Building one-time memories from isolated qubits

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

Cryptography in a quantum world

- Bit commitment, oblivious transfer =>
  secure 2-party computation

- Alas, BC and OT are impossible in a quantum world
  (if one wants unconditional security)

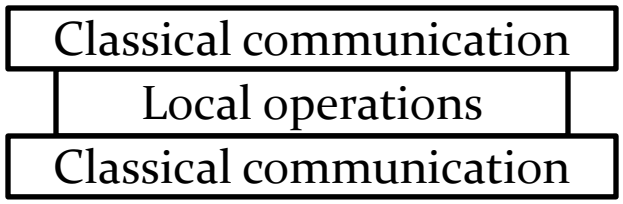
- Salvail '98: quantum bit-commitment is possible,
  if one assumes the adversary is k-local

This talk

- Revisit these ideas, in a different context: tamper-resistant cryptographic hardware
- "Isolated qubits"
  - Only allow local operations & classical communication (LOCC)
- "One-time memories" (OTM's)
  - Like oblivious transfer, but non-interactive
- Use OTM's to build "one-time programs"
  - Computational black boxes (Goldwasser et al, 2008)

“Isolated qubits”

- Have n qubits
- Can only be accessed using n-partite LOCC operations



- Intuition: conflicting requirements for a quantum memory
  - (1) isolation from environment
  - (2) coherent interaction with an external probe
- Isolated qubits: achieve (1) and frustrate (2)
  - Concrete example: NV centers?

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

“Isolated qubits”

- Have n qubits
- Can only be accessed using n-partite LOCC operations

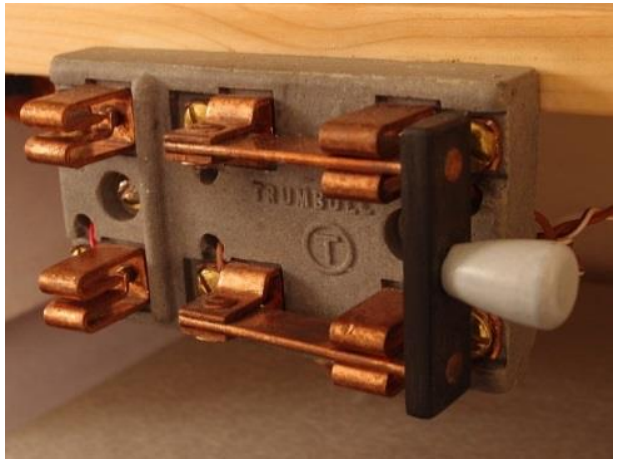
Classical communication
Local operations
Classical communication

Isolated qubits can exist in a world with quantum computers!

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

One-time memories (OTM's)

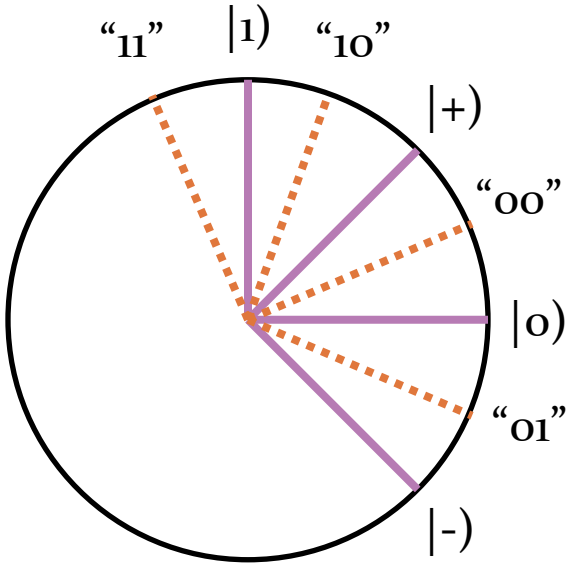
- An OTM contains two messages, s and t
  - Alice programs the OTM with (s,t), then gives it to Bob
  - Bob can choose to read either s or t, but not both
  - No other interaction between Alice and Bob
  - At least as powerful as oblivious transfer



Junkyardsparkle on Wikipedia
http://en.wikipedia.org/wiki/File:DPDT_knife_switch_in_closed_position.jpg

