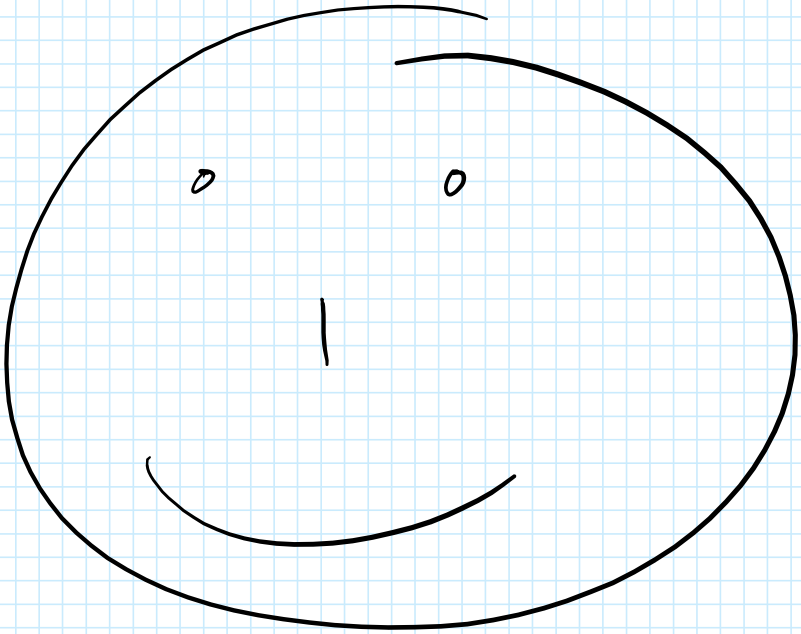
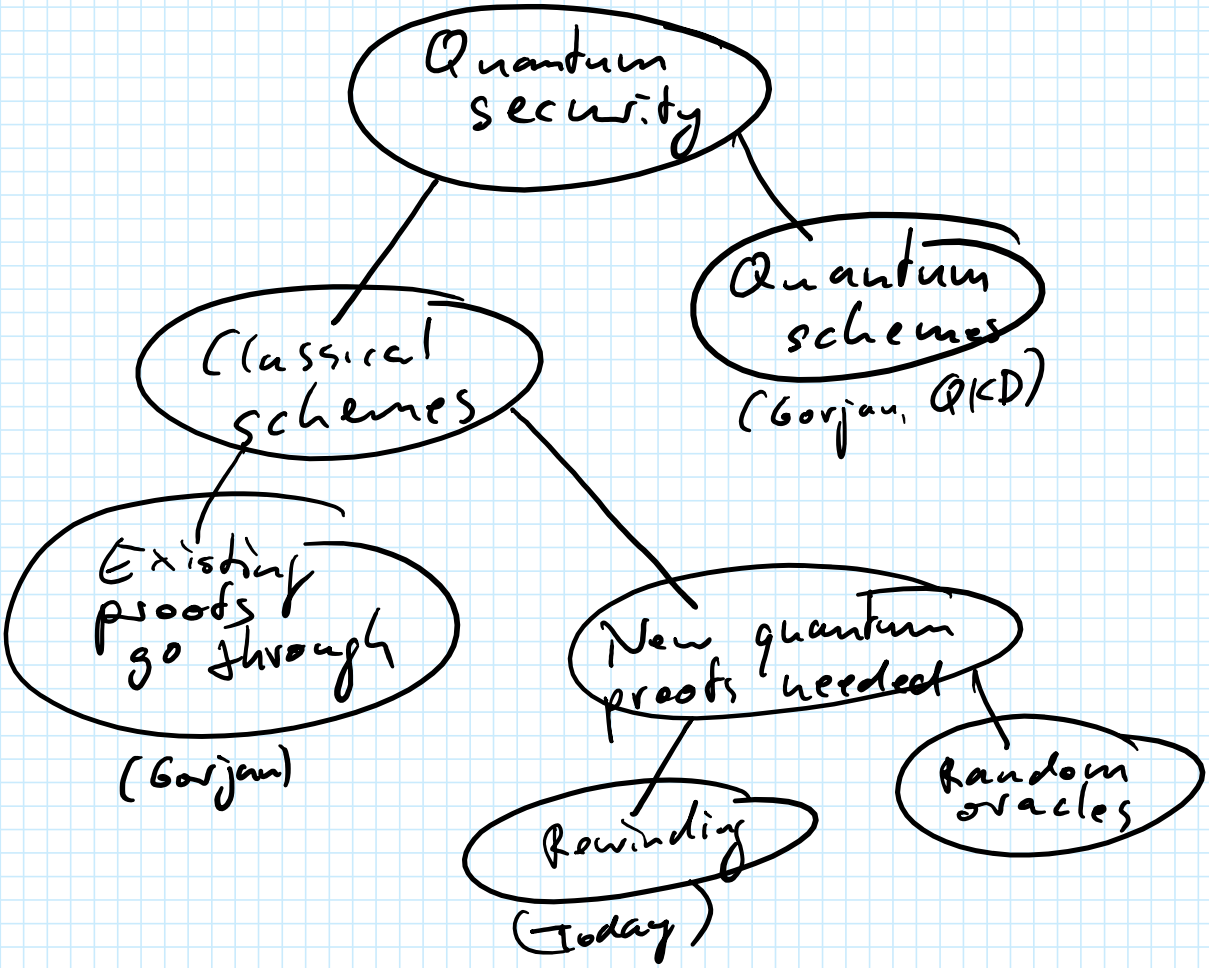
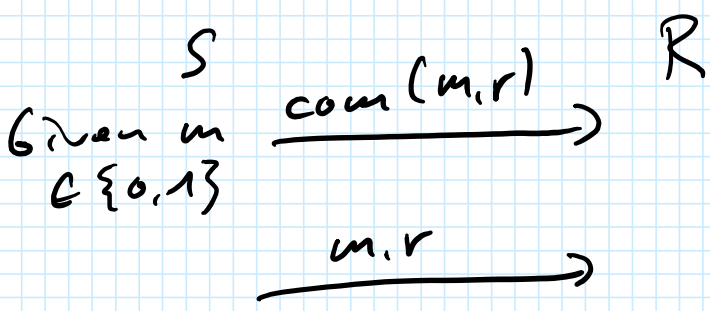




