An Information-Theoretic Security Analysis of Quantum String Sealing

MASAKI NAKANISHI
Nara Institute of Science and Technology
Ikoma, Nara 630–0101
JAPAN

SEIICHIRO TANI
NTT Communication Science Labs.
NTT Corporation
Atsugi, Kanagawa 243–0198
JAPAN

SHIGERU YAMASHITA
Nara Institute of Science and Technology
Ikoma, Nara 630–0101
JAPAN

Abstract: A quantum sealing protocol is a quantum cryptographic protocol that can detect unsealing of a message. It is known that quantum *bit* sealing is insecure. However, this does not imply that quantum *string* sealing is also insecure. So the possibility of quantum string sealing has been studied. In this paper, we propose a quantum sealing protocol and give an information theoretic analysis. We also show that our protocol is almost optimal for uniformly distributed inputs in the sense that the upper bound of information leaks almost matches the trivial lower bound.

Key–Words: Quantum cryptography, Quantum sealing, Security analysis

1 Introduction

A quantum sealing protocol was first proposed by Bechmann-Pasquinucci [1], in which the sender (Alice) can encode a secret bit in a quantum state in such a way that the receiver (Bob) can find out the value of the bit by an appropriate measurement which disturbs the quantum state, enabling Alice to detect such a measurement. It is shown that quantum sealing has wide applications such as protective packaging, loose bit commitment, eavesdropping detection and etc. [13]. Obviously such a sealing cannot be done by any classical protocol, thus it is very natural to consider an efficient quantum sealing protocol in various perspectives [2, 3, 6, 12].

However, it was proved by He [7] and Chau [4] independently that quantum *bit* sealing is insecure. Fortunately, this does not mean that quantum *string* sealing is also insecure. Thus, the security of quantum string sealing has been investigated [5, 6, 8]. Recently, Chau claimed that there is no secure quantum string sealing protocol [5] in the following sense: It was shown that there is a cheating strategy that can reveal the whole string with non-negligible probability while it is detected with probability less than $1/2$. Replying to this, He claimed that the whole string is not necessarily recovered even for honest players, and quantum string sealing protocols can be such that honest players can obtain a fraction of the sealed message with high probability but the whole message with exponentially small probability [8]. He also claimed that the amount of information that one can obtain by Chau's attack strategy is trivial in the sense that Chau's attack strategy is almost the same as measuring the quantum state honestly with probability 1/2 and doing nothing otherwise [8, 9].

These arguments are due to the lack of a formal definition of a measure of information leaks. As a measure of information leaks, a mutual information was mentioned in Chau's paper [5], however his analysis concentrated mainly on calculating Bob's success probability and covered only the limited case in which the attacker wants to retrieve the whole message. On the other hand, He's analysis concentrated on the success probability that Bob successfully obtains (a portion of) the sealed message without being detected [6].

In this paper, contrary to the above mentioned papers, we take a different approach, that is, we give an information theoretic analysis where the measure of information leaks is a mutual information between the inputs and the results of Bob's measurement. As He mentioned in [8, 9], it is obvious that if the attacker decodes the sealed message honestly with probability

δ and do nothing with probability $1-\delta$, he/she can retrieve $\delta \cdot I_{max}$ of information while it can be detected with probability at most δ, where I_{max} is the amount of information that honest players can retrieve. Thus, the point is whether the attacker can do more or not. To answer this question, we propose a quantum string sealing protocol that is almost optimal for the uniformly distributed input strings in the sense that the upper bound of information leaks almost matches the trivial lower bound. That is, the attacker can do nothing more than the above trivial attack.

Technically, we used the lemma shown by Lo and Chau [10], which gives an upper bound to the mutual information between the measurement results of the two quantum subsystems. The difficulty is to modify the quantum sealing scheme to fit the lemma since the lemma can be applied only to a pure quantum state while the actual quantum sealing scheme can be represented by mixed states. We give an ideal model of quantum sealing so that we can apply the lemma to it, while the model can be shown to be equivalent to the actual model.

