept/Reject

- Looking at the Zero Knowledge aspect of protocol

Σ-protocol – in quantum setting

(x) w

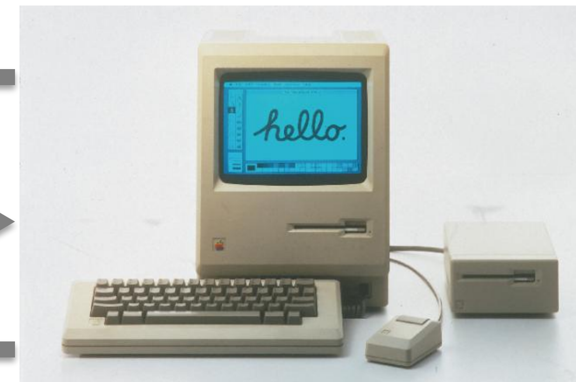
V P



a

c $\in_R$ {0,1}

z(a, c, w)



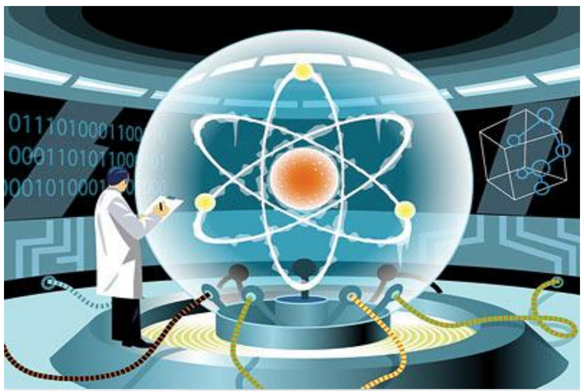
- Accept/Reject

- ZK if quantum verifier? $\approx$ YES [Wat06]

Σ-protocol – in quantum setting

(x) w

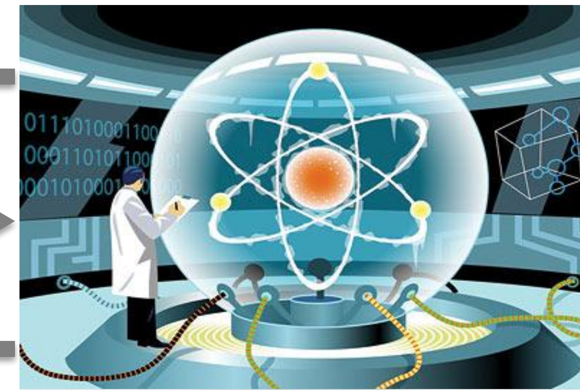
V P



a

$c \in_R \{0,1\}$

z(a, c, w)

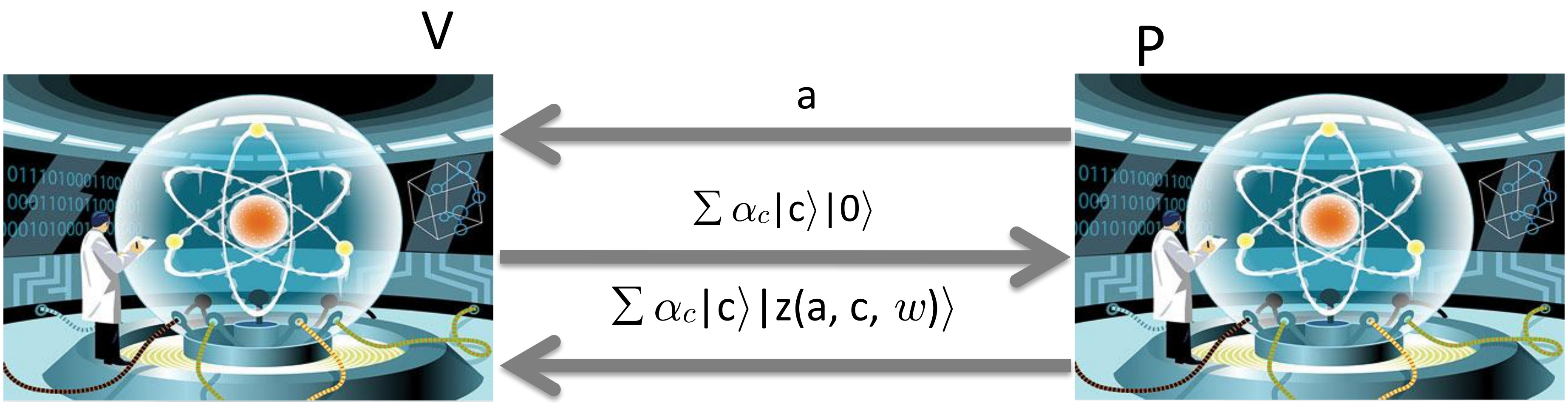


- Accept/Reject

- ZK if quantum verifier? $\approx$ YES [Wat06]