What is rewinding?

Motivational example: Commitment

C P



Hiding: m does not leak in commit phase

Binding: Sender cannot change his mind

Def (binding) ~~classical~~ quantum

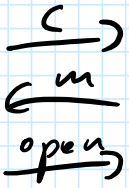
For any quantum poly S:

If $c, m, r, m', r' \leftarrow S()$ with $m \neq m'$

Then $P_0[cmr \text{ valid} \wedge cm'r' \text{ valid}]$ negligible

This implies:

Betting game

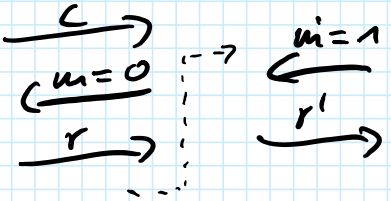


$\Pr[\text{success}] \leq \frac{1}{2} + \text{negl.}$

Intuitive But: Not correct for quantum S

What happened? Class. proof:

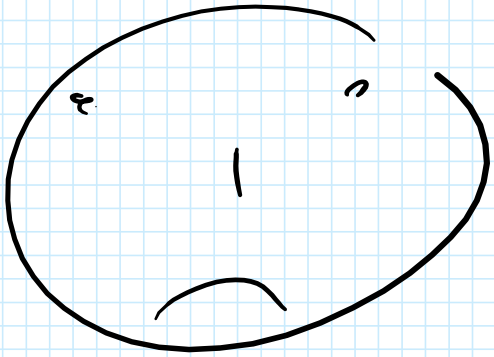
1. Assume S wins betting game. (with pr=1)
2. Run:



$m \neq m'$
cmr valid
$cm'r'$ valid

Quantumly: Cannot copy state of S

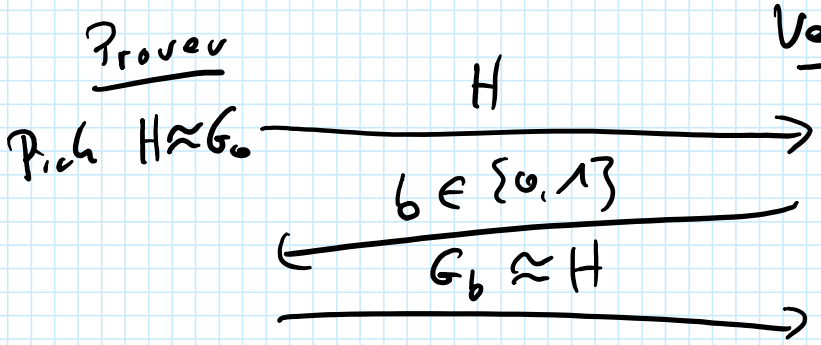
$\Rightarrow$ no rewinding here



Summary: - Some class proofs use rewinding ⇝ wrong in quantum setting
- other examples: ZK, Proof of knowledge, MPC

