Quantum Secret Sharing with Grover's Algorithm

Dylan Liu
Stanford University

Abstract

Quantum secret sharing addresses the same problem that classical secret sharing does, but via quantum means. That is, Alice wishes to send a secret to n agents, and any $k \leq n$ agents can collaborate to recover the secret. However, for any fewer than k agents, collaboration will information-theoretically reveal no information about the secret. Such protocols are called (k,n)-threshold schemes, and we focus on $(2,2)$-threshold quantum schemes in this paper. One technique used in quantum secret sharing is Grover's algorithm, which solves the unstructured search problem in sub-linear time. This can be utilized by preparing a superposition of two-qubit basis states, then flipping the phase of one of the components. Each agent receives one qubit, and when they collaborate, they can search for the phase error, thus reconstructing Alice's secret. Hsu's protocol outlines a $(2,2)$-threshold scheme, which has been generalized to a (n,n)-threshold scheme for arbitrary n. Tseng's protocol outlines a similar scheme, but one that doesn't require that the agents have quantum memory, and it also allows the agents to collaborate using shadows in classical bits. However, more powerful protocols require much more sophistication than Grover's algorithm, and even with the additional sophistication, none to date have been proven to be unconditionally secure against dishonest agents.

1 Introduction

Grover's algorithm was formulated in 1996 as an optimal quantum algorithm for an unstructured search problem, capable of solving a search problem over a set of n elements in $O(\sqrt{n})$ queries, thereby exhibiting a quadratic speedup over classical algorithms.[1][2] An immediate corollary of this is that brute force attacks against symmetric-key encryption schemes like the Advanced Encryption Standard (AES) can be done in $O(2^{n/2})$ time, where n is the key size, thus requiring the doubling of the key size to achieve the same security parameter. However, Grover's algorithm has much more significant implications for cryptography. Namely, various secure quantum secret sharing schemes can be constructed from it.

Quantum secret sharing addresses the problem in which Alice wishes to relay a secret message to two distant agents, Bob and Charlie, but at most one of the two agents may be dishonest. If the two agents work together, then the honest one will be able to prevent the dishonest one from sabotage. Therefore, she cannot entrust either agent individually with the entire message, but rather she encrypts her secret in two shadows, neither of which individually reveal any information about the secret. Only when the agents combine their shadows can they learn Alice's message. Such schemes need to satisfy the classical definition of secure secret sharing in that neither shadow individually can information-theoretically reveal any information about the secret. However, in the quantum setting, the protocol also needs to ensure that the shadows are securely transmitted, namely it needs to be secure against various eavesdropping techniques and other forms of cheating.

A two-qubit secret sharing protocol was developed by Hsu in 2003.[3] In this protocol, Alice randomly prepares a two-qubit initial state, then changes the phase of the component of the initial state corresponding to the marked state that Alice wishes to share. Alice sends one of the qubits to each of Bob and Charlie, who then confirm via classical channels that they have received the qubits. Alice publicly announces her initial state, then Bob and Charlie combine their qubits to recover the marked state. To do so, Grover's algorithm is used to search for component of the initial state that has undergone a phase change.

This result was generalized in 2007 by Bhandari and Chamoli into an n-qubit secret sharing scheme.[4] The initial state is composed of n qubits, over a $N = 2^n$ dimensional Hilbert space. The secret is encoded in $\frac{N}{4}$ of these basis states, which constitute the marked states. Half of the marked states contain the encryption of the first half of the message, and the other half of the marked states contain the encryption of the second half of the message. Alice applies a phase shift to the initial state, then sends the n qubits to the agents. When the agents collaborate, they will measure one of the marked states, so Alice needs to repeat this process several times to communicate all of the marked states.

A security flaw in Hsu's protocol was discovered in 2010 by Hao, et al that permits a dense-coding attack to recover the key information without detection.[5] Hao proposed an amendment to Hsu's protocol whereby instead of publicly broadcasting her initial state, Alice can instead require that the agents measure their qubits in a randomly chosen basis, and she can then verify that the results are consistent with her prepared initial state.

This protocol was further modified in 2011 by Tseng, et al such that no quantum memory is required by the agents, and the agents can recover the secret using shadows in classical bits, without a need for combining their shadows in photons.[6] This proceeds by using a more general initial state for Grover's algorithm. Let $|S\rangle$ be the initial state, $|\omega\rangle$ be the marked state, and $|\omega'\rangle$ be the measurement result. Then under this new initial state, the measurement result satisfies $|\omega'\rangle = |S\rangle \oplus |\omega\rangle$, which is exploited to generate a new quantum secret sharing protocol. The agents, Bob and Charlie, generate n-bit keys K_0, K_1, then communicate these keys to Alice via a sequence of photons. Alice combines these to generate the corresponding sequence of n two-qubit initial states, and she performs unitary transformations on each of these initial states in accordance with her secret ω. Alice then measures K_A, which she sends to each of the agents, who can then recover her secret $\omega = K_A \oplus K_0 \oplus K_1$.