This paper is organized as follows: In Section 2, we introduce a model of quantum sealing and show a trivial lower bound that is mentioned by He [8, 9]. In Section 3, we propose a quantum string sealing protocol and show the upper bound on the amount of information leaks, which almost matches the trivial lower bound for uniformly distributed inputs. Section 4 concludes this paper.

2 Preliminaries

We define the model of quantum sealing as follows:

- Alice encodes the input string into a quantum state that consists of two quantum registers.

  $$\text{input string } i\text{: } |0\rangle\,|0\rangle \longrightarrow \Sigma_j \alpha_j \left|\phi_j^i\right\rangle \left|\psi_j^i\right\rangle,$$

  where $\left|\phi_j^i\right\rangle$ are mutually orthogonal. Then Alice sends the second register to Bob. That is, Bob has the following state ρ_i.

  $$\rho_i = \Sigma_j |\alpha_j|^2 \left|\psi_j^i\right\rangle \left\langle\psi_j^i\right|$$

  Bob performs a POVM to ρ_i in order to decode the state, and obtain a result.

We define the amount of information Bob obtains to be a mutual information between X and Y, where X is a random variable representing the input string and Y is a random variable representing Bob's result of POVM. We also define the decoding rate as follows:

$$\text{(decoding rate)} = I_{max}/H(X),$$

where I_{max} is the mutual information between X and Y for the case that Bob performs the measurement honestly.

As He pointed out in [8], a trivial attack to quantum sealing protocols is to measure the quantum state honestly with probability δ and leave it untouched with probability $1-\delta$. Then, Bob can obtain $\delta \cdot I_{max}$ bits of information while it is detected with probability at most δ. Thus, we have the following lower bound on the amount of information Bob can obtain.

Theorem 1 *For any n-bit quantum string sealing protocol with decoding rate of $1-\varepsilon$, there is a cheating strategy that can retrieve $\delta \cdot (1-\varepsilon) \cdot H(X)$ bits of information with detection probability less than or equal to δ, where X is a random variable representing the input string.*

Proof: Let Y' be a random variable representing the value obtained by the following decoding scheme:

- With probability δ, decode the quantum state honestly, and with probability $1-\delta$, do nothing.

The amount of information Bob obtains is $I(X:Y')$. Let S_X be the set of possible input strings, and let S_Y be the set of possible outcomes that Bob obtains when he decodes the quantum state honestly. Also let $p_X(x)$ be the probability of $X=x$, and let $p_{X|Y}(x|y)$ be the conditional probability of $X=x$ given $Y=y$.

Then, Y' is z (no outcome) with probability $1-\delta$. Note that $p_{X|Y'}(x|z) = p_X(x)$.

Y' is $y \in S_Y$ with probability $\delta \cdot p_Y(y)$, where $p_Y(y)$ is the probability that y is obtained when Bob measures the quantum state honestly.

Thus,

$$\begin{aligned} & H(X|Y') \\ = \; & -(1-\delta)\Sigma_{x\in S_X} p_{X|Y'}(x|z)\log p_{X|Y'}(x|z) \\ & -\Sigma_{y\in S_Y}\delta\cdot p_Y(y)\Sigma_{x\in S_X} p_{X|Y}(x|y)\log p_{X|Y}(x|y) \\ = \; & (1-\delta)H(X) + \delta H(X|Y). \end{aligned}$$

Note that $I(X|Y) = (1-\varepsilon)H(X)$. Thus,

$$\begin{aligned} & I(X:Y') \\ = \; & H(X) - H(X|Y') \\ = \; & H(X) - ((1-\delta)H(X) + \delta H(X|Y)) \\ = \; & \delta(H(X) - H(X|Y)) \\ = \; & \delta I(X|Y) \\ = \; & \delta(1-\varepsilon)H(X). \end{aligned}$$

□

3 Our protocol and its security analysis

In this section, we propose a quantum sealing protocol, and show that our protocol is almost optimal for uniformly distributed input strings. That is, for uniformly distributed input strings, the upper bound on the amount of information Bob can obtain almost matches the lower bound shown in Theorem 1.

