Tamper-Resistant Cryptographic Hardware in the Isolated Qubits Model

Yi-Kai Liu

National Institute of Standards and Technology

Gaithersburg, MD, USA

University of Maryland 1856

Center for Quantum Information and Computer Science

NIST National Institute of Standards and Technology U.S. Department of Commerce

How to build tamper-resistant cryptographic devices?

<u>End goal:</u>

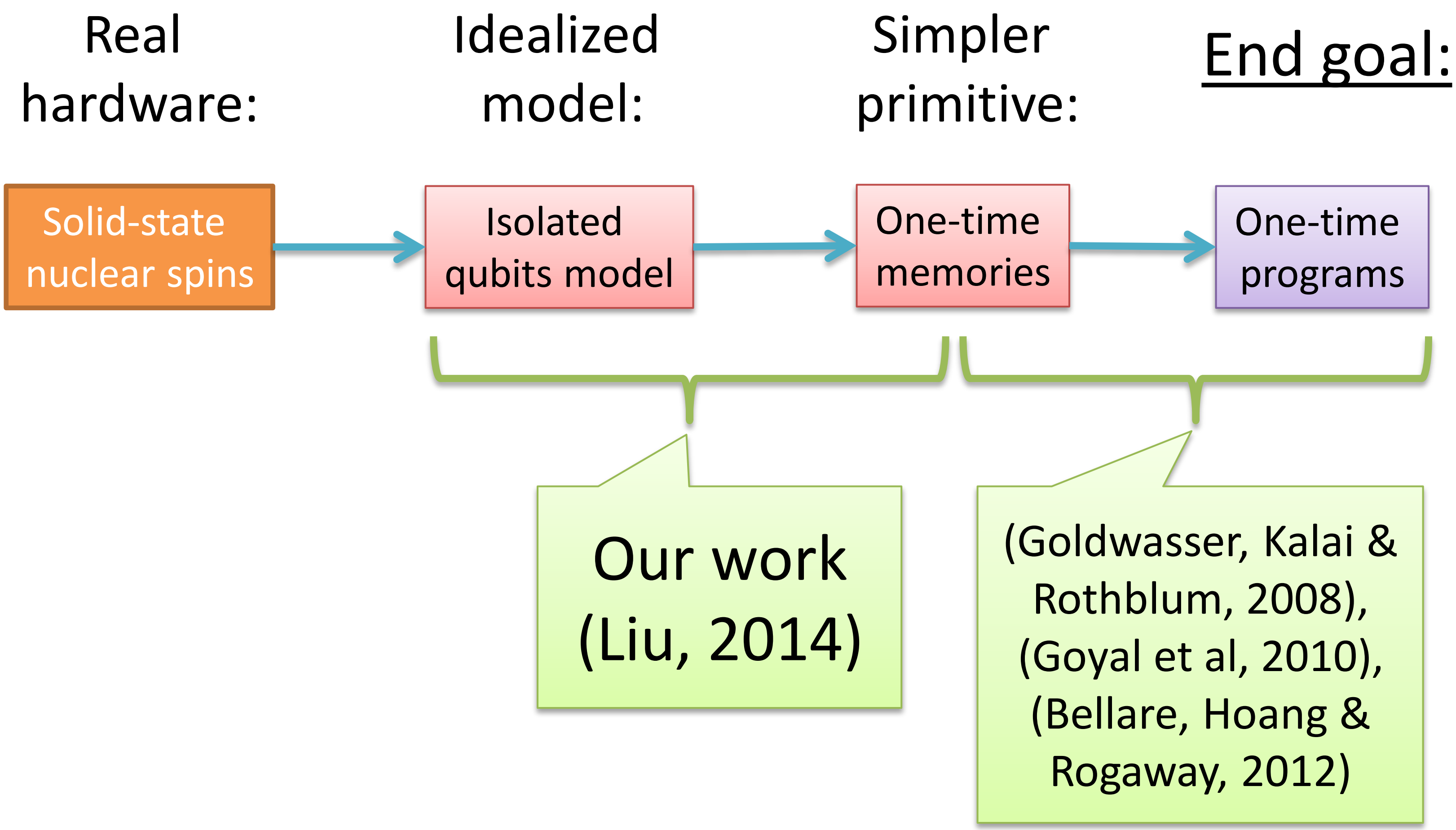
One-time programs

Program can be run <u>only once</u>, on an input supplied by the user

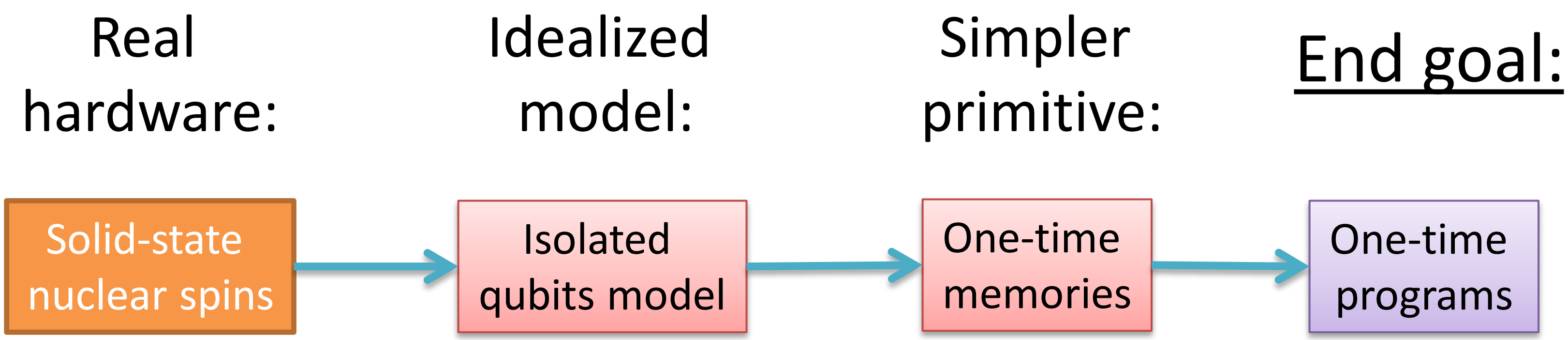
Intermediate results of the computation are <u>hidden</u>

Related to program obfuscation and copy-protection

How to build tamper-resistant cryptographic devices?



How to build tamper-resistant cryptographic devices?



- Why is quantum information useful?
  - Quantum states cannot be cloned, measurement disturbs the state, etc.
  - But it's more subtle than that… quantum bit-commitment, oblivious transfer are <u>not</u> possible (Mayers; Lo and Chau)

Our results (1/2)

- One-time memories based on "conjugate coding"
  - Old idea due to Wiesner, <u>not</u> secure against quantum adversaries
  - We show how to instantiate it, so that it <u>is</u> secure against a natural sub-class of quantum adversaries
    - "Isolated qubits model"
  - Construction has several desirable properties:
    - "Single-shot security"
    - Security against general LOCC adversaries
    - Efficiently implementable
    - But it leaks information…

Y.-K. Liu, CRYPTO 2014

Our results (2/2)

- How to stop leakage: privacy amplification in the isolated qubits model
  - Usual solution: use an extractor, w/ random seed
  - Trouble: OTM's are non-interactive
    - No way to generate a random seed that is unknown to the adversary
  - Instead, use a deterministic extractor
    - Can be secure because adversary is restricted to LOCC

Y.-K. Liu, in preparation

Isolated qubits are fun

- For theorists:
  - Another model, where many interesting cryptographic tasks are possible!
    - Known constructions seem very far from optimal!
    - Based on simple probabilistic constructions, crude bounds
- For experimentalists:
  - Another family of interesting quantum devices that can be realized
    - Very different from quantum repeaters
    - Want long coherence times, good single qubit operations, no entanglement swapping

This talk

- Overview
  - One-time memories, why they are useful
  - Isolated qubits model
- How to construct OTM’s in the isolated qubits model
  - Leaky OTM’s
  - Privacy amplification

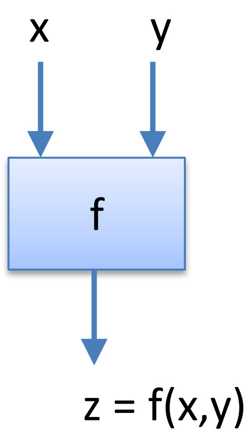
One-time memories

- One-time memory contains two messages s,t
  - Adversary can choose to read s or t, but not both
  - “Non-interactive oblivious transfer”

