Automated Search for Quantum Secret Sharing Protocols with Graph States

Dr Nick Papanikolaou
Research Fellow
International Digital Laboratory
http://go.warwick.ac.uk/nikos

QNET Workshop 2009
11 December 2009

Outline

Secret Sharing Protocols: Objective

Quantum Secret Sharing Schemes: Characteristics

General Protocol Structure – Encoding secrets on graph states

Doing an Automated Search (work in progress)

Using Model Checking

Extensions, Future Work, Open Questions

Secret Sharing: Objective

Secret sharing protocols allow a (quantum or classical) secret (string) to be shared between n parties so that up to n of these parties need to collaborate to obtain the secret.

Example: The president of a bank wishes to give access to a vault to three vice presidents who are not entirely trusted.

Instead of giving the combination to any one individual, he distributes the information so that two vice presidents are needed to jointly determine the combination.

In a (k,n)-threshold scheme, any set of k-1 or fewer shares contains no information about the secret.

Quantum Secret Sharing

A quantum (k,n) threshold scheme, with k≤n, is a method to encode and divide an arbitrary secret quantum state into n shares with the following two properties:

From k or more shares the secret state can be reconstructed.

From k-1 or less shares, no information at all can be deduced about the quantum state.

[R. Cleve, D. Gottesman, and H-K. Lo, *How to Share a Quantum Secret*, PRL 83(3), 1999]

(contains existence proofs and general properties)

[D. Markham, B.C. Sanders, *Graph States for Quantum Secret Sharing*, arXiv:0808.1532 [quant-ph]]

(generalisation to cover classical and quantum bits, while using graph states for encoding)

Quantum Secret Sharing: Characteristics

Three different classes of protocol:

CC: Classical secret sharing with private channels between the dealer and each player and private classical channels shared between each set of players.

CQ: Classical secret sharing with public channels between the dealer and each player and either quantum or classical channels shared between each pair of players

QQ: Quantum secret sharing wherein the dealer shares quantum channels with each player, and these channels can be private or public, and the players share either quantum or classical private channels between each other.

We are interested here in **CC** case.

In general a protocol will involve a dealer and a set of players. The dealer distributes the secret to the players in a determined manner, and the players can collude to obtain the secret.

Key point: If the secret is distributed across the joint quantum state of the players, the players then perform LOCC to obtain the secret.

General Protocol Structure (CC case)

Secret is a binary string $S = \{s_i\}$.

The dealer distributes the secret to players 1..n

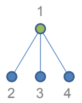
- Initial state is prepared by the dealer and is a graph state such that each qubit belongs to one of the players
- Each bit of secret corresponds to either an identity or Z operation on the ith qubit:
  - If s_i=1 dealer applies Z operation on qubit i

Of the n players, k players will measure and share their results. The results will be combined using a specified boolean operation (XOR) to produce the secret.

- Specified player j measures using X operator, obtaining c_j
- Other players measure using Z operator, obtaining $\{c_k, k\neq j\}$
- The secret is reconstructed by applying a boolean function $f:\{0,1\}^n \rightarrow \{0,1\}$ (actually XOR in Markham/Sanders)

(k=4,n=4) Protocol

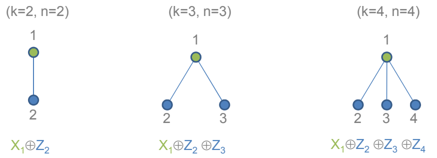
1. Dealer prepares the graph state:

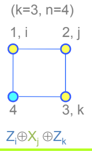


(start with |++++⟩, then apply $CZ_{1,2}$; $CZ_{1,3}$; $CZ_{1,4}$)

2. Secret bit is S. Dealer encodes S onto state 1 (if S=1, applies Z ⊗ I⊗ I⊗ I, ...)
3. Dealer sends qubit 1 → player 1, etc
4. Player 1 measures in X-basis; others in Z-basis
5. Classical communication between all players
6. Exclusive OR of all results.

Other Possibilities


(k=2, n=2)
1
2
$X_1 \oplus Z_2$
(k=3, n=3)
1
2
3
$X_1 \oplus Z_2 \oplus Z_3$
(k=4, n=4)
1
2
3
4
$X_1 \oplus Z_2 \oplus Z_3 \oplus Z_4$



- Different arrangements are possible
- Exclusive or of outcomes is denoted by ⊕

Doing an Automated Search

Key questions:

- For given n, how many protocols are there?
- Why do some values of (n,k) magically yield valid secret sharing protocols and not others?
- Is there a pattern?