2 Grover's algorithm

In 1994, Shor formulated a quantum algorithm to factor integers in polynomial time, a significant improvement from the most efficient classical algorithm, the general number field sieve, which runs in sub-exponential time. With such an advent, public-key encryption schemes like RSA were effectively broken, and interest in efficient quantum algorithms for classically difficult problems surged. As a result, in 1996, Grover formulated an optimal quantum algorithm for the unstructured search problem. For a domain of N elements, this algorithm has time complexity $O(\sqrt{N})$, a quadratic improvement over the classical linear search algorithm. This is optimal in the sense that a lower bound to the time complexity for this problem was shown to be $\Omega(\sqrt{N})$ by Bennett et al.

The unstructured search problem is formulated as follows. Given a function $f : X \to \{0,1\}$, we wish to find an element $\omega \in X$ such that $f(\omega) = 1$. To simplify the algorithm, we make a couple of assumptions. We assume that such an ω is unique, and that $|X| = 2^n = N$ for some $n \in \mathbb{N}$. No generality is lost in these assumptions as the algorithm can be extended to relax the uniqueness assumption, and the domain X can be extended until its cardinality is a power of 2. Therefore, we can reformulate the problem. Given a function $f : \{0,1\}^n \to \{0,1\}$, we wish to find the unique $\omega \in \{0,1\}^n$ such that $f(\omega) = 1$.

We begin with a uniform superposition over the basis vectors of the domain as our initial state.

$$\psi_0 = \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{N}} |x\rangle \tag{1}$$

To query f, we use an oracle gate O_f that will output

$$O_f|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{if } f(x) = 0 \\ -|x\rangle & \text{if } f(x) = -1. \end{cases} \tag{2}$$

Querying the initial state flips the $|\omega\rangle$ phase, yielding

$$\psi_1 = O_f|x\rangle = -\frac{1}{\sqrt{N}}|x^*\rangle + \sum_{x \neq x^*} \frac{1}{\sqrt{N}}|x\rangle. \tag{3}$$

Whilst this introduces an asymmetry in the $|\omega\rangle$ basis vector, it doesn't increase the amplitude of this component. To increase the amplitude of this component, we introduce the Grover diffusion gate D. For notational convenience, we let we α_x denote the coefficient of $|x\rangle$, then we define

$$\mu = \frac{1}{N} \sum_{x \in \{0,1\}^n} \alpha_x \tag{4}$$

as the average coefficient. The Grover diffusion gate then flips the coefficients of the basis vectors about the mean.

$$D\sum_{x\in\{0,1\}^n}\alpha_x|x\rangle=\sum_{x\in\{0,1\}^n}(2\mu-\alpha_x)|x\rangle \qquad (5)$$

The mean coefficient of ψ_1 is

$$\mu=\frac{1}{N}\Big(\frac{N-1}{\sqrt{N}}-\frac{1}{\sqrt{N}}\Big)=\frac{N-2}{N\sqrt{N}}\approx\frac{1}{\sqrt{N}}, \qquad (6)$$

so the coefficients of $|x\rangle\neq|\omega\rangle$ are approximately unchanged by the Grover diffusion gate, but the amplitude of $|\omega\rangle$ increases by a factor of 3. We then iterate application of the oracle gate and the Grover diffusion gate. For α_ω small, the coefficient of $|\omega\rangle$ increases by at least $\frac{1}{\sqrt{N}}$ per iteration, so after $O(\sqrt{N})$ iterations, we have $\alpha_\omega=\Theta(1)$.

Therefore, the unstructured search problem can be optimally solved by Grover's algorithm with time complexity $O(\sqrt{N})$.[1] An immediate consequence of this for cryptography is that brute force attacks against symmetric-key encryption schemes like the Advanced Encryption Standard (AES) can be done in $O(2^{n/2})$ time, where n is the key size, thus requiring the doubling of the key size to preserve the classical security parameter. However, Grover's algorithm has much deeper implications for cryptography, the first of which is a secure quantum secret sharing protocol developed by Hsu in 2003.