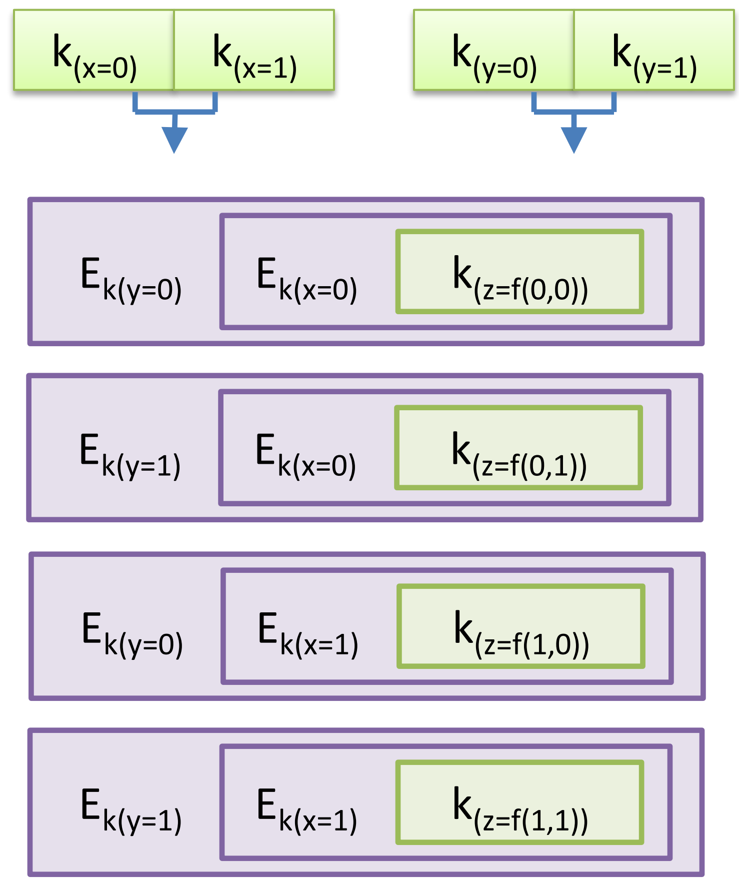
One-time programs from one-time memories

- Use Yao's garbled circuits (Goldwasser et al, 2008)

One gate from the original circuit:



One-time program:



One-time memories

E_k( ) means encryption with key k

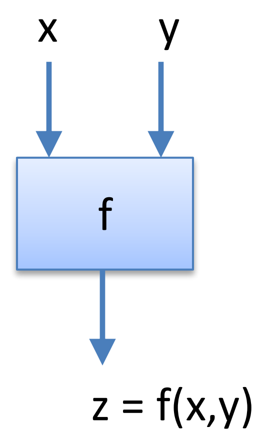
Also note: adaptive security (Bellare et al, 2012), quantum one-time programs (Broadbent et al, 2012)

One-time programs from one-time memories

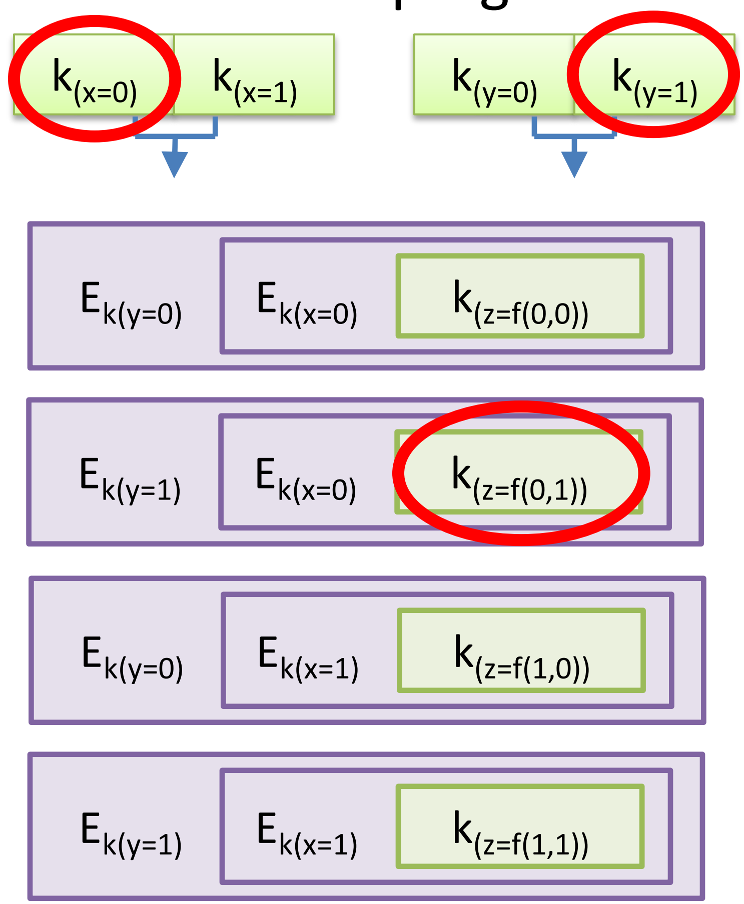
- Use Yao's garbled circuits (Goldwasser et al, 2008)

Choose inputs
x=0, y=1

One gate from the original circuit:



One-time program:



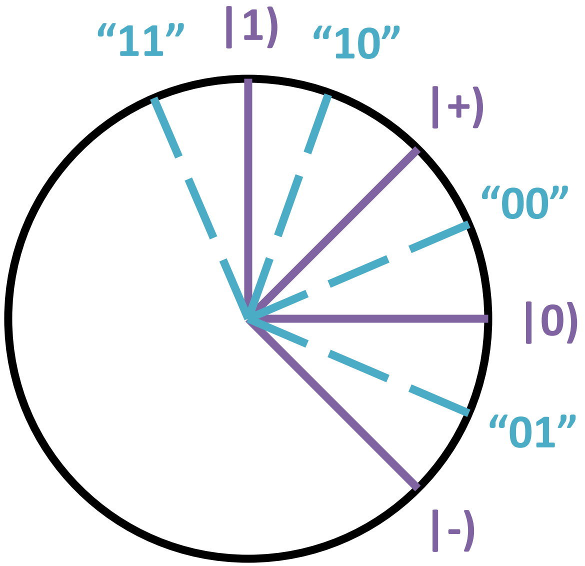
One-time memories

$E_k(\ )$ means encryption with key k

Also note: adaptive security (Bellare et al, 2012), quantum one-time programs (Broadbent et al, 2012)

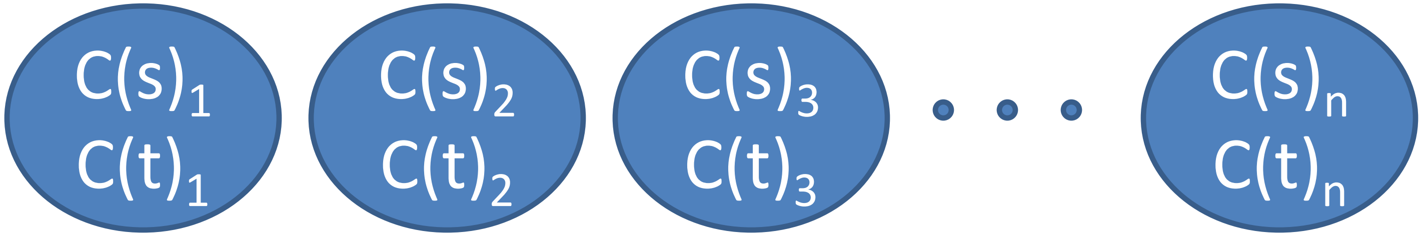
One-time memories using qubits?

- Conjugate coding (Wiesner, ~1970)
  - Encode two classical bits (x,y) into one qubit
  - Measure in standard basis: learn x, w/ prob ≈ 0.85
  - Measure in Hadamard basis: learn y, w/ prob ≈ 0.85



One-time memories using qubits?