Our approach is to program an explicit computational search for valid protocols.

The idea is to try:

- All possible graph states (viz. Network arrangements/configurations)
- All possible ways of encoding the secret on a graph state
- All possible ways of measuring the players' local states
- All possible boolean functions that combine the players' measurement outcomes

Doing an Automated Search: Feasibility/Efficiency

An obvious concern is the efficiencyandscalability of the search.

Note that we are working within the graph state formalism – through the reduction to stabilizer states, we are within the reach of the Gottesman-Knill theorem

- Hence efficient simulation of candidate protocols is possible!
  - (and we have a working implementation as part of the Quantum Model Checker QMC which includes an efficient simulation library – see http://go.warwick.ac.uk/nikos/)

Doing an Automated Search: Success Criteria

We have seen the general structure and characteristics of QSS (CC) protocols.

Given a QSS protocol, what is the main criterion for correctness?

- It should work for all secrets S of length N (input)

What is the output of the search?

- The values of k and N
- A list of encoding operators, one for each qubit/player (typically Z or I, but why not X or Y?)
- A list of measurement operators, one for each qubit/player
- A measurement combinator – a boolean function for combining the measurement results

Doing an Automated Search: Implementation

With Simon Gay, we are working on an implementation of a search algorithm for secret sharing protocols.

As mentioned before, the motivation here is to use a

Generate-and-test approach

Such an approach is naïve and greedy and makes use of the computing power of current hardware, and is intended to provide us with insights into the structure of quantum secret sharing and why it works.*

We intend to see whether there are values of (k,n) exist for which no protocols exist – and why.

Essentially a combinatorial problem!

* One could alternatively examine the mathematical formalism and graph structure to prove why certain values do or don't work ☺

Work in Progress

This is work in progress.

We have a Java implementation of part of the search algorithm.

We are considering links to related work

- Kashefi et al.
- Perdrix et al.

The measurement combinator may just be XOR in all cases, so trying other possibilities could be unnecessary

We will want to consider the overall performance of the search – and compare alternative approaches also, such as using combinations of existing tools etc.

- Interesting: GraphSim? Efficient simulation of graph states

What about model checking?

Model checking is a technique that is designed to solve this type of problem by design!!

A model checking approach would involve taking:

- A specification of the protocol structure/steps
- A specification of (the inverse of) the correctness criterion as a property
- … and supplying these to a tool that automatically does state space exploration and founds property violations (counterexamples)

This is the basis of our previous work, and we have a tool (QMC) that is designed for such analyses…

… however it is nontrivial to specify secret sharing protocols in the current implementations

- mostly due to the absence of general boolean operators

Future work

Completing the simulation algorithm and doing searches for large numbers of qubits

- Current known protocols are for 4 qubits or less

Extending QMC with syntactic features that will enable compact descriptions of protocol specifications

- Note that model checking is not intended for searching for protocols in general;
  - This is the task of protocol synthesis
- What we are proposing is a novel use for model checking in this sense

See work on quantum model checking

N. Papanikolaou, 'Model Checking Quantum Protocols', Ph.D. Thesis, Department of Computer Science, University of Warwick, 2008/9.

Simon Gay, Rajagopal Nagarajan and Nikolaos Papanikolaou, 'QMC: A Model Checker for Quantum Systems', Proceedings of 20th International Conference on Automated Verification (CAV 2008), Princeton, NJ, USA, July 7-14, 2008, Lecture Notes in Computer Science, vol. 5123, Springer.

Simon Gay, Rajagopal Nagarajan, Nikolaos Papanikolaou, 'Probabilistic Model-Checking of Quantum Protocols', Proceedings of 2nd International Workshop on Developments on Computational Models (DCM 2006).

Nick Papanikolaou, 'Reasoning Formally About Quantum Systems: An Overview', ACM SIGACT News, 36(3), pp. 51-66, 2005.

Rajagopal Nagarajan, Nikolaos Papanikolaou, Garry Bowen, Simon Gay, 'An Automated Analysis of the Security of Quantum Key Distribution', Proceedings of the Third International Workshop on Security Issues in Concurrency (SECCO'05), August 22, 2005, San Francisco, USA.

Online…

NP:

http://go.warwick.ac.uk/nikos

Simon Gay:

http://www.dcs.gla.ac.uk/~simon

QMC – available from NP's page incl. examples.

Questions?