3 Quantum Secret Sharing with Hsu's Protocol

Hsu's protocol is a one-to-two party quantum secret sharing protocol. The proposed problem is that Alice wishes to relay a message to two parties, Bob and Charlie, but one of the agents may be dishonest. As long as the two parties collaborate, the original message will be faithfully recovered, but the shadow of any individual agent reveals no information about the secret.

Formally, Alice wishes to share a bit of information in a two-qubit marked state $|\omega\rangle$. In the original Grover's algorithm, the initial state is

$$|S_1\rangle=\Big(\frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)\Big)^{\otimes 2}. \qquad (7)$$

Let $U_x=I-2|x\rangle\langle x|$ be the unitary transformation corresponding to flipping the sign of the $|x\rangle$ component. Then two applications of this operator yield the marked state with certainty.

$$-U_{S_1}U_\omega|S_1\rangle=|\omega\rangle \qquad (8)$$

With regards to Grover's algorithm, this corresponds to flipping the phase of the $|\omega\rangle$ component, then searching for this flipped phase. In general, some other initial state $|S_j\rangle$ can be prepared prepared, where each qubit in $|S_j\rangle$ is in any of the following four states: $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)$, and $\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)$. Then by applying the same transformations, we obtain

$$-U_{S_j}U_\omega|S_j\rangle=e^{i\phi_j}|\omega\rangle, \qquad (9)$$

where ϕ_j is a phase factor.

The protocol begins with Alice preparing an initial state $|S_j\rangle$ with $j\overset{R}{\leftarrow}\{1,\ldots,16\}$. She then performs U_ω on $|S_j\rangle$ and sends each of Bob and Charlie one of the two qubits. Bob and Charlie each confirm via classical communication means that they have received the qubits, then Alice publicly announces her initial state $|S_j\rangle$. Bob and Charlie then combine their qubits and perform $-U_{S_j}$ to recover the marked state $|\omega\rangle$ with certainty. The agents then perform their respective local measurements in the computational basis, and inform Alice of their results.

In this protocol, Alice encrypts her information in the perfectly anti-correlated states $|01\rangle,|10\rangle$, whereas the perfectly correlated states $|00\rangle,|11\rangle$ are used as cheat-detecting states. If the honest agent finds that the outcome state is perfectly correlated, then he concludes that either Alice prepared a cheat-detecting state, or that eavesdropping has occurred. Furthermore, the dishonest agent cannot alter the public classical messages, so Alice will at least receive the honest agent's true outcome. Therefore, Alice will be aware of any cheating behaviour that perturbs the qubits and changes the correlation of the outcome.

This protocol has also been shown to be secure against various other cheating schemes. If the dishonest agent outright declares the wrong outcome, the correlation of the outcome will be changed, and such cheating will immediately be detected. In the intercept-and-measure attack, if Bob intercepts Charlie's qubit and chooses a random $-U_{S_j}$ to perform on the two-qubit system, there is only a $\frac{1}{16}$ probability that Bob will choose the right $-U_{S_j}$. If Bob applies the wrong $-U_{S_j}$, the result is a uniform superposition of states, so there is only a $\frac{1}{4}$ probability of measuring the correct result. Furthermore, it can be shown that after Bob sends the collapsed product state to Charlie, Alice will be able to detect such cheating with probability $\frac{5}{16}$.

In the intercept-and-resend attack, Bob can instead intercept Charlie's qubit and send Charlie a different qubit, then wait until Alice broadcasts the initial state $|S_j\rangle$. Bob then performs the corresponding unitary transformation. However, since Bob has no knowledge of the marked state when he sends Charlie a qubit, it can be assumed that he sends Charlie a uniformly random qubit. It can be shown that when Bob and Charlie collaborate, they will measure a cheat-detecting state with probability at least $\frac{1}{2}$, and the sender and honest agent will immediately detect such cheating. Two other eavesdropping strategies, the intercept-resend strategy with orthogonal measurements and a strategy based on entanglement, have also been shown to be ineffective in Hsu's original paper.[3]

4 Generalized Hsu's Protocol

In 2007, Bhandari and Chamoli generalized Hsu's protocol into an n-qubit secret sharing scheme.[4] The initial state is composed of n qubits, over a Hilbert space of dimension $N = 2^n$. When Grover's algorithm is generalized to search for one of M marked states in a domain of N elements, it turns out that a marked state can be found in time $O(\sqrt{\frac{N}{M}})$. Furthermore, the probability of success after one iteration of Grover's algorithm is

$$p = 9\frac{M}{N} - 24\Big(\frac{M}{N}\Big)^2 + 16\Big(\frac{M}{N}\Big)^3. \tag{10}$$

This equals unity for $\frac{M}{N} = \frac{1}{4}$, so in this protocol, one-fourth of the basis states will be marked. Notice that in the original Hsu's protocol, only one of the four basis states was marked, thus allowing this state to be found with certainty after one iteration of Grover's algorithm.