Building an OTM

- "Conjugate coding" (Wiesner, 1970's)
  - Given two k-bit messages s, t
  - Choose two error-correcting codes C, D
  - Get two n-bit codewords C(s), D(t)
  - For each qubit i = 1,2,…,n, prepare a state that…
    - Returns information about $C(s)_i$ when measured in the |0),|1) basis
    - Returns information about $D(t)_i$ when measured in the |+),|-) basis



Building an OTM

- This is not secure against general quantum adversaries
  - There exists a joint measurement on all the qubits that recovers both messages simultaneously
  - "Run the classical decoding algorithm on a superposition of inputs"
- But it may be secure in the isolated qubits model…
  - Honest strategies require only LOCC operations
  - Cheating strategy requires entangling gates?
  - Caveat: adversary may be able to obtain partial information about both messages

A weaker definition of security

- Assume messages S,T are uniformly distributed
- For any LOCC adversary that receives the OTM and outputs classical information Z,
  - Require $H^{\varepsilon}_{\infty}(S,T|Z) \geq (1-\delta)k$
  - Adversary is allowed to learn partial information about both S and T

- Call these "weak OTM's"
  - Does our contruction yield weak OTM's? (Maybe)
  - Are weak OTM's sufficient to construct one-time programs? (Probably)

One-time programs

- A one-time program is a set of software and hardware that lets you run a program once
  - Alice chooses a circuit C, prepares an OTP, and gives it to Bob
  - Bob chooses an input x, runs the OTP, and obtains the output C(x)
  - OTP cannot be run again
  - Internal state of OTP is hidden

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

One-time programs

- One-time programs can be built using OTM's together with Yao's garbled circuits (Goldwasser et al, 2008)

- Conjecture: weak OTM's are good enough for this purpose
  - OTM's contain secret keys, which are chosen uniformly at random
  - Use leak-resistant encryption (Akavia et al 2006) =>
    it's ok if the OTM's leak some information

  - Open problem: prove this rigorously?

Security of our OTM's

- Choose random error-correcting codes C, D
- Consider all one-pass LOCC adversaries
  - that use 2-outcome measurements
  - and output classical info Z

- Theorem: w/ high prob. (over C, D), for all such adversaries,
  - $I(Z; S,T) \leq (1.9190)k + O(\sqrt{n} \log n)$
  - Equivalently, $H(S,T|Z) \geq (0.081)k - O(\sqrt{n} \log n)$

  - Caveat: C, D are not efficiently decodable!
  - Caveat: H is Shannon entropy, not (smoothed) min-entropy!

Security of our OTM's

- Some issues to consider…
- Adversary knows everything at the beginning of the game
  - Contrast with QKD: honest parties keep some information secret, use it to do privacy amplification later
- Choice of C and D is crucial
  - Want them to be "unstructured" => choose them at random
- General LOCC adversaries are hard to analyze
  - Can make a long sequence of weak measurements
  - We only consider 1-pass LOCC adversaries

Proof techniques

- Step 1: for the first k steps of the adversary,
  - Consider all separable measurement outcomes M_A
  - Lower-bound the collision entropy $H_2(S,T|M_A)$
    - Use large-deviation bounds for locally dependent rv's
    - Union bound over all M_A
- Step 2: for the next k steps of the adversary,
  - Consider all decision trees representing the adversary
  - Upper-bound $I(Z_{k+1\ldots 2k}; S,T \mid M_A)$
    - Use Dudley's inequality for empirical processes
    - Prove that "similar" decision trees produce "similar" results
    - Cover the set of decision trees with ε-nets at varying resolution

Related work

- Quantum bit-commitment secure against k-local adversaries (Salvail '98)
- Bounded / noisy storage model (Damgaard et al, Wehner et al)
- Data-hiding states (DiVincenzo et al, …)

- Unforgeable quantum tokens (Pastawski et al) – today
- Quantum networks using NV centers (Childress) – Thursday
- Quantum one-time programs (Broadbent et al) – Friday

Outlook

- This talk
  - Isolated qubits model
  - One-time memories based on conjugate coding (our main result)
  - One-time programs based on Yao's garbled circuits (Goldwasser et al, 2008)
- Can we prove a stronger security guarantee for our OTM's?
  - Get tighter bounds?
  - Use efficiently-decodable codes?
  - Prove security against general LOCC adversaries?
  - Prove composable security (using the (smoothed) min-entropy)?