Σ-protocol – in quantum setting

(x) w



- Accept/Reject

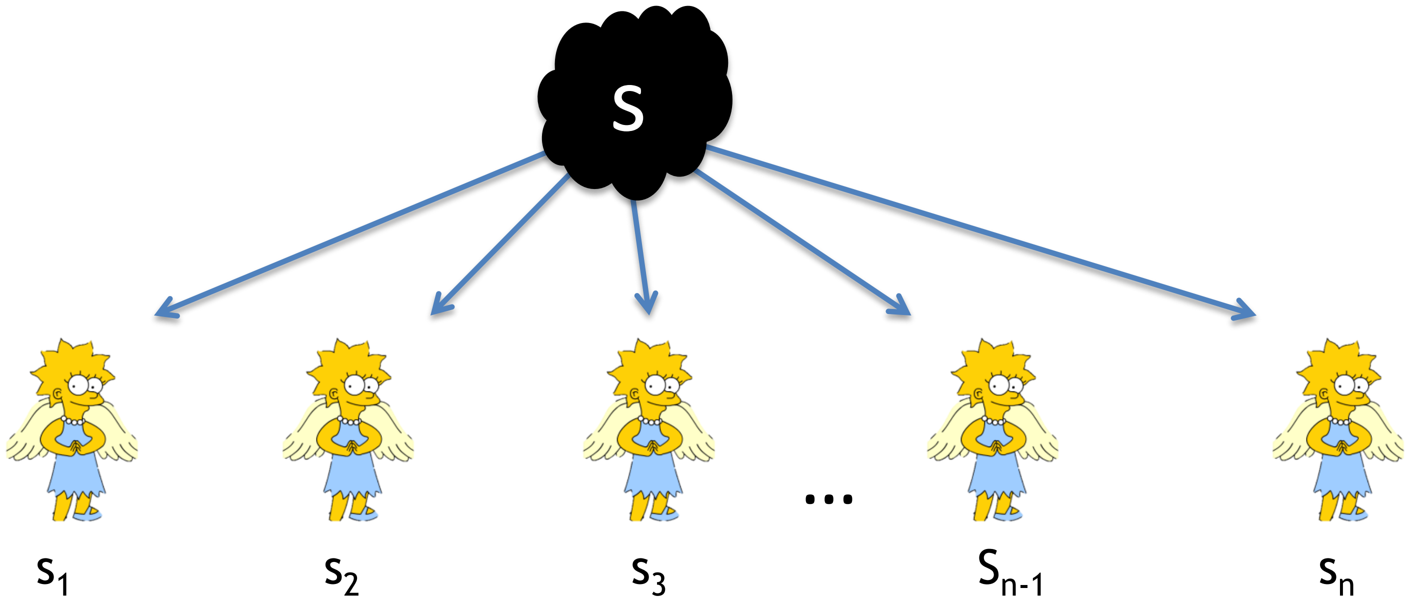
- ZK if quantum verifier? $\approx$ YES [Wat06]
- ZK if quntum access to P? NO – at least not generally

Analysis of graph isomorphism ZK proof

- Hard problem: is the two graphs (G_0,G_1) isomorphic?
- Secret witness: $\pi(G_0)=G_1$
- c = $\phi(G_0)$
- Challenge is isomorphism from c to either G_0 or G_1
- Superposition attacks allows for a superposition of a isomorphism from c to G_0 and e to G_1
- Is this Zero knowledge?
  - No. Unless GI in most cases is easy on a quantum computer.

Shamir's Secret Sharing

Shamir's Secret Sharing



- Let f be a random polynomial of degree at most t
- $s_i = f(i)$, $f(0) = s$
- *Classically secure* iff attacker acquires at most t shares
  - We call the family of such sets (A) the ‘adversary structure’ (F).

Superposition attacks against Shamir's Secret Sharing

- We gain access to the shares in superposition
- Superposition attack: $\sum_{\mathrm{A}} \alpha_A |\mathrm{A}\rangle |0\rangle$
- Response: $\rho_s = \sum p_r |\psi_r\rangle\langle \psi_r|$
- Where $|\psi_r\rangle = \sum_{\mathrm{A}} \alpha_A |\mathrm{A}\rangle |\text{shares in A}\rangle$

- We say it's secure iff for all s, s': $\rho_s = \rho_{s'}$

Superposition attacks against Shamir's Secret Sharing

- We show security for adversary structure G, where G is at most t/2 shares.