Therefore, the secret is encoded in $\frac{N}{4}$ of these basis states, which constitute the marked states. Half of the marked states contain the encryption of the first half of the message, and the other half of the marked states contain the encryption of the second half of the message. Letting Ω be the set of marked states, we generalize the unitary transformation U_ω to

$$U_\Omega = I - 2\sum_{\omega\in\Omega} |\omega\rangle\langle\omega|. \tag{11}$$

Alice prepares an initial state $|S_j\rangle$ with $j \overset{R}{\leftarrow} \{1,\ldots,4^n\}$, then flips the phase of the marked components with the U_Ω operator and sends to each of the agents one of the N qubits. The agents again confirm via classical communication channels that they are in receipt of the qubits, and Alice publicly announces her initial state $|S_j\rangle$. When the agents collaborate and apply $-U_{S_j}$, they will measure one of the marked states with uniform probability, so Alice needs to repeat this process several times to communicate all of the marked states.

Just like in the original Hsu's protocol, Alice can use cheat-detecting states to detect dishonest agents, and the cheating strategies mentioned earlier can still be detected. In this general case, in the event that a dishonest agent intercepts all of the bits and performs a random $-U_{S_j}$ on the system, there is a 4^{-n} probability of choosing the correct $-U_{S_j}$, and if the agent applies the wrong $-U_{S_j}$, there is again only a $\frac{1}{4}$ probability of measuring one of the $\frac{N}{4}$ marked states.[4]

5 Dense-coding Attack

Hsu's protocol as originally presented turned out to be insecure against a dense-coding attack, which was discovered by Hao, et al in 2010. In such an attack, a dishonest agent can steal the key information without detection. Suppose Bob is the dishonest agent, and he intercepts Charlie's qubit. He prepares the Bell-state

$$|S_0\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big), \tag{12}$$

and sends one qubit of this state to Charlie. Then when Alice publicly announces the carrier state $|S_j\rangle$, Bob can recover the marked state $|\omega\rangle$ from $U_\omega|S_j\rangle$ with certainty as in the original Hsu protocol. Bob can then perform local operations on his fake qubit to transform its state from $|S_0\rangle$ to $U_\omega|S_j\rangle$. Such procedures are presented in Hao's paper. He thereby changes the state of Charlie's qubit such that it is consistent with the protocol, and neither Alice nor Charlie can detect this eavesdropping.

To remedy this security flaw, Hao et al proposed a revision to Hsu's protocol. After both of the agents confirm via classical communication channels that they are in receipt of the qubit, Alice can perform one of two actions. Alice can broadcast her initial state $|S_j\rangle$ as in the original protocol, or Alice can require the agents to measure their qubit in a randomly chosen basis from the plus-basis $\{|0\rangle, |1\rangle\}$, the cross-basis $\{|+\rangle, |-\rangle\}$, or the circular basis $\{|+i\rangle, |-i\rangle\}$. In the former scenario, the agents continue the protocol as usual. In the latter scenario, the agents must publicly announce their outcomes and measurement bases. If the outcomes are inconsistent with the initial state, then Alice concludes that eavesdropping has occurred, and the session is terminated. In this way, the dense-coding attack can be detected with probability $\frac{1}{2}$.[5]

6 Tseng's Protocol

In 2012, Tseng proposed a different quantum secret sharing protocol that has two key advantages over Hsu's protocol. In Tseng's protocol, the agents do not need to have quantum memory, and the agents can collaborate to recover the boss's secret by using shadows in classical bits. In contrast, Hsu's protocol requires that the agents store the secret shadows in long-term quantum memory, and the agents must combine their shadows in photons to recover the boss's secret.