Zero-Knowledge Proofs

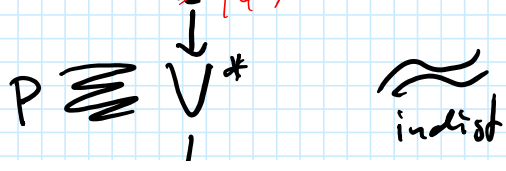
Example: I want to prove that $G_0 \not\simeq G_1$ without leaking isomorphism

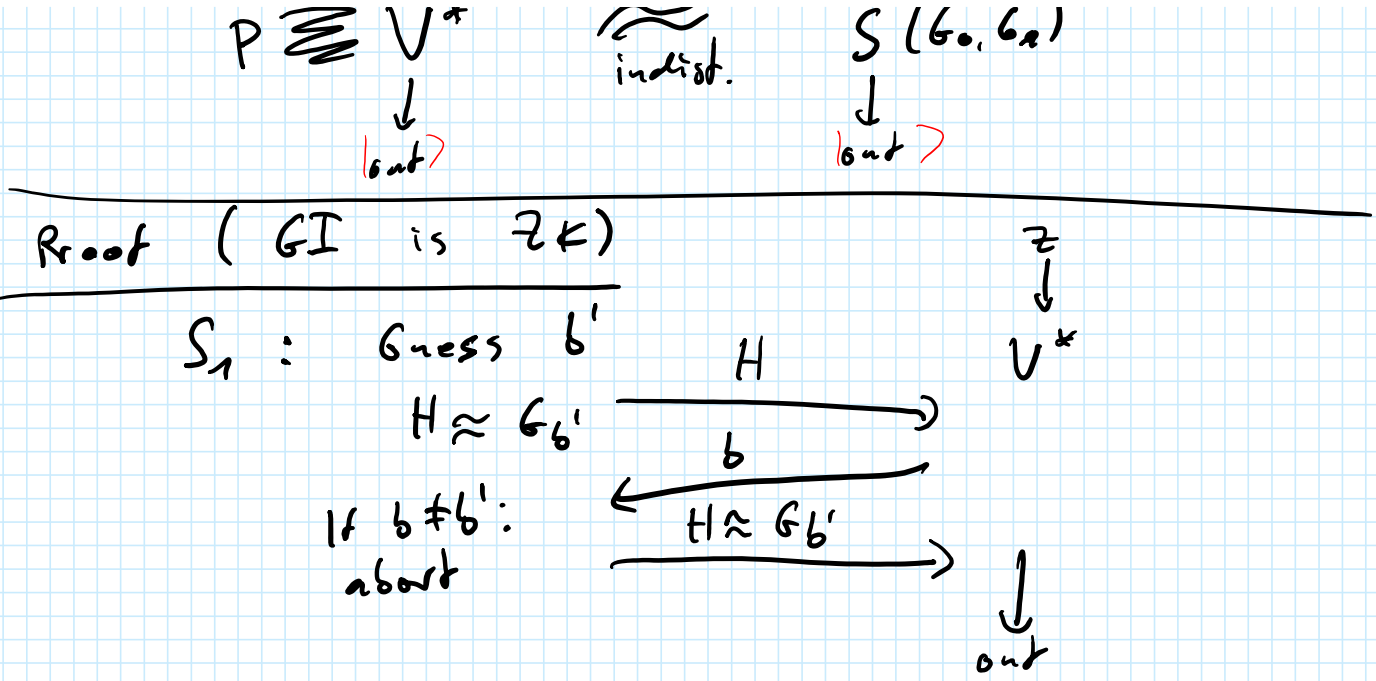


- Soundness: If $G_0 \not\simeq G_1$, with prob $\frac{1}{2}$: fail
- Zero-Knowledge: Verifier learns nothing about isomorphism (witness)

