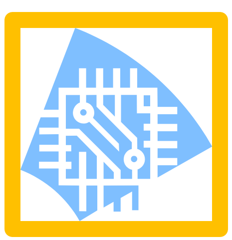
Single-shot security for one-time memories in the isolated qubits model

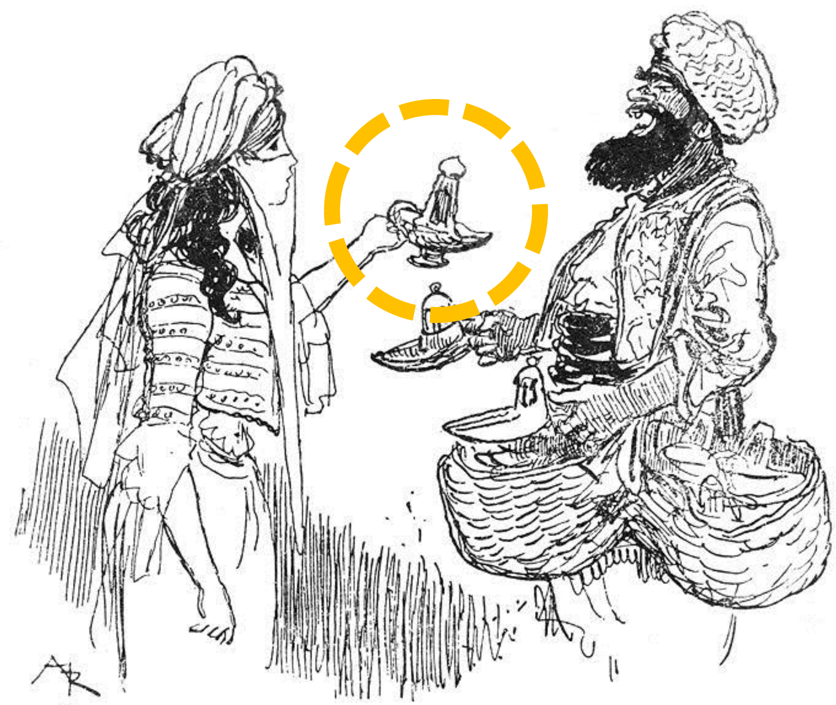
Yi-Kai Liu
National Institute of Standards and Technology (NIST)
Gaithersburg, MD, USA

Arxiv: 1402.0049

One-time memories

- Tamper-resistant cryptographic hardware
  - Needed in situations where Alice's data resides on hardware that is controlled by Eve
  - E.g., a stolen smartphone
- Want to use *simple* tamper-resistant chips to implement complex functions





Aladin - illustré par Albert Robida http://en.wikipedia.org/wiki/File:Robida_Aladin_illustration_page11.jpeg

One-time memories

- One-time memory (OTM) contains two messages s,t
  - Adversary can choose to read s or t, but not both
  - "Non-interactive oblivious transfer"
- Can be used to construct one-time programs
  - Evaluate some circuit
  - Can only be run *once*
  - Intermediate results of computation are hidden
  - [Goldwasser, Kalai & Rothblum, 2008], [Goyal et al, 2010]

One-time memories

- Can we build OTM's based on some physical principle?
  - Classical physics: no!
    (information can always be copied)
  - Quantum physics: no!
    (no-go theorems for bit-commitment, oblivious transfer)

- However, if one assumes that the adversary is k-local, then quantum bit-commitment is possible! [Salvail '98]
  - Adversary cannot entangle more than k qubits

Isolated qubits model

- All parties (both honest and dishonest) are restricted to LOCC operations
  - LOCC = "local operations and classical communication"
  - Pick a qubit, measure it, get some classical outcome, repeat...
  - No entangling gates
- Example: nuclear spins?
  - Isolated qubits can exist in a world with quantum computers

Evan-Amos, http://en.wikipedia.org/wiki/File:Oreo-Two-Cookies.jpg

Isolated qubits model

- Is there anything quantum going on here?
  - State remains separable at all times