- Conjugate coding (Wiesner, ~1970)
  - Take two strings (s,t), apply a classical error-correcting code C, then encode using n qubits

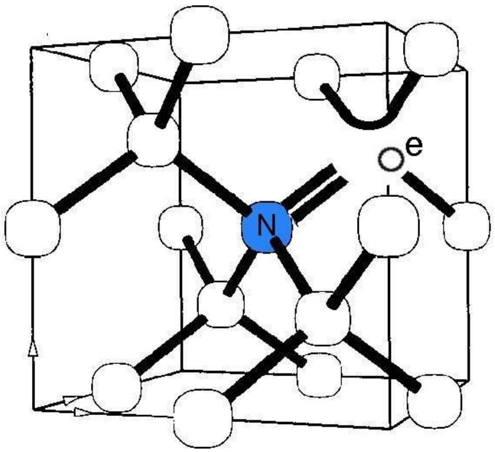


- Bad news: can recover both messages, using many-qubit entangling operations
  - Run the classical decoding algorithm in superposition
  - Recover s without collapsing the superposition
  - Then repeat the procedure to recover t

Isolated qubits model

- We propose a new class of quantum devices: isolated qubits
  - Single qubit operations are allowed
  - Cannot perform operations that entangle multiple qubits
  - LOCC = “local operations and classical communication”

- Modeled on nuclear spins in solid-state materials
  - Easier to build than quantum computers
  - Can still be secure in a world with quantum computers



Credit: http://en.wikipedia.org/wiki/Nitrogen-vacancy_center

Related work

- "Nonlocality without entanglement" [Bennett et al, 1999]
  - There exist quantum operations that are "one-way" with respect to parties who are restricted to LOCC
- Quantum bit-commitment secure against k-local adversaries [Salvail, 1998]
  - Relies on interactive privacy amplification, won't work here
- Quantum bounded storage model [Damgaard et al, 2005]
- Quantum tokens [Pastawski et al, 2012]
- Password-based identification [Bouman et al, 2012]

This talk

- Overview
  - One-time memories, why they are useful
  - Isolated qubits model

- How to construct OTM's in the isolated qubits model
  - Leaky OTM's
  - Privacy amplification

How to construct OTM's

- Step 1: Leaky string-OTM's
  - Conjugate coding
  - Device stores two strings, leaks at most a constant fraction of the information

- Step 2: Deterministic privacy amplification
  - "Almost-perfect" single-bit OTM
  - Device stores two bits, leaks an exponentially small amount of information

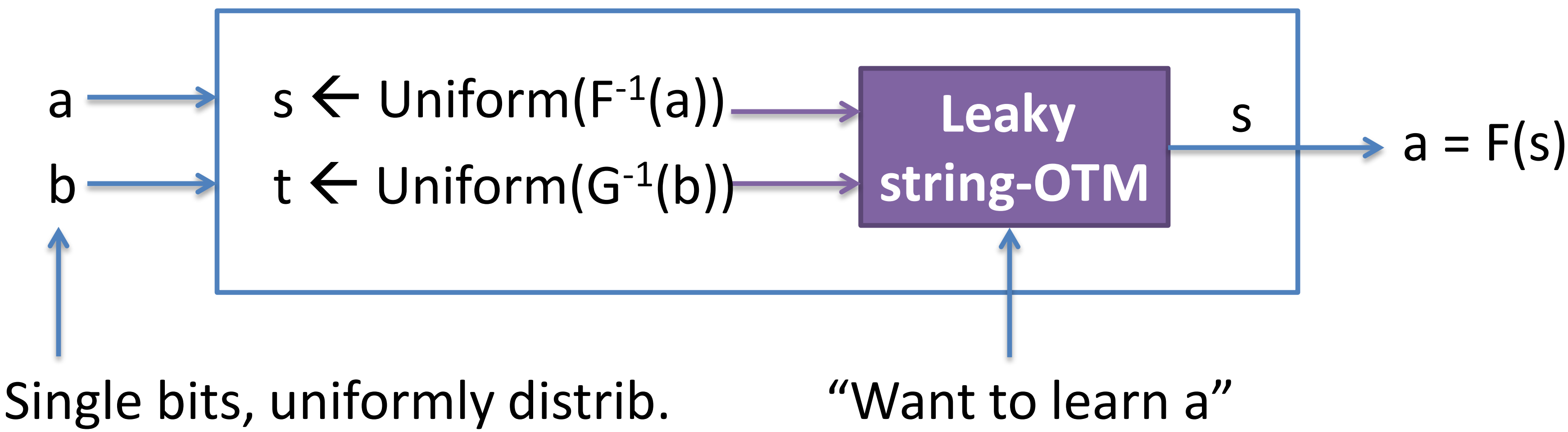
Assume we have a leaky string-OTM

- Device stores two messages S and T, each ℓ bits long
  - Assume they are uniformly distributed
  - Ideal security goal: adversary can learn either S or T, but not both

- A weaker ("leaky") notion of security:
- For any LOCC adversary, $H^{\varepsilon}_{\infty}(S,T|Z) \geq (0.5 - \delta)\,\ell$
  - Z is the adversary's output

Step 2: Deterministic privacy amplification

- Given a leaky string-OTM, construct an "almost-perfect" bit-OTM
  - Choose two (r-wise independent) random functions $F, G: \{0,1\}^{\ell} \rightarrow \{0,1\}$
    - Set ℓ, r to be polynomial in the security parameter k
    - Fix F and G permanently, as part of the construction



“Almost perfect” security

- With high probability over the choice of F and G, the following holds:
- For every LOCC adversary, there exists a binary random variable C, such that:
- $H^{\varepsilon}_{\infty}(A|C=0, Z) \geq 1 - 2^{-\Omega(k)}$
- $H^{\varepsilon}_{\infty}(B|C=1, Z) \geq 1 - 2^{-\Omega(k)}$
  - where Z is the adversary’s output, and $\varepsilon \leq 2^{-\Omega(k)}$
  - Note: adversary’s strategy may depend on F and G!
  - Random variable C comes from “entropy splitting” [Damgard et al]

Proof of security

- First, prove security wrt a single fixed meas. outcome
  - For any fixed measurement outcome M,
    with high probability over the random functions F and G,
    the scheme is secure
- Proof
  - Leaky string-OTM: $H^{\varepsilon}_{\infty}(S,T|M) \geq \Omega(k)$
  - Entropy splitting: ∃ random variable C, $H^{\varepsilon}_{\infty}(S|C=0, M) \geq \Omega(k)$
  - Want to bound: $\mathrm{bias}(A|C=0, M) = E_A((-1)^A|C=0, M)$
    $= \Sigma_s (-1)^{F(s)} \Pr(S=s|C=0, M)$
  - This is a sum of r-wise independent random variables $(-1)^{F(s)}$
  - Use Hoeffding-like large-deviation bound
  - Note $\Sigma_s \Pr(S=s|C=0, M)^2 = 2\text{^}[-H_2(S|C=0, M)] \leq 2^{-\Omega(k)}$

Proof of security

- Covering argument
  - Construct an ε-net for the set of all tensor product measurement outcomes
  - This has cardinality ≤ $2^{\text{poly}(k)}$ (singly, not doubly exponential, because adversary is restricted to LOCC measurements)

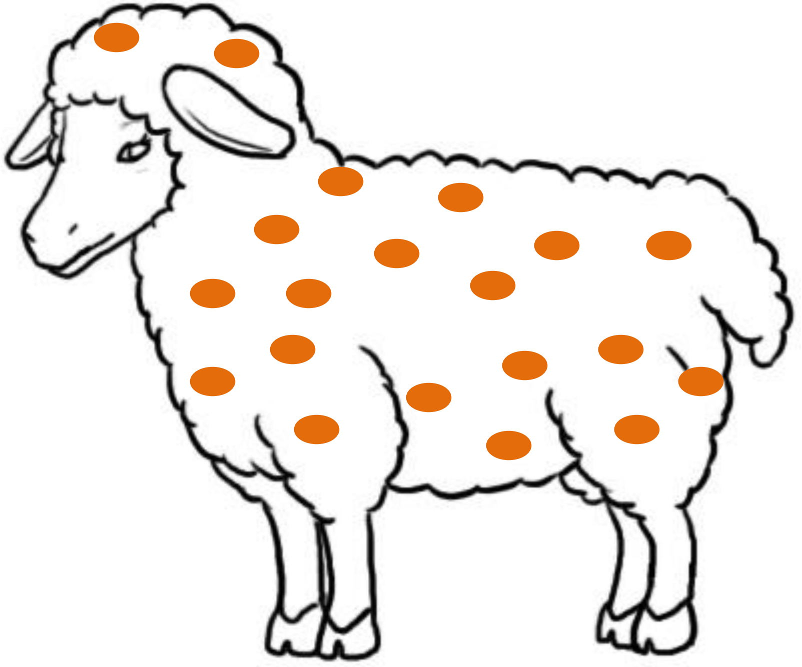
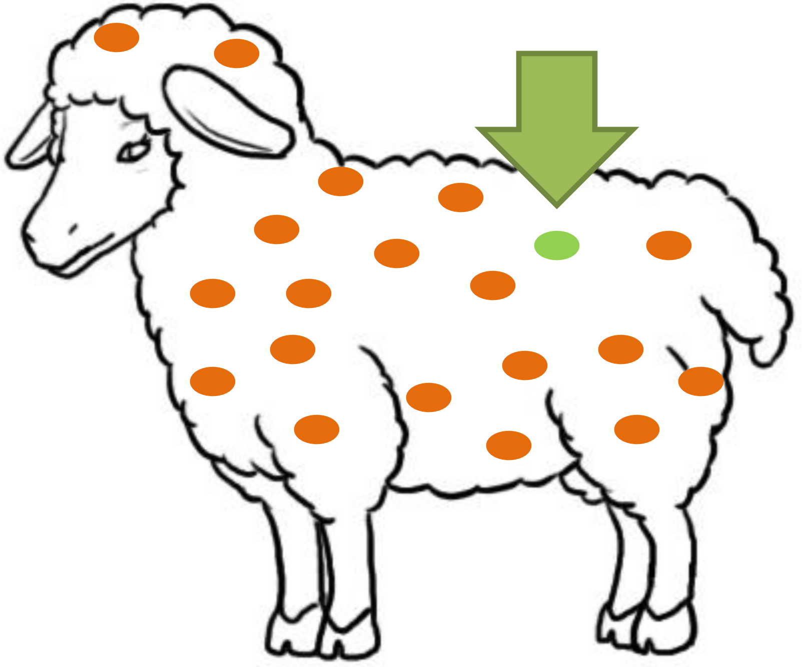