- That is, the state $\sum_{A \in G} \alpha_A |A\rangle |\text{shares in } A\rangle$ is (over the randomness) independent of the secret iff $G^2 \subseteq F$
  - Where $G^2 = \{ A \mid A = B \cup C \text{ where } B, C \in G \}$

- This extends naturally to all classical SS schemes.

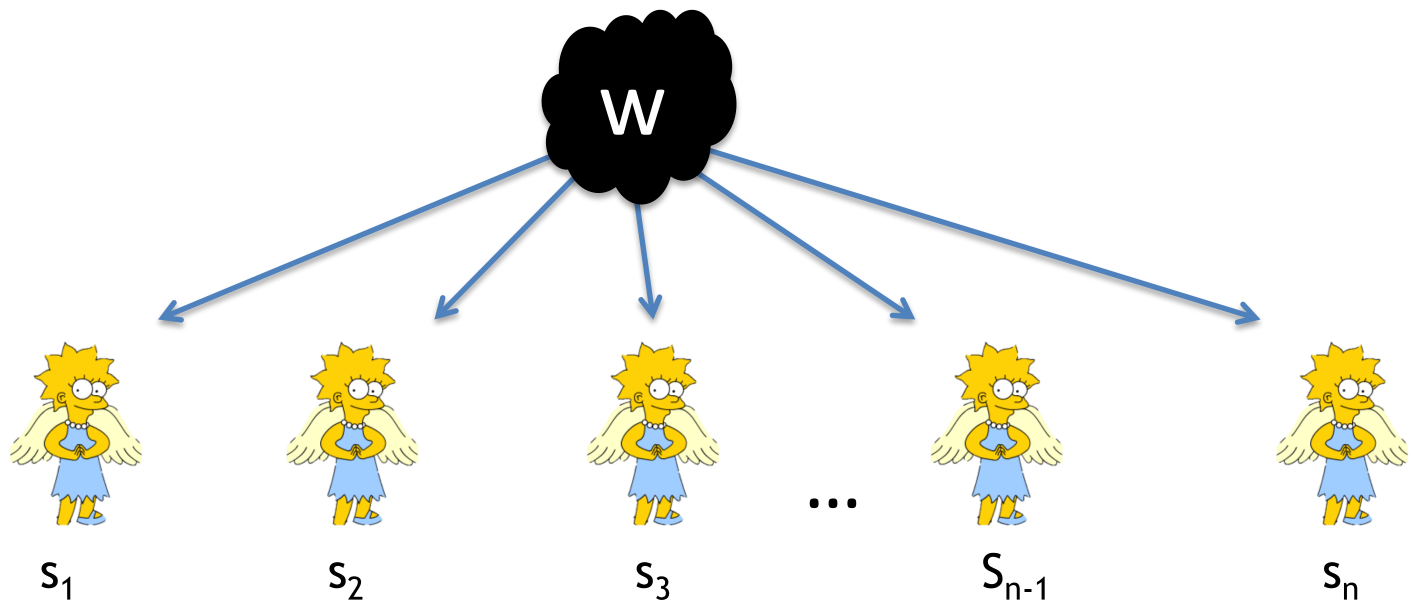
General result for SS

- General Theorem for Secret Sharing
- Let F be the classical adversary structure for SS scheme S,
- S is perfectly secure against superposition G-attacks if and only if $G^2 \subseteq F$.
- $G^2 = \{ A \mid A = B \cup C \text{ where } B,C \in G\}$