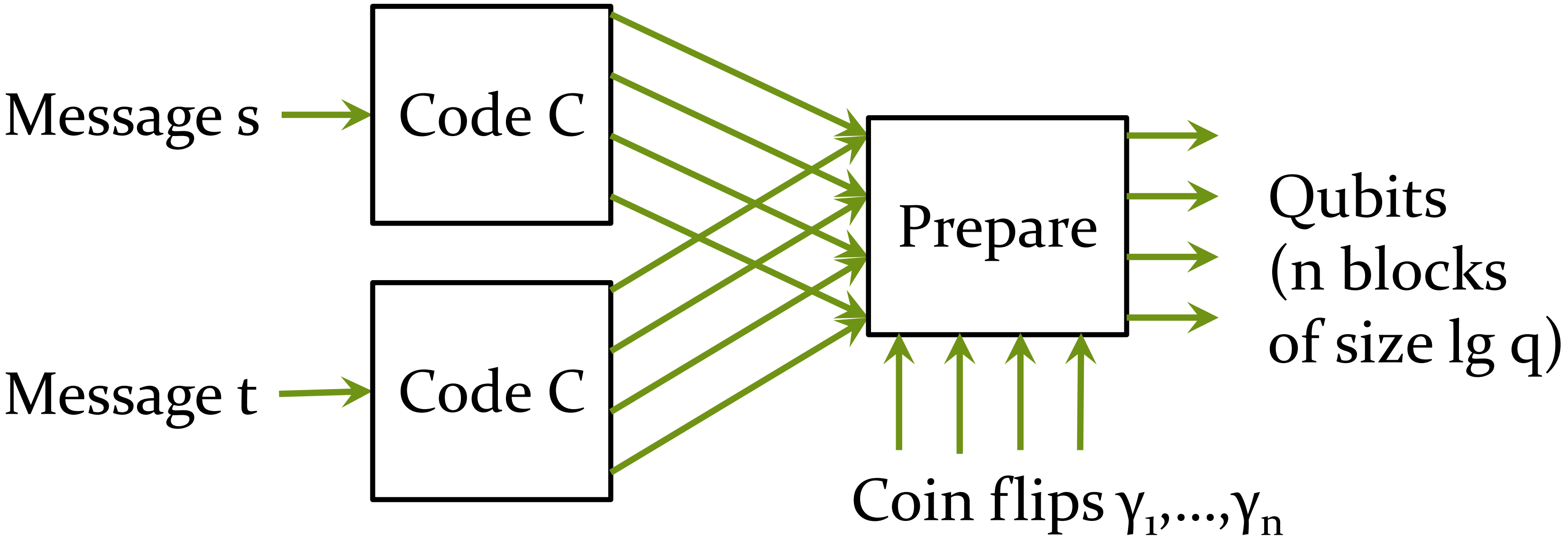
- "Nonlocality without entanglement" [Bennett et al, 1999]
  - Certain transformations using LOCC operations *can be inverted* using entangling operations, *but cannot be inverted* using LOCC

Our results

New paper: Arxiv:1402.0049

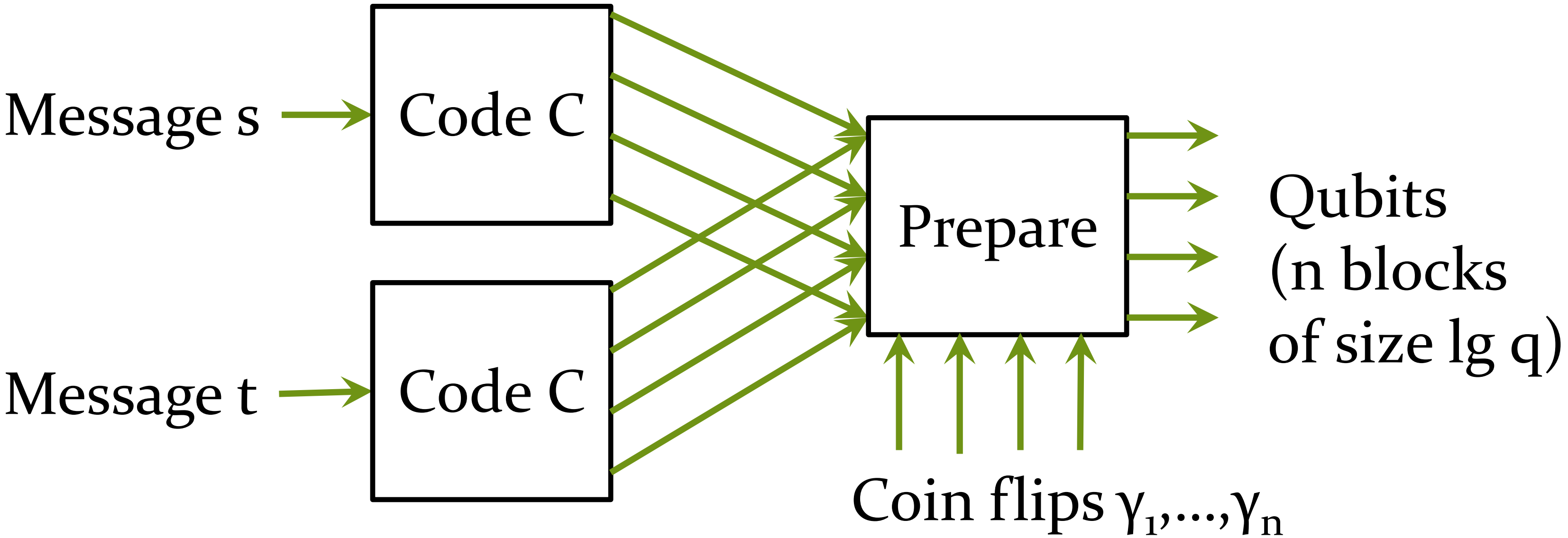
- One-time memories in the isolated qubits model
  - Based on Wiesner's idea of conjugate coding
  - Single-shot security: measure the adversary's uncertainty using the smoothed min-entropy
  - Secure against general LOCC adversaries: including adaptive sequences of weak measurements
  - Efficiently implementable: OTM's can be built using a large class of error-correcting codes