Image credit: http://www.wikihow.com/Draw-Sheep

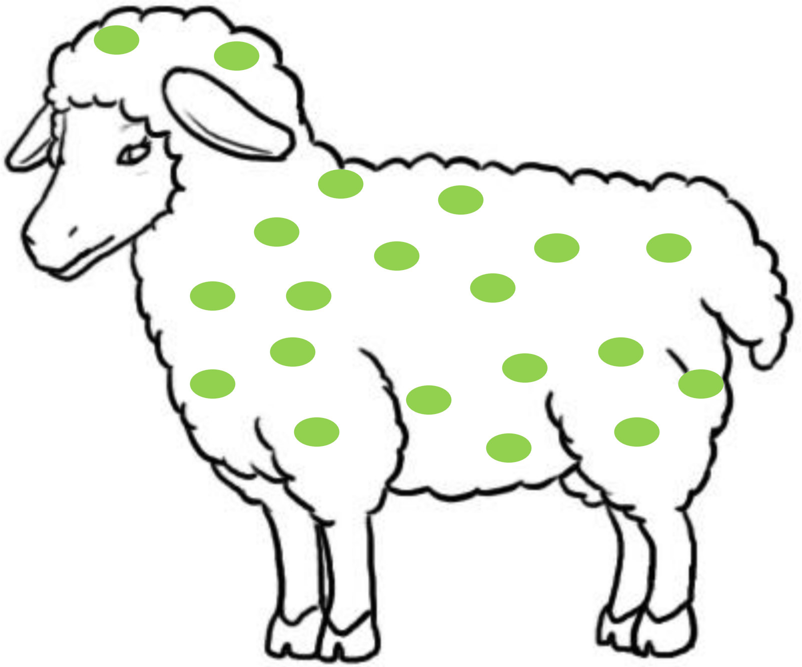
Proof of security

- Covering argument
  - Construct an ε-net for the set of all tensor product measurement outcomes
  - This has cardinality $\leq 2^{\mathrm{poly}(k)}$
- Prove security at one point in the ε-net
  - For any fixed measurement outcome M, with high probability over the random functions F and G, the scheme is secure
  - Failure probability is $\leq 2^{-\mathrm{poly}(k)}$



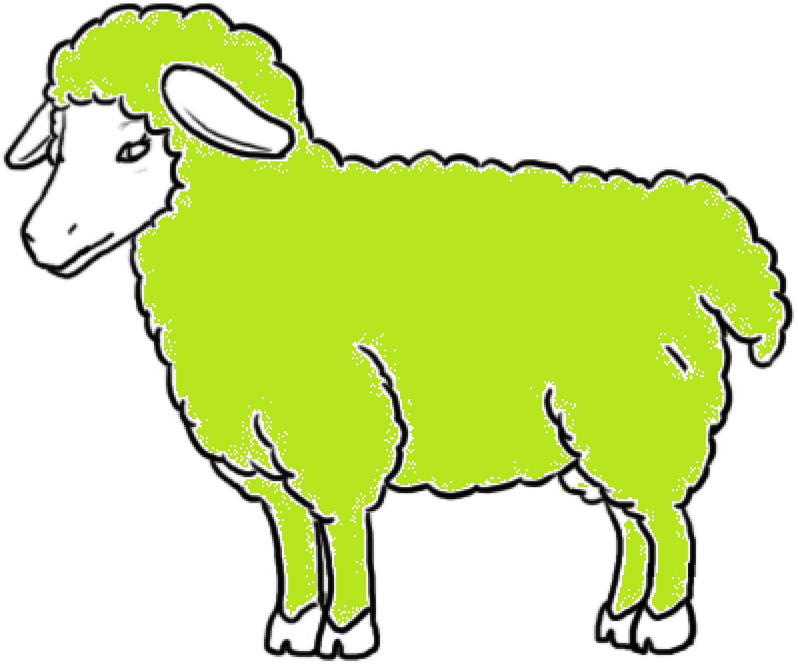
Proof of security

- Then use the union bound over all M in the ε-net
  - With high probability over F and G,
    for all M in the ε-net (simultaneously),
    the scheme is secure

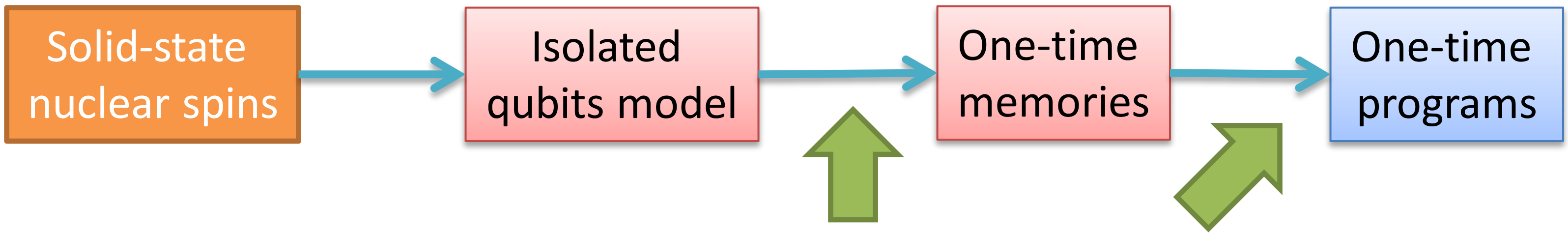


Proof of security

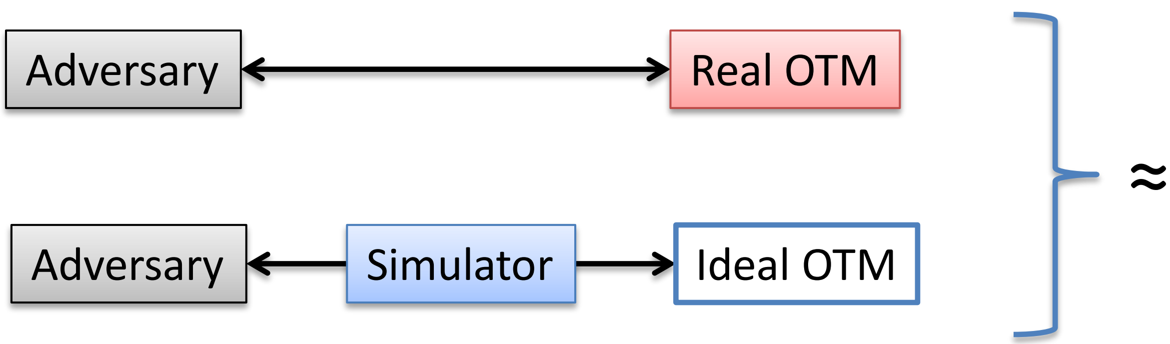
- Then use the union bound over all M in the ε-net
  - With high probability over F and G,
    for all M in the ε-net (simultaneously),
    the scheme is secure
- "Continuity argument"
  - Security does not change much
    when we perturb M
  - So for all tensor product M
    (simultaneously),
    the scheme is secure



Outlook



- Deterministic privacy amplification helps us to control information leakage
  - This helps to construct one-time programs…
  - Can our OTM's achieve composable security?