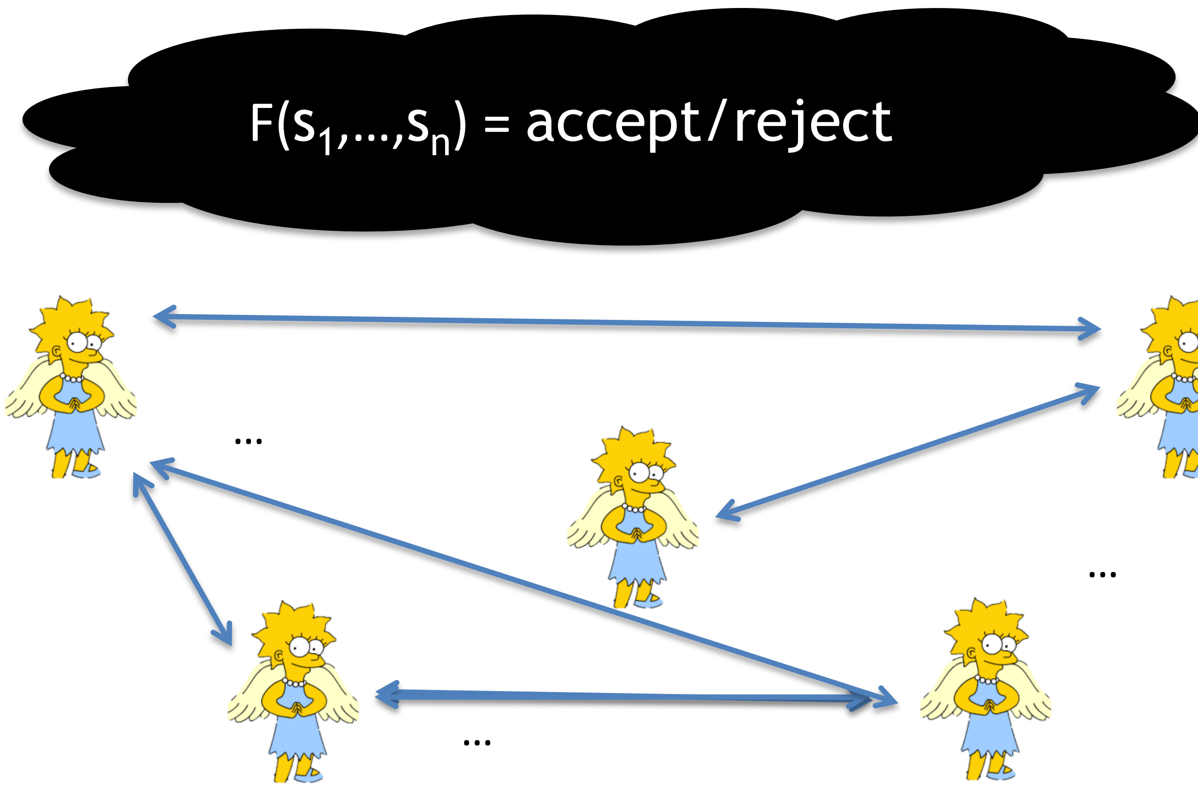
Superposition-secure ZK proof for all of NP

Based on [IKOS09]

Secret sharing of witness



MPC to test if correct sharing



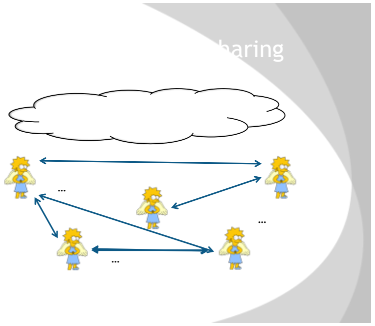
ZK protocol

(x)

w

V

P



a = (com(s_1), …, com(s_n))

A ∈ F

Assuming SS is secure against superposition attacks, even if A is chosen in superposition, V learns nothing about the secret.

Accepts if all parties output accept

What about quantum protocols?

- Surely security proofs already assume full quantum oracle access?

- Not always!

- Any QSS or QMPC scheme (we know of) assumes corruption is classical.

- Our SS result naturally extends to a large class of QSS schemes.

General Theorem for QSS

- Assume QSS scheme S is based on a linear classical SS scheme.
- Let F be the classical adversary structure for S,
- S is perfectly secure against superposition G-attacks if and only if $G^2 \subseteq F$.
- $G^2 = \{ A \mid A = B \cup C \text{ where } B,C \in G\}$

Justification

Justification (classical protocols)

- *"Being classical"* is a hardware assumption
- This may be an extremely good assumption
  - Human, laptop, etc.
- However classical computing is moving towards the quantum limit
- Consider especially devices where the attack has full physical control over the devices(eg. a smart card)
  - Could there come a time where an attack would be able to get quantum effects by exposing it to extreme conditions? (eg. freezing it)

Justification (classical protocols)

- Quantum protocols using classical sub-protocols?
  - Would require separate hardware to run classical sub-protocol.

- In general it's (almost) always preferable to have the broadest model possible.

Justification (quantum protocols)

- Corruption in QSS and QMPC in particular;
  - We’re *not* claiming you can bribe a human in superposition.
- However corruption cover much more
  - Eg. Interacting with hardware outside of its specification (similar to QKD attacks)
  - Type of attacks possible can be extremely hardware implementation dependent and almost impossible to predict.

Summary

- Introduce new model for attacks on cryptographic protocols
- Show a number of well known schemes are not secure as they stand
  - ZK proofs, (Q)SS, (Q)MPC.
- Show how to do secure (Q)SS and secure ZK proofs in our model.

Open problems

- Our superposition attack models are slightly ad-hoc, more general approach to modeling would be preferred.
- More general results for QSS
- What kind of (Q)MPC protocols are possible?
  - We do have some results for classical MPC
- Security of cryptographic protocols in general

Questions?