Conjugate coding



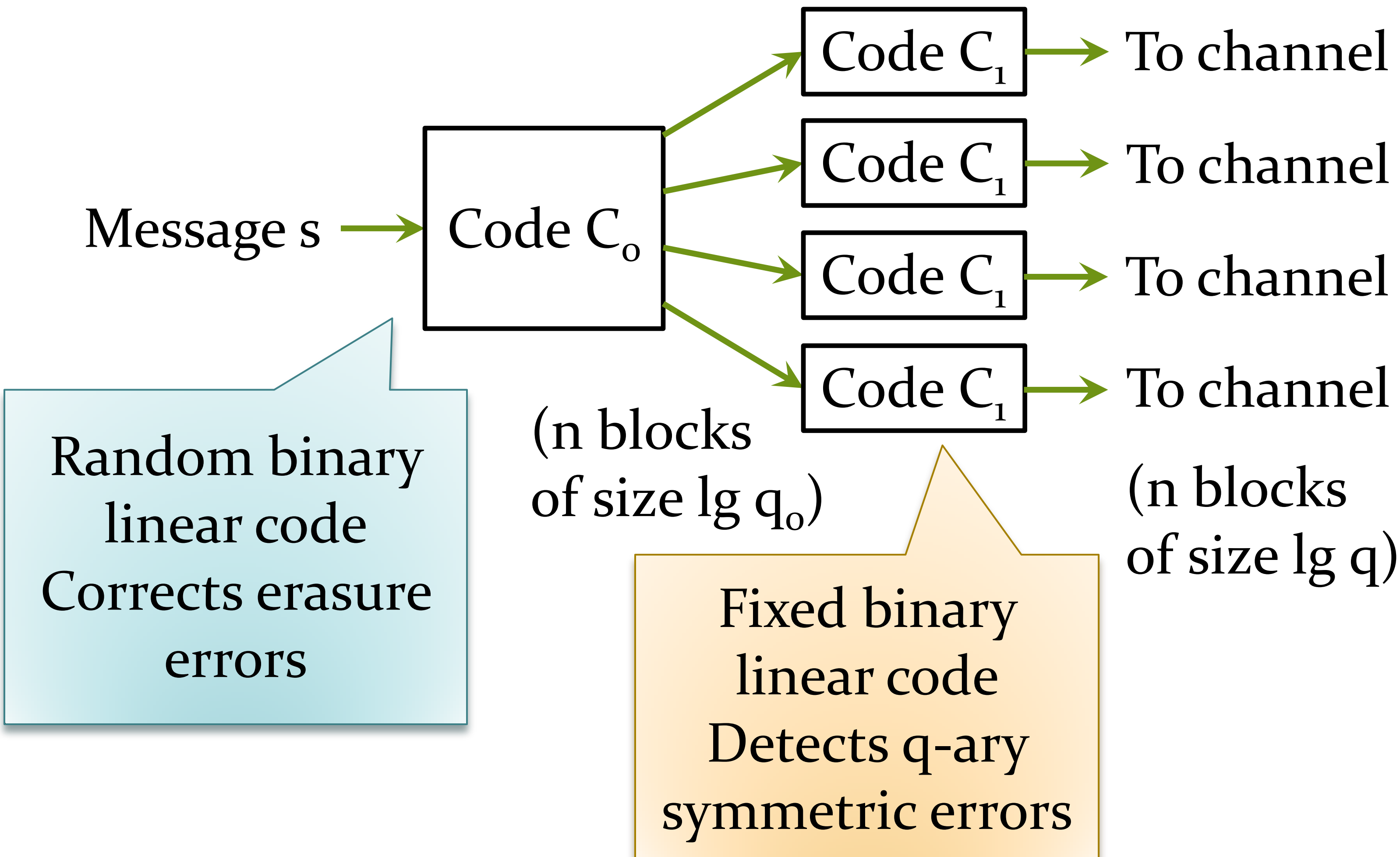
- To prepare the i'th block of qubits:
- If $\gamma_i = 0$, use the i'th block of C(s) and the standard basis
- If $\gamma_i = 1$, use the i'th block of C(t) and the Hadamard basis