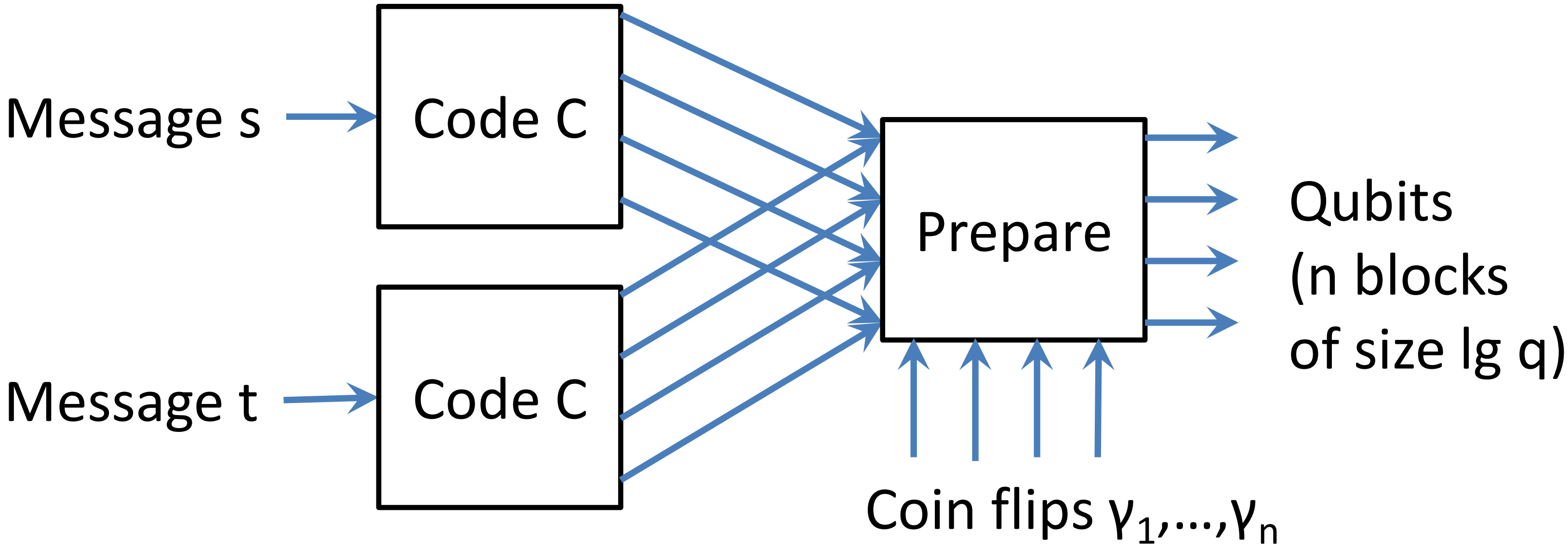


How to construct OTM's

- Step 1: Leaky string-OTM's
  - Conjugate coding
  - Device stores two strings, leaks at most a constant fraction of the information

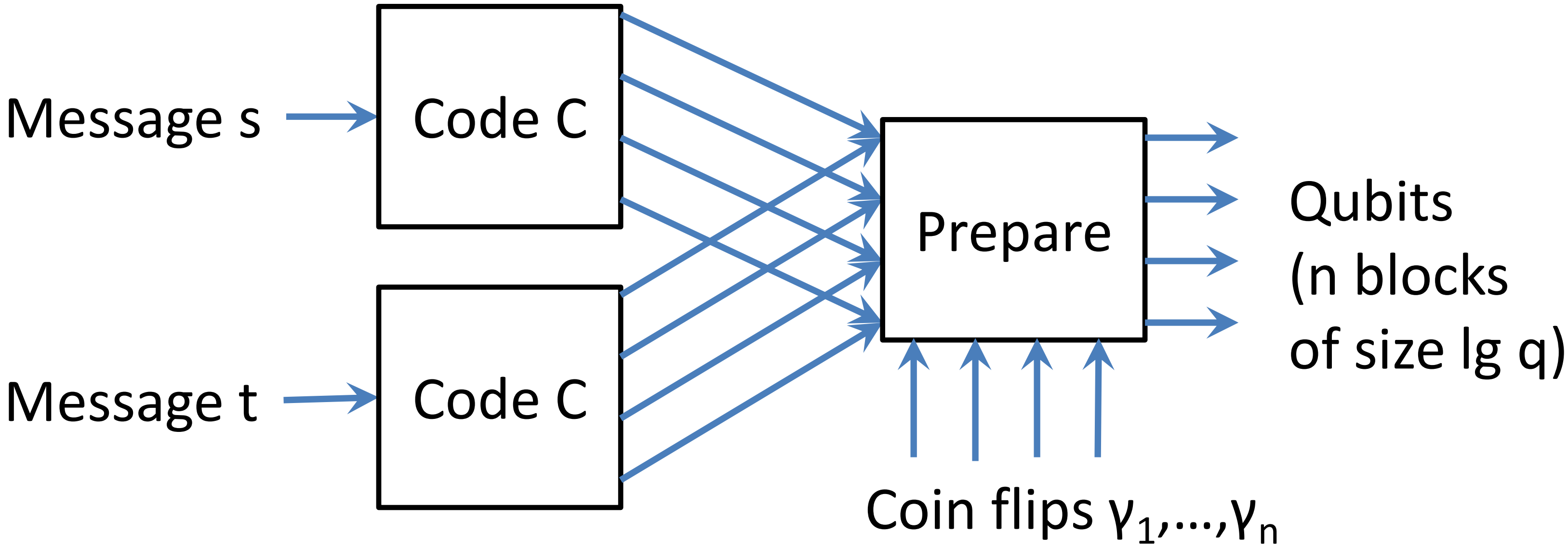
- Step 2: Deterministic privacy amplification
  - "Almost-perfect" single-bit OTM
  - Device stores two bits, leaks an exponentially small amount of information