The proposed protocol is as follows.[1] Let i be an input string ($0 \leq i \leq 2^n - 1$). Alice randomly chooses $X \in \{X_0, \ldots, X_{2^n-1}\}$, and encodes the input as $\frac{1}{\sqrt{2}}(|i\rangle + |X\rangle)$, where $\{|0\rangle, \ldots, |2^n - 1\rangle, |X_0\rangle, \ldots, |X_{2^n-1}\rangle\}$ are mutually orthogonal. Then Alice sends the encoded state to Bob. For decoding of the message, Bob measures the received quantum state with respect to the computational basis, by which Bob can obtain the correct message with probability $1/2$. Note that the quantum state after the measurement is $|i\rangle$ or $|X\rangle$. Thus Alice can detect Bob's measurement with probability $1/2$ by measuring the state with respect to $\frac{1}{\sqrt{2}}(|i\rangle + |X\rangle)$.

Honest Bob can obtain $H(X)/2$ bits of information as proved in the following theorem, where X is a random variable representing the input string. Especially, for uniformly distributed input strings, Bob can obtain $n/2$ bits of information.

Theorem 2 *Our protocol achieves decoding rate* $1/2$.

Proof: Let $Y_1 = \{0, 1, \ldots, 2^n - 1\}$. Also let $Y_2 = \{X_0, X_1, \ldots, X_{2^n-1}\}$. We define S_X and S_Y in the same way as in Theorem 1.

$$\begin{aligned}
& H(X|Y) \\
= \; & -\Sigma_{y \in S_Y} p_Y(y) H(X|y) \\
= \; & -\Sigma_{y \in S_Y} p_Y(y) \Sigma_{x \in S_X} p_{X|Y}(x|y) \log p_{X|Y}(x|y) \\
= \; & -\Sigma_{y \in Y_1} p_Y(y) \Sigma_{x \in S_X} p_{X|Y}(x|y) \log p_{X|Y}(x|y) \\
& -\Sigma_{y \in Y_2} p_Y(y) \Sigma_{x \in S_X} p_{X|Y}(x|y) \log p_{X|Y}(x|y) \\
= \; & -\Sigma_{y \in Y_1} p_Y(y) \cdot 0 \\
& -\Sigma_{y \in Y_2} p_Y(y) \Sigma_{x \in S_X} p_X(x) \log p_X(x) \\
= \; & -\Sigma_{y \in Y_2} p_Y(y) H(X) \\
= \; & H(X)/2
\end{aligned}$$

Therefore

$$I(X:Y) = H(X) - H(X|Y) = H(X)/2.$$

□

For our protocol, we have the following upper bound.

[1]Note that our protocol uses a single register, while two registers are used in our general model defined in Section 2. That is, our protocol is the special case of the general model where the first register is fixed to $|0\rangle$, which we omit to describe.

Theorem 3 *We consider arbitrary decoding scheme. For the decoding scheme, if Bob can be detected with probability at most* δ*, then the amount of information that Bob can obtain is* $O((\delta + 1/2^n)n)$. □

Note that for uniformly distributed input strings, the upper bound almost matches the lower bound, $\delta n/2$, in Theorem 1.

In order to prove Theorem 3, we introduce the following lemma shown by Lo and Chau [10].