Conjugate coding



- To read s: measure qubits in standard basis
- To read t: measure qubits in Hadamard basis
- This is equivalent to receiving C(s) or C(t) through a q-ary symmetric channel

Good codes for the q-ary symmetric channel



Good codes for the q-ary symmetric channel

- For large q (growing with n), this approaches the capacity of the q-ary symmetric channel
- Efficient decoding: solving linear systems of equations over GF(2)

- Other constructions:
  interleaved Reed-Solomon codes, interleaved AG codes
  [Bleichenbacher et al; Shokrollahi; Brown et al]

Security

- Ideal security goal: adversary can learn either S or T, but not both
  - Impossible, if the adversary can perform entangling gates
- We show a weaker ("leaky") notion of security, in the isolated qubits model
  - "Any cheating strategy *requires* entangling gates"
  - Honest strategies require only LOCC operations
  - However, some extra information leaks out
- For any LOCC adversary, $\mathbf{H^{\varepsilon}_{\infty}(S,T|Z) \geq (0.5 - \delta)\,\ell}$
  - Each of the messages S and T is ℓ bits long
  - Z is the adversary's output

Security

- Some issues to consider:
- Privacy amplification doesn’t work in this setting
  - Honest parties can try to use a randomness extractor, but adversary also knows the seed!
- Security comes from the choice of the code C
  - Want it to be “unstructured” – what does this mean?
- General LOCC adversaries can be quite complicated
  - Can make a long sequence of weak measurements, w/ adaptive choices

Security proof

- Prove security against separable adversaries
  - Every POVM element is a tensor product of 1-qubit operators
  - Includes LOCC as a special case

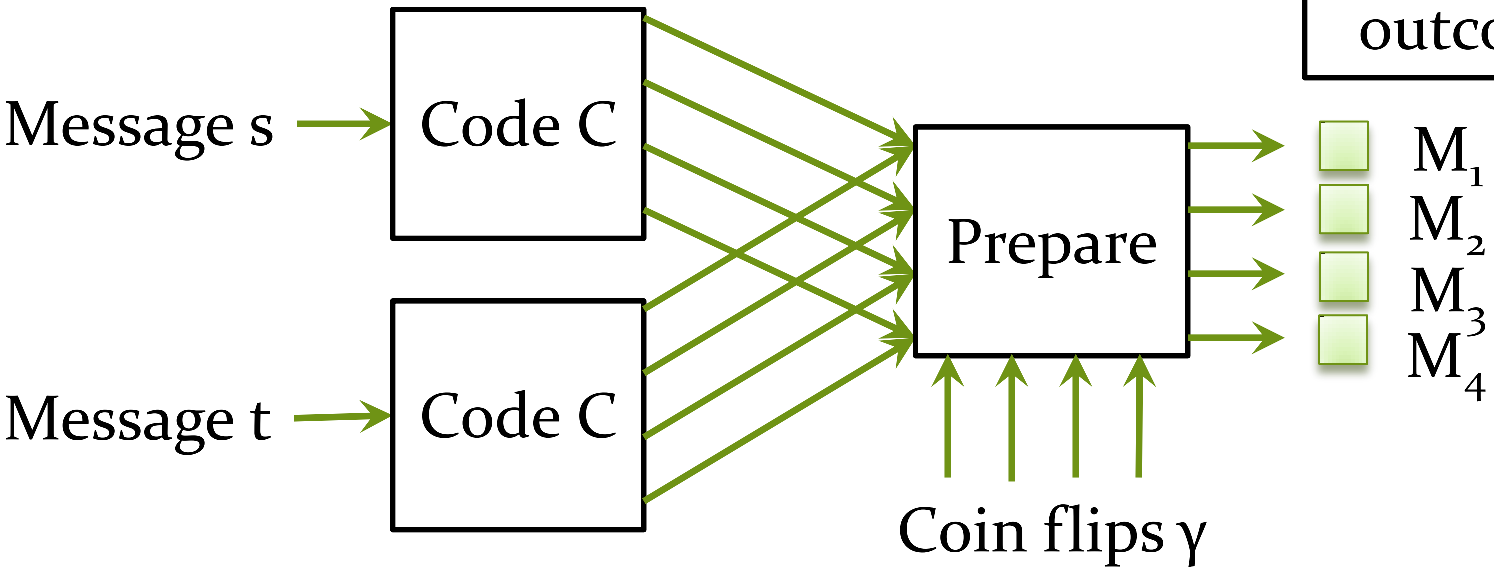
- Assume the code C is linear over GF(2)
  - Given a random codeword, a large subset of the bits will be uniformly distributed => "unstructured"
  - Prevents the adversary from learning the basis choices γ