Step 1: Leaky string-OTM's



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

Step 1: Leaky string-OTM's

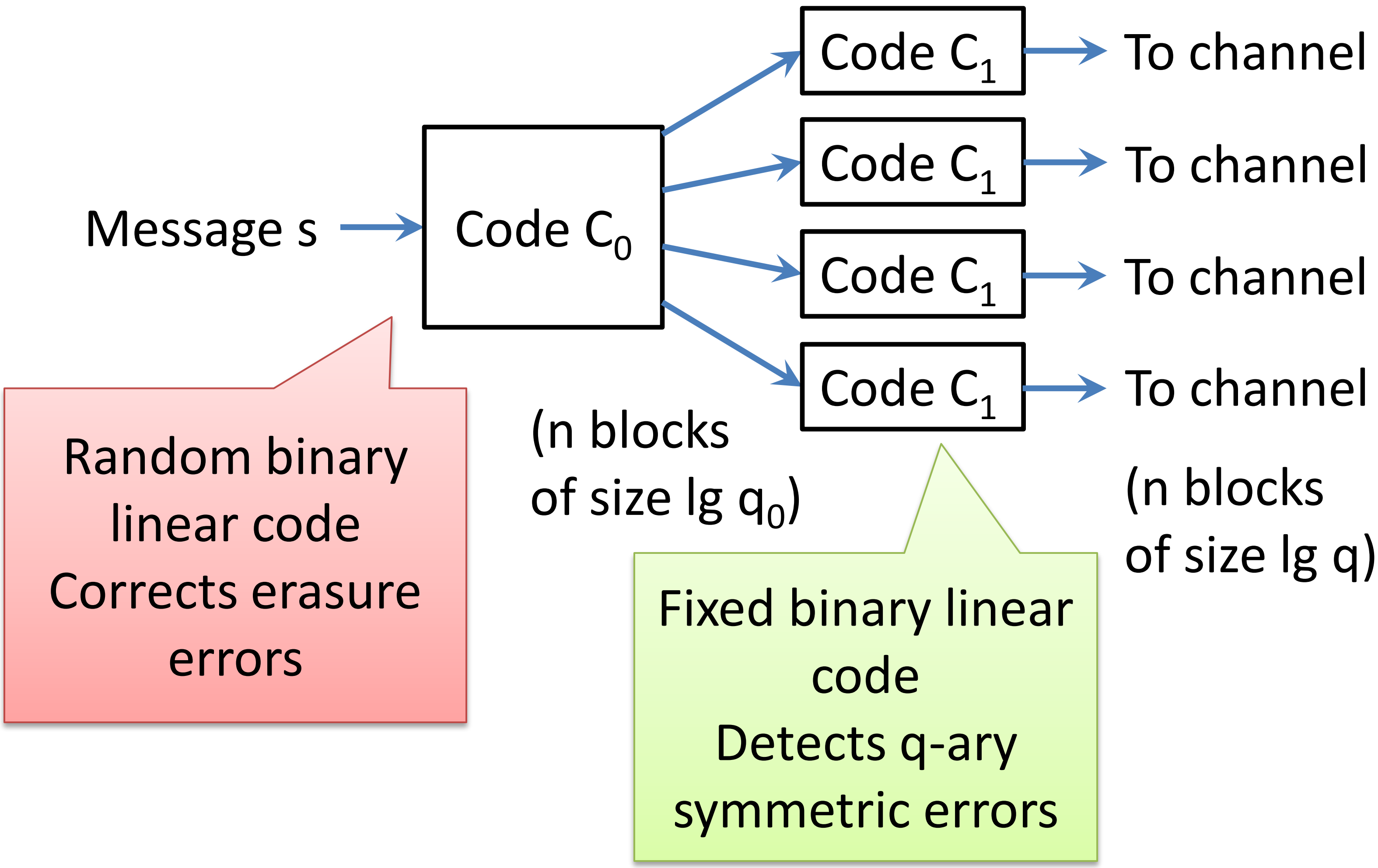


- To read s: measure qubits in standard basis
- To read t: measure qubits in Hadamard basis
- This is equivalent to receiving C(s) or C(t) through a q-ary symmetric channel

Choosing the code C

- To ensure security:
  - C should approach the capacity of the q-ary symmetric channel
  - C should be "unstructured"
    - One way to formalize this: let C be linear over GF(2)
    - Generator matrix has full rank
    - Suppose message S is uniformly distributed
    - Then codeword C(S) will have a large subset of bits that are uniformly distributed
  - Also, C should be efficiently decodeable

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)

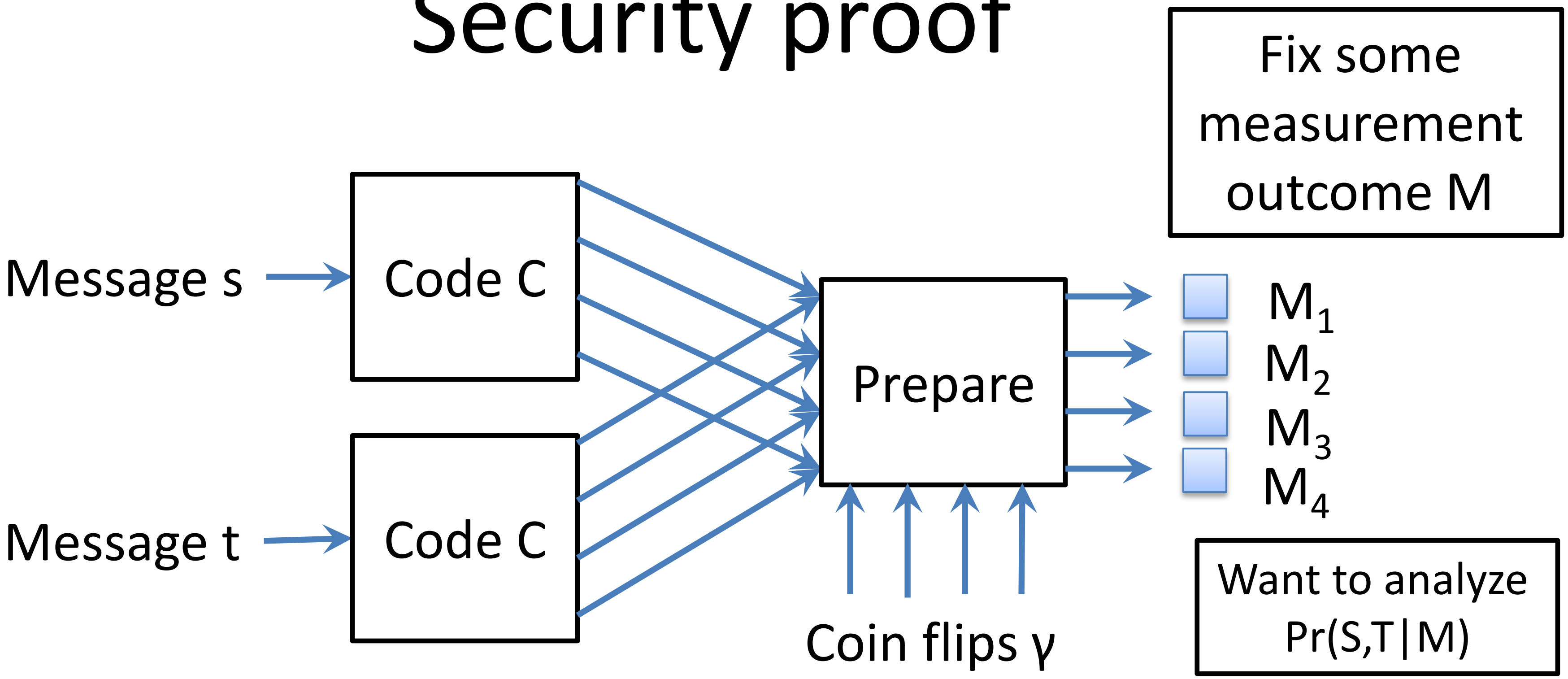
- Other constructions:
  – Interleaved Reed-Solomon codes, interleaved AG codes [Bleichenbacher et al; Shokrollahi; Brown et al]

Security proof

- Prove security against separable adversaries
  - Every POVM element is a tensor product of 1-qubit operators
  - Separable adversaries include LOCC as a special case
  - LOCC can be complicated: e.g., adaptive sequences of weak measurements