Lemma 4 *Given any pure state* ϕ_{AB} *of a system consisting of two subsystems* A *and* B*, and any measurements* X *and* Y *on* A *and* B *respectively, the entropy of each subsystem* $S(\rho_A)$ *(where* $\rho_A = Tr_B |\phi_{AB}\rangle \langle\phi_{AB}|$*) is an upper bound to the amount of mutual information between* X *and* Y. □

We regard A and B as the quantum states that Alice and Bob have, respectively. We also regard X and Y as the measurements on Alice's input and Bob's state respectively. Then we can calculate the upper bound to the mutual information between the inputs and Bob's results of POVM, i.e., the amount of information leaks. However, the model of quantum sealing defined in Section 2 does not fit Lemma 4. To apply Lemma 4 to our quantum sealing scheme, we introduce the following cheating model. We consider three quantum registers. The first register has a superposition of input strings, $\Sigma_{i=0}^{2^n-1} \sqrt{p_i} |i\rangle$, where p_i is the probability that Alice has i as an input. Alice encodes the input string into the second register, and sends it to Bob. We assume that Alice chooses $X \in \{X_0, \ldots, X_{2^n-1}\}$ randomly in advance and uses the same X to encode every input string. That is, the state right after Alice encodes the input string is

$$\Sigma_{i=0}^{2^n-1} \sqrt{p_i} |i\rangle \otimes \left(\frac{1}{\sqrt{2}} (|i\rangle + |X\rangle) \right) \otimes |0\rangle .$$

The third register is Bob's ancilla. Bob applies arbitrary unitary operator U_B to the second and the third registers, and then measures the third register to obtain information. In order to detect Bob's measurement, Alice measures the second register. In this model, Bob's measurement is restricted to the third register. However, this does not restrict Bob's ability (See Section 2.2.8 in [11]). Note that after Alice encodes the input string, the first register is no longer referred to. This means that the state that Alice and Bob can have after Alice encodes the input string is a mixed state obtained by tracing out the first register. This mixed state is the same state as in the actual protocol. Thus our analysis using the above cheating model is valid for the actual situation.

Let X be a random variable representing the result of a measurement on the first register, and let Y

be a random variable representing the result of Bob's measurement. Then mutual information $I(X : Y)$ represents the amount of information that Bob can obtain.

Considering the above cheating model, we have the following as a corollary of Lemma 4.

Corollary 5 *Let ρ_A be the state of the subsystem consisting of the first and the second registers right before Bob's measurement. Then the amount of information that Bob can obtain is upper bounded by $S(\rho_A)$.* □

To prove Theorem 3, we also introduce the following lemma.

Lemma 6 *Let U_B be an arbitrary unitary operator that Bob applies to the second and the third registers. Then U_B is equivalent to U'_B that satisfies the condition below in the sense that the detection probability and the amount of information Bob can obtain are invariant between U_B and U'_B.*

$$U'_B |i\rangle |0\rangle = \Sigma_{j=0}^{2^n-1} a_j |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_{j=0}^{2^n-1} b_j |j\rangle |w_j\rangle,$$

where $|a_1| = |a_2| = \ldots = |a_{2^n}| (\leq \frac{1}{\sqrt{2^n}})$.

Proof: We can write as follows:

$$U_B |i\rangle |0\rangle = \Sigma_{j=0}^{2^n-1} a_j |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_{j=0}^{2^n-1} b_j |j\rangle |w_j\rangle,$$

$X \in \{X_0, \ldots, X_{2^n-1}\}$ is chosen randomly when Alice encodes the input string. Thus applying the following U_B^π instead of U_B does not affect the detection probability and the amount of information Bob can obtain:

$$\begin{aligned} & U_B^\pi |i\rangle |0\rangle \\ = \; & \Sigma_{j=0}^{2^n-1} a_j \left|X_{\pi(j)}\right\rangle \left|w_{X_{\pi(j)}}\right\rangle + \Sigma_{j=0}^{2^n-1} b_j |j\rangle |w_j\rangle, \end{aligned}$$

where π is a random permutation of j. Since π is chosen randomly, the resulting state will be a mixed state. By purifying the resulting (mixed) state with enough number of ancilla, the operation can be written as

$$U'_B |i\rangle |0\rangle = \Sigma_{j=0}^{2^n-1} a_j |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_{j=0}^{2^n-1} b_j |j\rangle |w_j\rangle,$$

where $|a_1| = |a_2| = \ldots = |a_{2^n}| (\leq \frac{1}{\sqrt{2^n}})$. □

We prove Theorem 3 in the following.