Formalize ZK

Def: For any quantum poly V^* $\exists$ quantum poly S $\forall z \in \{0,1\}^*$





Proof (GI is ZK)

S_1 : Guess b'

$H \approx G_{b'}$

If $b \neq b'$: abort

$\Rightarrow$ $S_1 \mid$ not abort $\equiv \langle P, V \rangle$

S: Repeat S_1 until success

$\Rightarrow S \equiv \langle P, V^* \rangle$ ← Rewinding

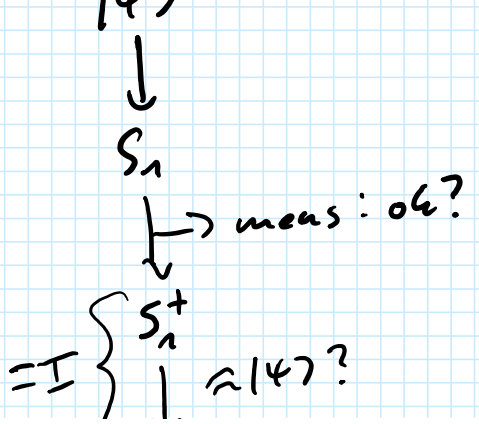
$\Rightarrow$ GI is ZK

Quantum-setting:

S_1 : Same constr. but takes $|\psi\rangle$

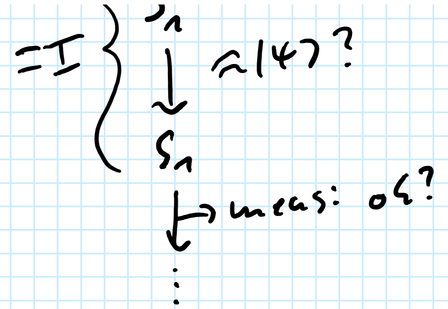
$S_1 \mid$ not abort $\equiv \langle P, V \rangle$

But: How to build S?

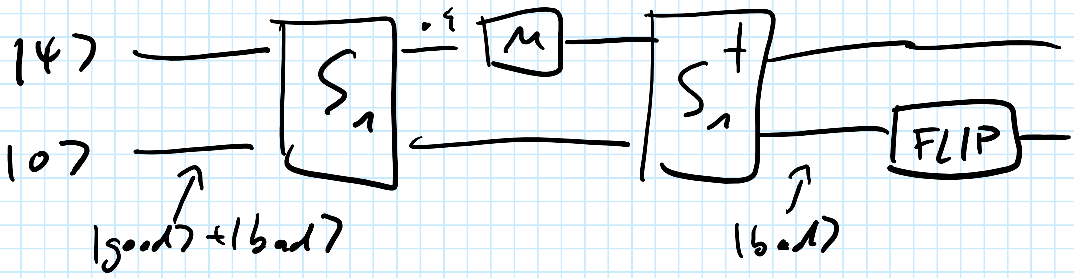


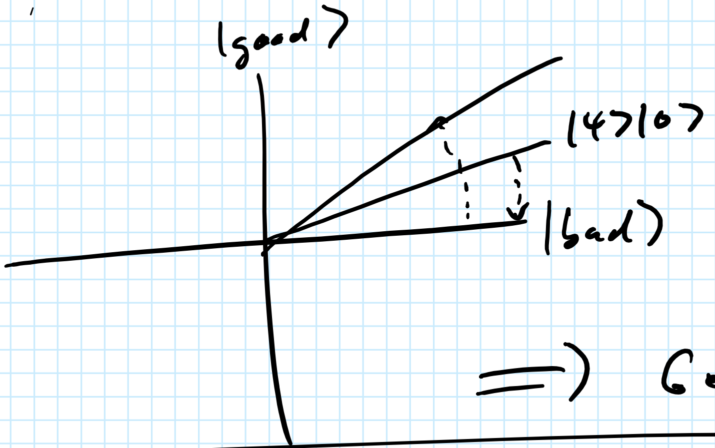
Does not work.

After first meas.: stuck



stuck





FLIP: $|0\ldots0\rangle \to -|0\ldots0\rangle$
$|x\rangle \to |x\rangle$

$\Longrightarrow$ Get good.

Challenge:
- GI is PoK
- GNI is ZK
- Fiat-Shamir is secure