Given a separable adversary A

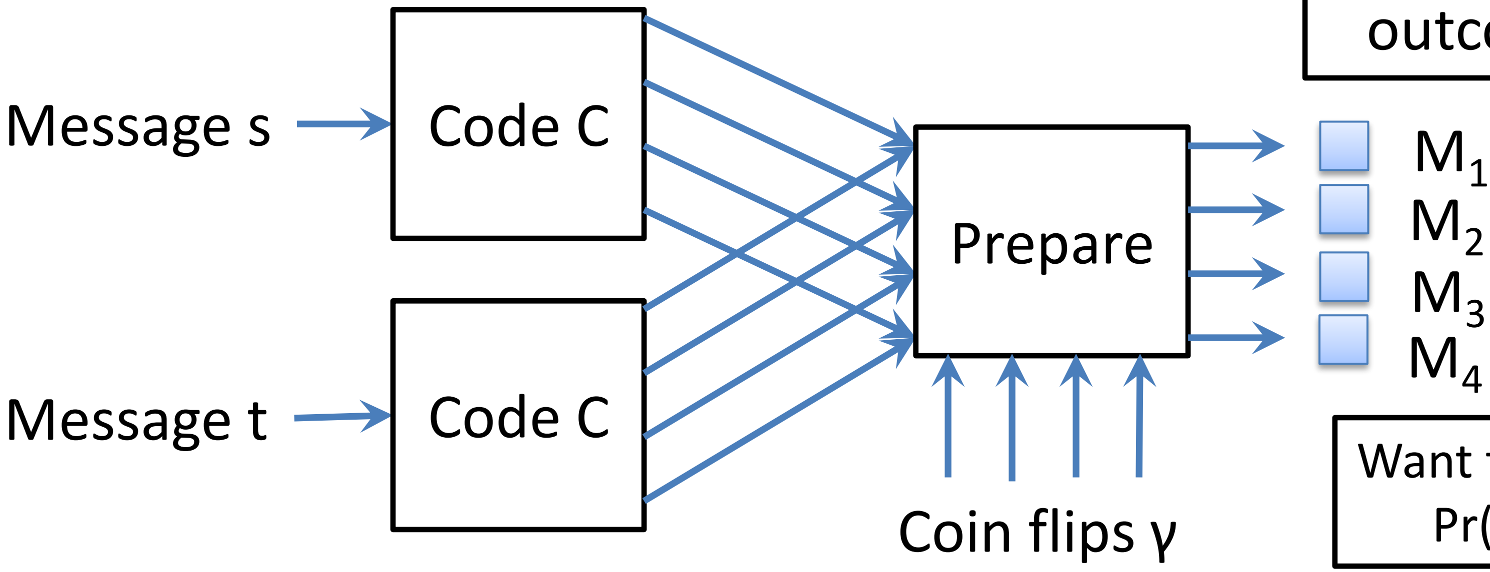
Security proof



Given a separable adversary A

Security proof

Fix some measurement outcome M

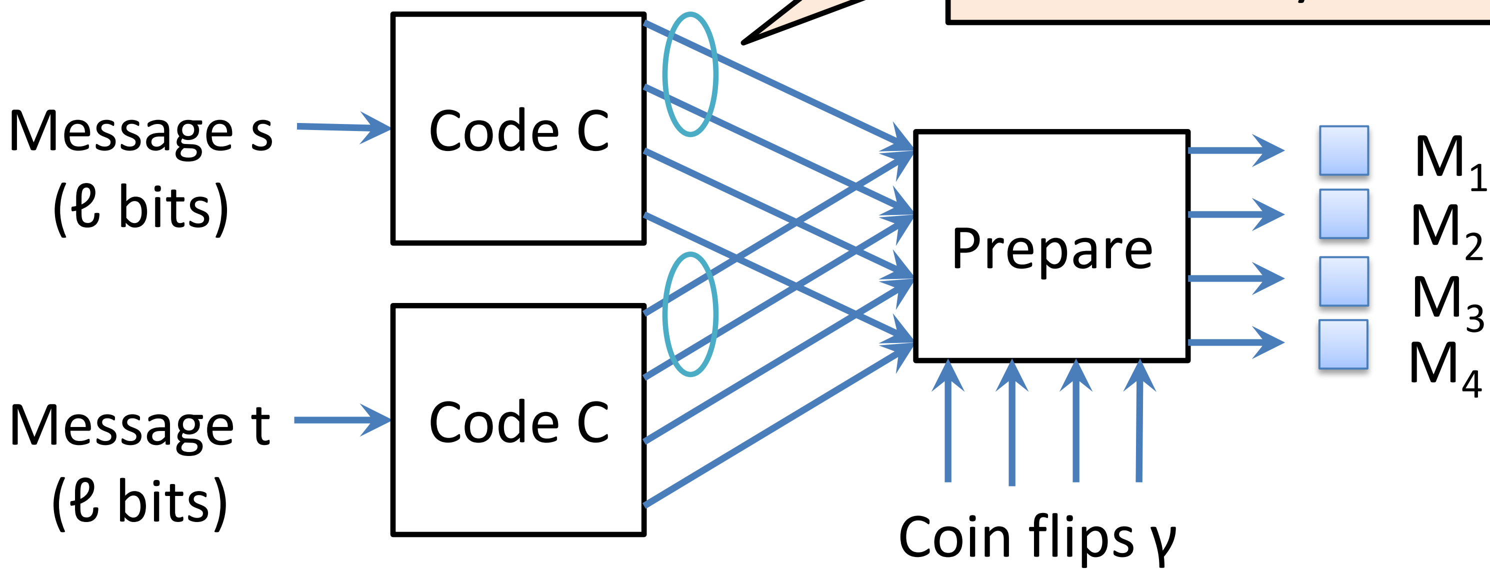


Want to analyze Pr(S,T|M)

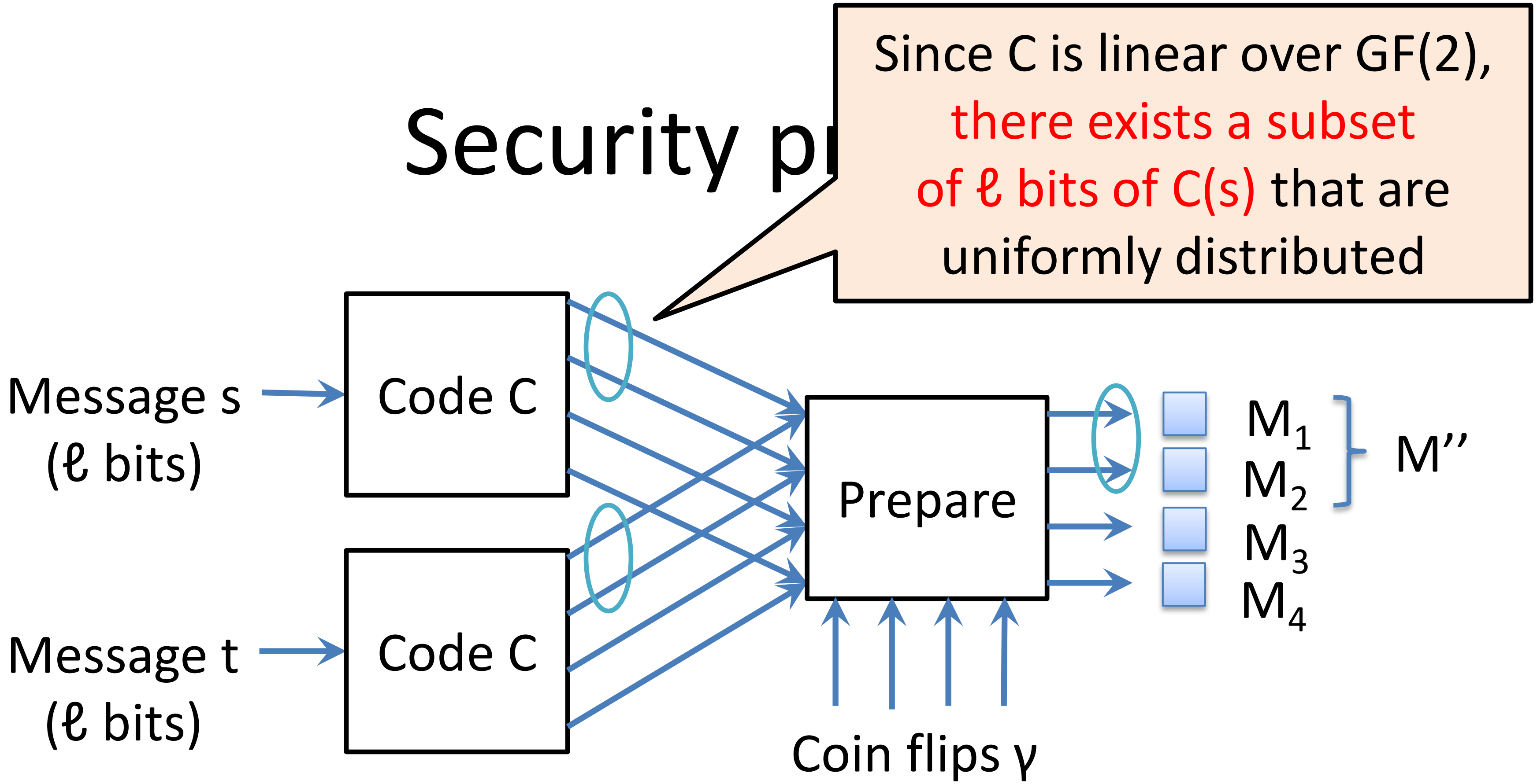
- Consider a fictitious adversary A' that measures each qubit once, such that M_1,M_2,M_3,… are possible outcomes
- Call this event M'
- Then Pr(S,T|M) = Pr(S,T|M')

Security pr

Since C is linear over GF(2), there exists a subset of ℓ bits of C(s) that are uniformly distributed