Proof of Theorem 3: Let $|\psi\rangle \in \mathcal{H}_n$. Also let $\mathcal{H}_m$ and $\mathcal{H}_{n-m}$ be the subspaces of $\mathcal{H}_n$, where $m < n$, and let $|\phi\rangle \in \mathcal{H}_m$. We define notation $\tilde{\perp}$ as follows:

- $|\phi\rangle \tilde{\perp} |\psi\rangle$ means that for any $|\phi'\rangle \in \mathcal{H}_{n-m}$, the composite system of $|\phi\rangle$ and $|\phi'\rangle$ is perpendicular to $|\psi\rangle$.

We can write as follows:

$$U_B |X\rangle |0\rangle = \alpha_1 |X\rangle |w_\alpha\rangle + \alpha'_1 |\psi_{\alpha_1}\rangle |w_\alpha\rangle + \beta_1 |\psi_{\beta_1}\rangle,$$

where $|X\rangle \tilde{\perp} |\psi_{\beta_1}\rangle$, $|w_\alpha\rangle \tilde{\perp} |\psi_{\beta_1}\rangle$ and $|X\rangle \perp |\psi_{\alpha_1}\rangle$. Also we can write as follows:

$$U_B \left(\frac{1}{\sqrt{2}} |i\rangle + \frac{1}{\sqrt{2}} |X\rangle\right) |0\rangle = \alpha |\psi_\alpha\rangle |w_\alpha\rangle + \beta |\psi_\beta\rangle, \quad (1)$$

where $|w_\alpha\rangle \tilde{\perp} |\psi_\beta\rangle$. We calculate a lower bound on the detection probability in the following, and then derive an upper bound on $|\beta|$. We consider a projection of $\beta |\psi_\beta\rangle$ onto the subspace in which the second register is fixed to $(\frac{1}{\sqrt{2}} |i\rangle + \frac{1}{\sqrt{2}} |X\rangle)^\perp$ $(= \frac{1}{\sqrt{2}} |i\rangle - \frac{1}{\sqrt{2}} |X\rangle)$. Since $|w_a\rangle \tilde{\perp} |\psi_\beta\rangle$, the detection probability is at least the absolute square of the length of the projection. We first express $\beta |\psi_\beta\rangle$ in terms of $|X\rangle$ and $|i\rangle$. By Lemma 6, we can assume the following:

$$\begin{aligned} & U_B |i\rangle |0\rangle \\ = \; & \Sigma_{j=0}^{2^n-1} \frac{e^{i\theta_{X_j}} a'}{\sqrt{2^n}} |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_{j=0}^{2^n-1} b_j |j\rangle |w_j\rangle, \end{aligned}$$

where $0 \leq a' \leq 1$. We can write as follows:

$$\frac{e^{i\theta_X} a'}{\sqrt{2^n}} |X\rangle |w_X\rangle = \frac{a''}{\sqrt{2^n}} |X\rangle |w_\alpha\rangle + \frac{a}{\sqrt{2^n}} |X\rangle \left|w_\alpha^\perp\right\rangle,$$

where $|w_\alpha\rangle \perp \left|w_\alpha^\perp\right\rangle$. Then $\beta |\psi_\beta\rangle$ can be described as follows:

$$\beta |\psi_\beta\rangle = \frac{a}{\sqrt{2}\sqrt{2^n}} |X\rangle \left|w_\alpha^\perp\right\rangle + b |i\rangle |w\rangle + c \left|\psi'_\beta\right\rangle,$$

where $|X\rangle \tilde{\perp} \left|\psi'_\beta\right\rangle$, $|i\rangle \tilde{\perp} \left|\psi'_\beta\right\rangle$, $|a| \leq a' \leq 1$ and $|\frac{a}{\sqrt{2^{n+1}}}|^2 + |b|^2 + |c|^2 = |\beta|^2$.