Tseng's protocol exploits a feature of Grover's algorithm if the initial state is taken to be $|S\rangle \in \{|+\rangle, |-\rangle\}^{\otimes n}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. We henceforth consider the case of a two-qubit system with $n = 2$. Instead of using the unitary operator U_{S_j}, we use the unitary operator

$$U_+ = I - 2|++\rangle\langle++|. \tag{13}$$

Let $|++\rangle, |-+\rangle, |+-\rangle, |--\rangle$ correspond to the classical two-bit information 00, 01, 10, and 11 respectively. Similarly, let $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ correspond to the same information, respectively. Then after Grover's algorithm is performed under these conditions, the measurement result $|\omega'\rangle$ satisfies the relationship

$$|\omega'\rangle = |S\rangle \oplus |\omega\rangle. \tag{14}$$

The protocol proceeds as follows. Let $\omega \in \{0,1\}^N$ be the secret that Alice wishes to share, and let $i \in \{B, C\}$ denote the agents Bob and Charlie, respectively. The agents i choose keys $K_i \xleftarrow{R} \{0,1\}^N$, and prepare a corresponding sequence of photons S_i. For each bit of K_i, if the bit is 0, the agent prepares $|+\rangle$, and if the bit is 1, the agent prepares $|-\rangle$. The agents also prepare sufficiently many decoy photons, which are chosen uniformly at random from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, then insert these into random positions in S_i to obtain a new sequence of photons S_i'. The agents then relay S_i' to Alice.

Alice publicly confirms that she has received S_i', then the security of the quantum channels is verified by public discussion. The agents announce the positions, bases, and values of the decoy photons, and Alice measures these photons in the corresponding bases. If the error rate exceeds a predetermined threshold, then the protocol is terminated.

Alice combines the two sequences of photons to obtain a sequence $|S\rangle$ of N two-qubit states $|S^{(j)}\rangle = |S_0^{(j)} S_1^{(j)}\rangle$. For each state $|S^{(j)}\rangle$, Alice applies the unitary transformation $U^{\omega^{(j)}}$, where $\omega^{(j)}$ denotes the j-th bit of ω, $U^0 \in \{U_{00}, U_{11}\}$, and $U^1 \in \{U_{01}, U_{10}\}$. Alice then performs $-U_+$ on each $|S^{(j)}\rangle$ in accordance with Grover's algorithm, obtaining $-U_+ U_\omega |S\rangle$. Alice uses the Z basis to measure the photons of $|S\rangle$, and records the results, where a measurement result of $|00\rangle, |11\rangle$ corresponds to a bit of 0, and a measurement result of $|01\rangle, |10\rangle$ corresponds to a bit of 1. Alice sends the result $K_A \in \{0,1\}^N$ to the agents, who then recover her secret as

$$\omega = K_A \oplus K_0 \oplus K_1. \tag{15}$$

We now analyze the security of this protocol. The decoy photons protect the protocol from an intercept-and-resend attack, since if Bob intercepts Charlie's photons and sends Alice a stream of different photons, each decoy photon has a $\frac{1}{4}$ probability of being correct. Therefore, the probability that he evades detection is $1 - (\frac{3}{4})^n$, where n is the number of decoy photons. It can also be shown that this protocol is secure against the entangle-and-measure attack, in which Bob intercepts Charlie's photons, entangles auxiliary photons with them, and then resends the original photons. In such an attack, Bob will information-theoretically be unable to obtain any information about Alice's secret.[6]

7 Closing Remarks

Despite almost two decades of work on quantum secret sharing, no existing protocol has been proven to be unconditionally secure against cheating schemes by dishonest agents, even those that don't rely on Grover's algorithm. Therefore, quantum secret sharing remains a theoretical curiosity, and any practical implementation of secure secret sharing must defer to conventional parallel quantum key distribution. Furthermore, many of the stronger protocols require ideal single-photon sources or quantum memories, which are difficult to realize in practice.

However, progress is still being made towards a secure and realizable quantum secret sharing protocol, with Kogias, et al publishing earlier this year an unconditional security proof for entanglement-based continuous-variable quantum secret schemes for an arbitrary number of agents, in the limit of asymptotic keys.[7] As such, there is still hope that quantum secret sharing could become a viable primitive for quantum technologies.

References

[1] Grover, Lov. ”A fast quantum mechanical algorithm for database search.” 1996.

[2] Grover, Lov. ”From Schrodinger’s Equation to the Quantum Search Algorithm.” 2001.

[3] Hsu, Li-Yi. ”Quantum secret-sharing protocol based on Grover’s algorithm.” 2003.

[4] Bhandari, C. and Chamoli, A. ”Grover’s algorithm based multi-qubit secret sharing scheme.” 2007.

[5] Hao, L., Li, J., and Long, G. ”Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution.” 2010.

[6] Tseng, H., Tsai, C., and Hwang, T. ”Quantum Secret Sharing Based on Quantum Search Algorithm.” 2012.

[7] Kogias, I., et al. ”Unconditional security of entanglement-based continuous-variable quantum secret sharing.” 2017.