- Use a high-order entropic uncertainty relation
  - Measuring an arbitrary state in a random BB84 basis
  - Borrowed from the bounded quantum storage model [Damgard et al, 2006]

Given a separable adversary A

Security proof

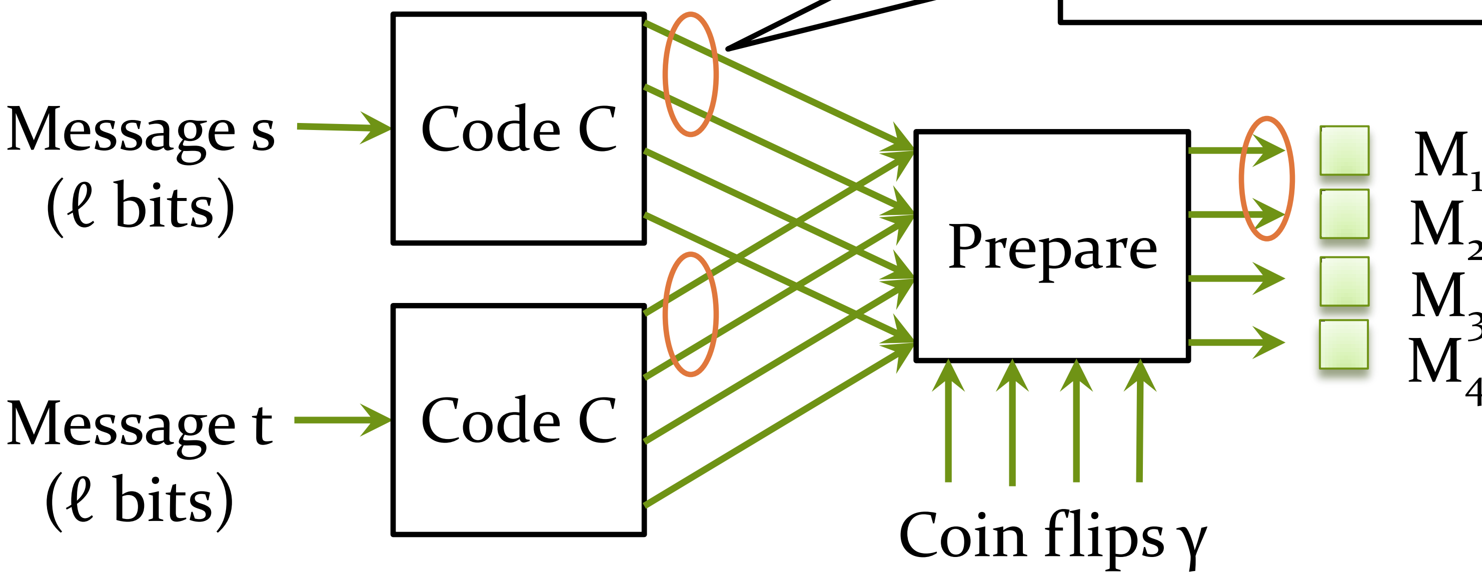
Fix some measurement outcome M



- Want to analyze Pr(S,T|M)
- Consider a fictitious adversary A' that measures each qubit once, and observes $M_1, M_2, M_3, \ldots$ (call this event M')
- Then Pr(S,T|M) = Pr(S,T|M')