As mentioned in the above, we consider a projection of $\beta |\psi_\beta\rangle$ onto the subspace in which the second register is fixed to $(\frac{1}{\sqrt{2}} |i\rangle + \frac{1}{\sqrt{2}} |X\rangle)^\perp$ $(= \frac{1}{\sqrt{2}} |i\rangle - \frac{1}{\sqrt{2}} |X\rangle)$. Let p be the square of the length of the projection. Then the detection probability is at least p. Since the detection probability is at most δ, we have $p \leq \delta$. By the lower bound on p and the condition $p \leq \delta$, it can be shown that $|\beta| \leq \sqrt{2\delta} + \frac{1}{\sqrt{2^n}}$ (See Appendix). This implies that $|\alpha| \geq \sqrt{1 - O(\delta + 1/2^n)}$. We rewrite Eq. (1) as follows:

$$\begin{aligned} & U_B \left(\frac{1}{\sqrt{2}} |i\rangle + \frac{1}{\sqrt{2}} |X\rangle\right) |0\rangle \\ = \; & \alpha^i \left|\psi_\alpha^i\right\rangle |w_\alpha\rangle + \beta^i \left|\psi_\beta^i\right\rangle \end{aligned}$$

Then, the whole state including the first to the third registers $|\Psi\rangle$ is described as follows:

$$\begin{aligned} |\Psi\rangle &= \Sigma_i \sqrt{p_i}\,|i\rangle \left(\alpha^i \left|\psi^i_\alpha\right\rangle |w_\alpha\rangle + \beta^i \left|\psi^i_\beta\right\rangle\right) \\ &= A\,|\Psi_A\rangle\,|w_\alpha\rangle + B\,|\Psi_B\rangle\,, \end{aligned}$$

where $\{p_i\}$ is the probability distribution of inputs. Note that $|A| \geq \sqrt{1 - O(\delta + 1/2^n)}$. By tracing out the third register, we obtain the following:

$$\begin{aligned} \rho_A &= |A|^2\,|\Psi_A\rangle\langle\Psi_A| + |B_1|^2\,|\Psi_{B_1}\rangle\langle\Psi_{B_1}| \\ &\quad + |B_2|^2\,|\Psi_{B_2}\rangle\langle\Psi_{B_2}| + \ldots \end{aligned}$$

Thus,

$$\begin{aligned} S(\rho_A) &\leq -|A|^2 \log |A|^2 + \Sigma_j - B_j \log B_j \\ &\leq -|A|^2 \log |A|^2 \\ &\quad + \Sigma_1^{2^{2n+1}} - \frac{(1-|A|^2)}{2^{2n+1}} \log \frac{(1-|A|^2)}{2^{2n+1}} \\ &= H(|A|^2) + (1-|A|^2)\log 2^{2n+1} \\ &\leq 1 + O(\delta + 1/2^n)(2n+1) \end{aligned}$$

Thus, $S(\rho_A) \leq O((\delta + 1/2^n)n)$. By Corollary 5, Bob can obtain the information at most $O((\delta + 1/2^n)n)$.□

4 Conclusion

We proposed a quantum string sealing protocol and analyzed it information-theoretically. We showed that our protocol is optimal in the sense that the upper bound of information leaks almost matches the trivial lower bound if the probability distribution of input strings is uniform, i.e., the lower bound is $\delta n/2$, and the upper bound is $O((\delta + 1/2^n)n)$. This result gives the trade-offs between the amount of information leaks and detection probabilities. Note that this result says that there is a quantum string sealing protocol in which the attacker can do nothing more than the trivial cheating strategy.

In our protocol, optimality is guaranteed only in the case that inputs are uniformly distributed. The future work is to show the optimality for arbitrary distribution.