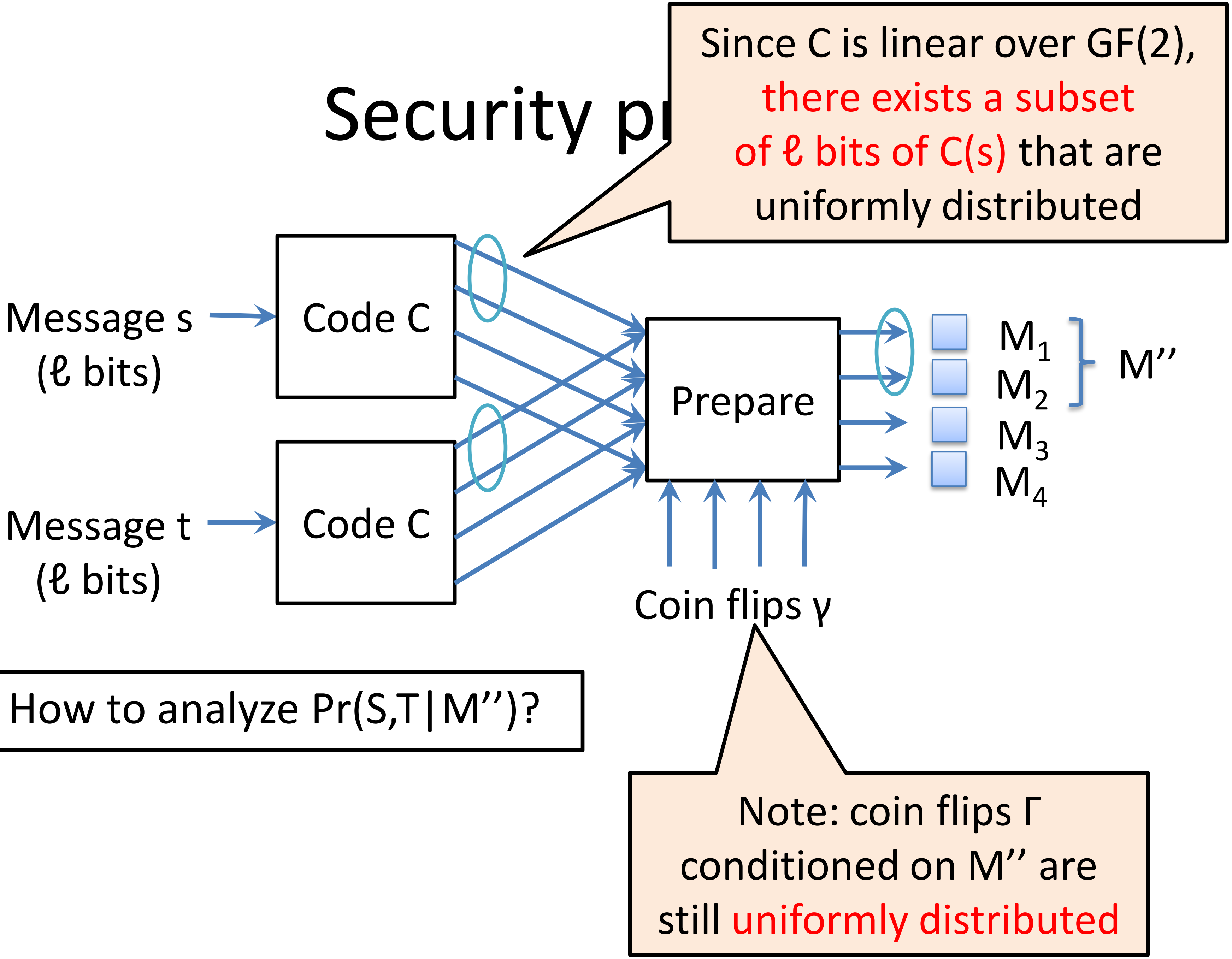


Security pr



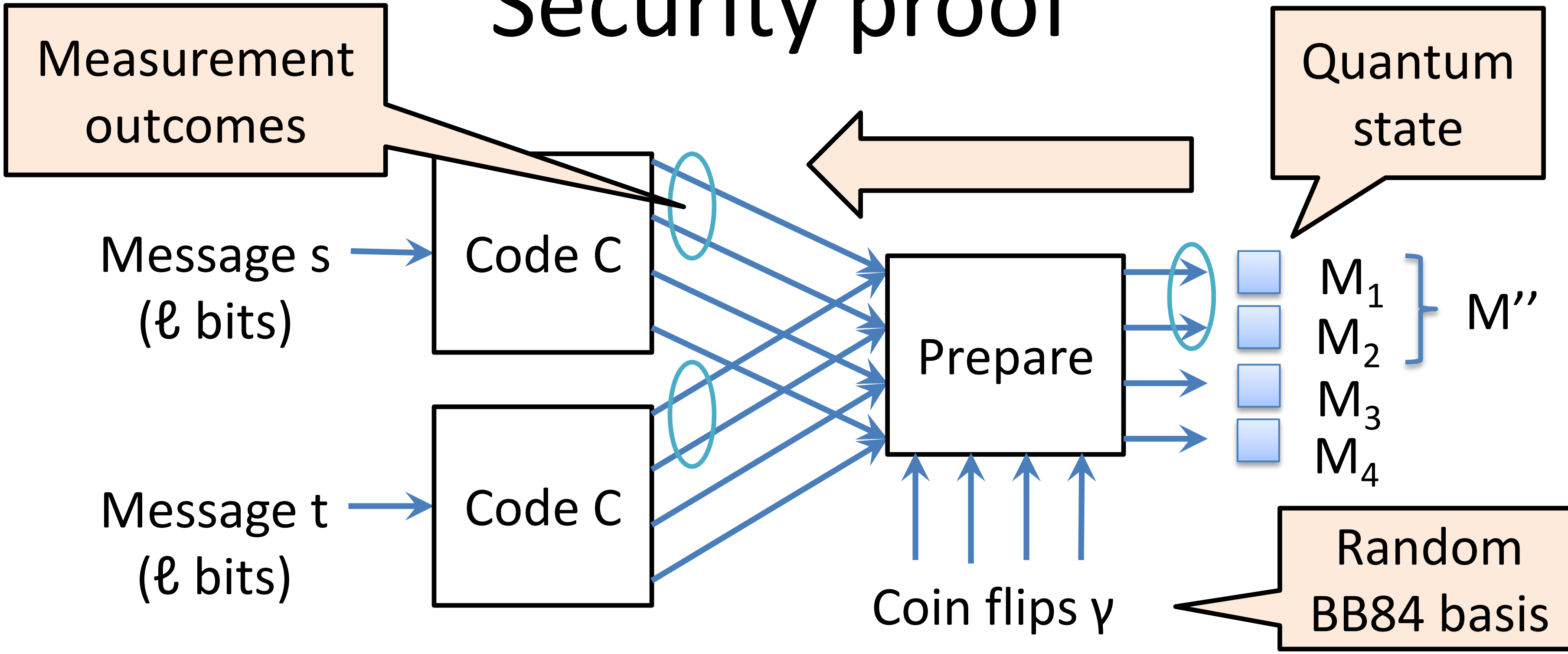
- Wlog, suppose the fictitious adversary A’ measures this subset of qubits first
- When A’ observes M_i for all i in this subset, call this event M’’
- Want to analyze Pr(S,T|M’’)

Security pr



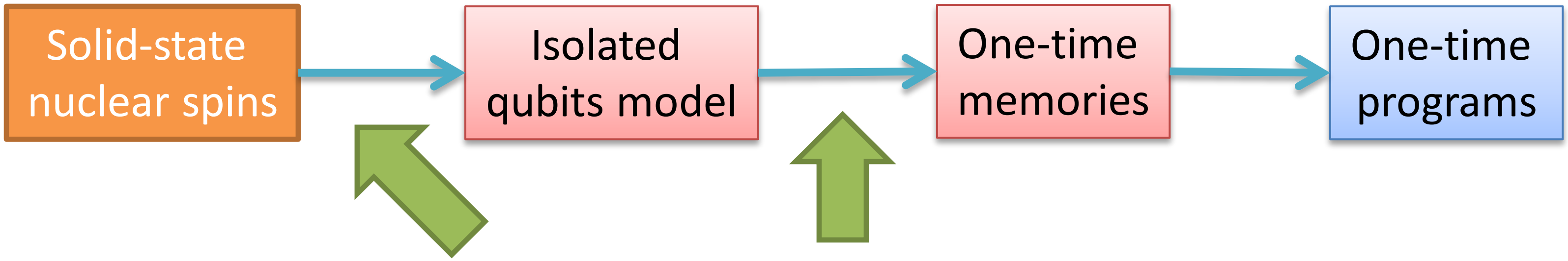
- How to analyze Pr(S,T|M'')?

Security proof



- Now run the experiment backwards…
  - Measuring a quantum state using a sequence of random BB84 bases
- Use an entropic uncertainty relation to lower-bound $H^{\varepsilon}_{\infty}(S,T|M'')$
  - Borrowed from the bounded quantum storage model [Damgard et al, 2006]

Outlook



- We have showed how to construct OTM's based on isolated qubits
  - Instead of isolated qubits, can we use more realistic models of the underlying hardware?
  - Noisy entangling operations?
  - Shallow quantum circuits?

Isolated qubits are fun

- For theorists:
  - Another model, where many interesting cryptographic tasks are possible!
    - Known constructions seem very far from optimal!
    - Based on simple probabilistic constructions, crude bounds
- For experimentalists:
  - Another family of interesting quantum devices that can be realized
    - Very different from quantum repeaters
    - Want long coherence times, good single qubit operations, <u>no</u> entanglement swapping

Isolated qubits are fun

- For theorists:
  - Another model, where many interesting cryptographic tasks are possible!
    - Known constructions seem very far from optimal!
    - Based on simple probabilistic constructions, crude bounds
- For experimentalists:
  - Another family of interesting quantum devices that can be realized
    - Very different from quantum repeaters
    - Want long coherence times, good single qubit operations, no entanglement swapping

Thank you!