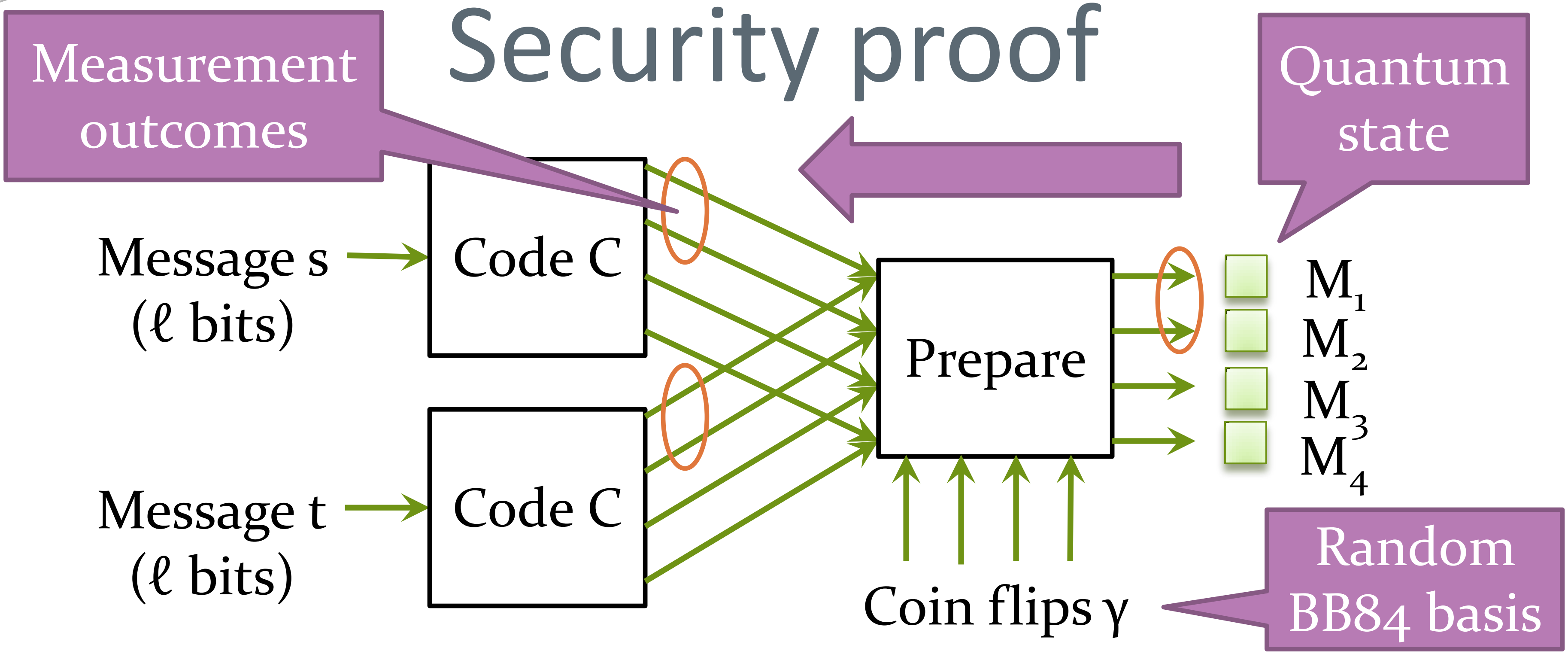
Security pro

There exists a subset of ℓ bits of C(s) that are uniformly distributed



- Wlog, suppose the fictitious adversary A' measures this subset of qubits first, and observes M_1, M_2 (call this event M'')
- Want to analyze Pr(S,T|M'')
- Note: coin flips Γ conditioned on M'' are still uniformly distributed

Security proof



- Note: coin flips Γ conditioned on M" are still uniformly distributed
- Now run the experiment backwards…
- Use the uncertainty relation to lower-bound $H^{\varepsilon}_{\infty}(S,T|M")$

Outlook

- Isolated qubits model
- One-time memories (OTM's) using conjugate coding
  - Efficient implementations
  - Single-shot security against general LOCC adversaries

- **Can we control the leakage of information from our OTM's?**
  - Necessary to construct one-time programs
  - Note: LOCC also implies strong constraints on the types of information that the adversary can learn
  - Conjecture: for one-time programs based on garbled circuits, the relevant information cannot be extracted via LOCC
  - More generally, can we construct ideal OTM's using a random oracle, or some variant of leakage-resilient encryption?

- **Beyond LOCC and the isolated qubits model**
  - Are our OTM's secure against Salvail's k-local adversaries?