Acknowledgements: This work was supported in part by KAKENHI (16092218), (18700011), (19700010), (19700019).

References:

[1] H. Bechmann-Pasquinucci, Quantum seals, *International Journal of Quantum Information*, vol. 1, no. 2, 2003, pp. 217–224.

[2] H. Bechmann-Pasquinucci, G. M. D'Ariano, and C. Macchiavello, Impossibility of perfect quantum sealing of classical information, *International Journal of Quantum Information*, vol. 3, no. 2, 2005, pp. 435–440.

[3] H. F. Chau, Sealing quantum message by quantum code, quant-ph/0308146, 2003.

[4] H. F. Chau, Insecurity of imperfect quantum bit seal, *Physics Letters A*, vol. 354, no. 1-2, 2006, pp. 31–34.

[5] H. F. Chau, Quantum string seal is insecure, *Physical Review A*, vol. 75, no. 1, 012327, 2007.

[6] G.–P. He, Quantum bit string sealing, *International Journal of Quantum Information*, vol. 4, no. 4, 2006, pp. 677–687.

[7] G.–P. He, Upper bounds of a class of imperfect quantum sealing protocols, *Physical Review A*, vol. 71, no. 5, 054304, 2005.

[8] G.–P. He, Secure quantum string seal exists, quant-ph/0602159, 2006.

[9] G.–P. He, Comment on "Quantum string seal is insecure", quant-ph/0612071, 2006.

[10] H.–K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science*, vol. 283, 1999, pp. 2050–2056.

[11] M. L. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[12] S. K. Singh and R. Srikanth, Quantum seals, *Physica Scripta*, vol. 71, no. 5, 2005, pp. 433–435.

[13] G. Gordon Worley III, Applications of quantum message sealing, *SPIE paper 5815-25 at Quantum Information and Computation III*, SPIE defense & Security Symposium 2005.

Appendix

To show $|\beta| \leq \sqrt{2\delta} + \frac{1}{\sqrt{2^n}}$, we first calculate a lower bound on p. p is minimized when $c = 0$ and $\left|w^\perp_\alpha\right\rangle = |w\rangle$ ($\stackrel{\triangle}{=} |W\rangle$). Then we have

$$\begin{aligned} &\beta\,|\psi_\beta\rangle \\ &= \frac{a}{\sqrt{2^{n+1}}}\,|X\rangle\,|W\rangle + e^{i\theta}\sqrt{|\beta|^2 - \frac{|a|^2}{2^{n+1}}}\,|i\rangle\,|W\rangle\,. \end{aligned}$$

We also consider the following state:

$$\frac{1}{\sqrt{2}}\,|X\rangle\,|W\rangle - \frac{1}{\sqrt{2}}\,|i\rangle\,|W\rangle$$

Then the absolute square of the inner product of the above two vectors is equal to p. Thus,

$$\begin{aligned} p &= \left| \frac{|a|}{\sqrt{2^{n+2}}} - e^{i\theta}\sqrt{\frac{|\beta|^2}{2} - \frac{|a|^2}{2^{n+2}}} \right|^2 \\ &\geq \left(\frac{|a|}{\sqrt{2^{n+2}}} - \sqrt{\frac{|\beta|^2}{2} - \frac{|a|^2}{2^{n+2}}} \right)^2 \\ &\stackrel{\triangle}{=} f(|a|) \ (\stackrel{\triangle}{=} F^2), \end{aligned}$$

where $\frac{|\beta|^2}{2} - \frac{|a|^2}{2^{n+2}} \geq 0$, i.e., $|a| \leq 2^{(n+1)/2}|\beta|$. Then

$$f'(|a|) = 2F(\frac{d}{d|a|}F),$$

where

$$\frac{d}{d|a|}F = \frac{1}{\sqrt{2^{n+2}}} + \frac{|a|}{2^{n+1}} \cdot \frac{1}{2\sqrt{\frac{|\beta|^2}{2} - \frac{|a|^2}{2^{n+2}}}}.$$

Since $\frac{d}{d|a|}F > 0$, $f'(|a|) = 0$ at $|a| = 2^{n/2}|\beta|$. This value satisfies the condition of $|a| \leq 2^{(n+1)/2}|\beta|$. Since $|a| \leq 1$ and $f'(|a|)$ is a monotone-increasing function, $f(|a|)$ attains the minimum at

$$|a| = \text{Min}\{2^{(n+1)/2}|\beta|, 1\},$$

i.e., at

$$\begin{aligned} |a| &= 2^{(n+1)/2}|\beta| \text{ for } |\beta| \leq \frac{1}{2^{(n+1)/2}} \text{ and} \\ |a| &= 1 \text{ otherwise.} \end{aligned}$$

In the case of $0 \leq |\beta| \leq \frac{1}{2^{(n+1)/2}}$, it is obvious that $|\beta| \leq \sqrt{2\delta} + \frac{1}{\sqrt{2^n}}$. We consider the case of $|\beta| > \frac{1}{2^{(n+1)/2}}$ in the following.

$f(|a|)$ attains the minimum at $|a| = 1$.

$$\begin{aligned} f(1) &= \left(\frac{1}{\sqrt{2^{n+2}}} - \sqrt{\frac{|\beta|^2}{2} - \frac{1}{2^{n+2}}} \right)^2 \\ &= \frac{|\beta|^2}{2} - \frac{1}{\sqrt{2^n}}\sqrt{\frac{|\beta|^2}{2} - \frac{1}{2^{n+2}}} \\ &= Y - \frac{1}{\sqrt{2^n}}\sqrt{Y - \frac{1}{2^{n+2}}}, \end{aligned}$$

where $Y = \frac{|\beta|^2}{2}$. Note that $\delta \geq p \geq f(1)$. Thus,

$$Y - \delta \leq \frac{1}{\sqrt{2^n}}\sqrt{Y - \frac{1}{2^{n+2}}}.$$

In the case of $Y - \delta < 0$, it is obvious that $|\beta| \leq \sqrt{2\delta} + \frac{1}{\sqrt{2^n}}$. We consider the case of $Y - \delta \geq 0$ in the following. From

$$Y - \delta \leq \frac{1}{\sqrt{2^n}}\sqrt{Y - \frac{1}{2^{n+2}}},$$

we have

$$(Y - \delta)^2 \leq \frac{1}{2^n}(Y - \frac{1}{2^{n+2}}),$$

i.e.,

$$Y^2 - (2\delta + \frac{1}{2^n})Y + (\delta^2 + \frac{1}{2^{2n+2}}) \leq 0.$$

The solutions of $Y^2 - (2\delta + \frac{1}{2^n})Y + (\delta^2 + \frac{1}{2^{2n+2}}) = 0$ are

$$Y = \delta + \frac{1}{2^{n+1}} \pm \sqrt{\frac{1}{2^n}\delta}.$$

Thus,

$$\delta + \frac{1}{2^{n+1}} - \sqrt{\frac{1}{2^n}\delta} \leq Y \leq \delta + \frac{1}{2^{n+1}} + \sqrt{\frac{1}{2^n}\delta}.$$

Since $|\beta|^2 = 2Y$,

$$\begin{aligned} |\beta| &\leq \sqrt{2}\sqrt{\delta + \frac{1}{2^{n+1}} + \sqrt{\frac{1}{2^n}\delta}} \\ &\leq \sqrt{2}\sqrt{\delta + \frac{1}{2^{n+1}} + \sqrt{\frac{2}{2^n}\delta}} \\ &= \sqrt{2}\sqrt{(\sqrt{\delta} + \frac{1}{2^{(n+1)/2}})^2} \\ &= \sqrt{2\delta} + \frac{1}{\sqrt{2^n}} \end{aligned}$$

□