Quantum messages with signatures forgeable in arbitrated quantum signature schemes

Taewan Kim,[1] Jeong Woon Choi,[2] Nam-Su Jho,[3] and Soojoon Lee[4,5]

[1] *Institute of Mathematical Sciences, Ewha Womans University, Seoul 120-750, Korea*
[2] *Emerging Technology R&D Center, SK Telecom, Kyunggi 463-784, Korea*
[3] *Cryptography Research Team, Electronics and Telecommunications Research Institute, Daejeon 305-700, Korea*
[4] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea*
[5] *School of Mathematical Sciences, The University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom*

(Dated: July 8, 2014)

Even though a method to perfectly sign quantum messages has not been known, the arbitrated quantum signature scheme has been considered as one of good candidates. However, its forgery problem has been an obstacle to the scheme being a successful method. In this paper, we consider quantum messages with signatures which can be forged in arbitrated quantum signature schemes, and show that there exists such a forgeable quantum message-signature pair for every known scheme. Furthermore, we present our modified arbitrated quantum signature scheme, and numerically show that any forgeable quantum message-signature pairs do not exist in the scheme.

PACS numbers: 03.67.Dd, 03.67.Hk

arXiv:1407.1380v1 [quant-ph] 5 Jul 2014

I. INTRODUCTION

Digital signature has been considered as one of the most important cryptographic tools for not only authentication of digital messages and data integrity but also non-repudiation of origin. Thus, since the advent of quantum cryptography which provides us with unconditional security in key distribution, many studies on quantum-mechanics-based signatures have been conducted.

In particular, it was pointed out that digitally signing quantum messages is not possible [1] although quantum mechanics can be helpful in digital signature [2]. Hence, quantumly signing quantum messages with the help of an arbitrator has been suggested [3–7], and the signature schemes are called the *arbitrated quantum signature* (AQS) schemes.

In all AQS schemes on the qubit system, their quantum signature operators consist of two parts. One is called the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ defined by two Pauli operators σ_x and σ_z, that is, $R_0=\sigma_x$ and $R_1=\sigma_z$, and the other is called the quantum encryption $\{E_k\}_{k\in\mathbb{Z}_4}$ [8] such that for all qubit states ρ

$$\frac{1}{4}\sum_{k\in\mathbb{Z}_4}E_k\rho E_k^\dagger=\frac{1}{2}I, \tag{1}$$

where E_k are unitary operators.

In the AQS schemes, by applying these two parts of operators to a given quantum message $|M\rangle$ according to the previously shared key (j,k), the signature

$$|S\rangle=E_kR_j|M\rangle \tag{2}$$

is obtained, and the validity of the signature can basically be determined as follows: Let $|M'\rangle$ be the transmitted message and $R_j^\dagger E_k^\dagger|S'\rangle$ be the state obtained by applying the inverse of quantum signature operators to the transmitted signature $|S'\rangle$, then the signature is valid if and only if

$$|M'\rangle\simeq R_j^\dagger E_k^\dagger|S'\rangle, \tag{3}$$

where $A\simeq B$ means that A and B are the same up to global phase. In other words, for each $j\in\mathbb{Z}_2$ and $k\in\mathbb{Z}_4$, there exists a real number θ_{jk} such that

$$|M'\rangle=e^{i\theta_{jk}}R_j^\dagger E_k^\dagger|S'\rangle. \tag{4}$$

We note that one can judge with high probability whether or not the two states $|M'\rangle$ and $R_j^\dagger E_k^\dagger|S'\rangle$ are equal up to global phase, by exploiting the swap test [10] for appropriate number of copies of the states.

We remark that all quantum encryptions are not useful for AQS schemes. In particular, it has been shown that if quantum encryption consists of only the Pauli operators σ_x, σ_y, σ_z and the identity operator I, then the AQS schemes with the quantum encryption are not secure against receiver's forgery attack [6, 7, 9]. In order to recover the security of the AQS schemes, the following form of quantum encryption E_k was proposed [6]: For $k\in\mathbb{Z}_4$, $E_k=V\sigma_kW$, where V and W are proper unitary operators, $\sigma_0=I$, $\sigma_1=\sigma_x$, $\sigma_2=\sigma_y$, and $\sigma_3=\sigma_z$. However, if the above encryption is employed then, as seen in Eq. (2), the unitary operator V in the signature $|S\rangle=V\sigma_kWR_j|M\rangle$ can always be eliminated by an attacker's applying the inverse of V. Therefore, the quantum encryption proposed in Ref. [6] can be reduced to the encryption

$$E_k=\sigma_kW, \tag{5}$$

for $k\in\mathbb{Z}_4$. This unitary operator W is called an *assistant unitary operator* of the AQS scheme [7].

Let us consider a situation that there exists a non-identity unitary operator Q such that all the operators $R_j^\dagger W^\dagger\sigma_kQ\sigma_kWR_j$ become the identical unitary operator

U up to global phase, regardless of the shared key (j,k), that is, for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$,

$$R_j^\dagger W^\dagger \sigma_k Q \sigma_k W R_j \simeq U. \tag{6}$$

We remark that if $|S\rangle = \sigma_k W R_j |M\rangle$ and the transmitted message-signature pair is $(|M\rangle, |S\rangle)$ then the pair can be forged as $(U|M\rangle, Q|S\rangle)$ since the forged message $U|M\rangle$ and the forged signature $Q|S\rangle$ satisfy the validity condition (3), that is, for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$

$$U|M\rangle \simeq R_j^\dagger W^\dagger \sigma_k Q |S\rangle. \tag{7}$$

It follows that it is possible for the receiver to forge all quantum message-signature pairs in this situation.

Recently, Zhang *et al.* [7] pointed out that if an unitary operator Q satisfies Eq. (6) for some unitary U and W then Q must be one of the Pauli operators. Furthermore, for each Pauli operator σ_l, they characterized the class of the assistant unitary operators W satisfying the following: There exists an unitary U such that

$$R_j^\dagger W^\dagger \sigma_k \sigma_l \sigma_k W R_j \simeq U \tag{8}$$

for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$. From the characterization, one can obtain the class of the W's that provide us with quantum encryptions in which all quantum message-signature pairs cannot be forged.

Now, let us take into account a slightly different situation as the following: For a given assistant unitary operator W, there exist a quantum message $|M_0\rangle$, non-identity unitary Q and unitary U such that

$$R_j^\dagger W^\dagger \sigma_k^\dagger Q \sigma_k W R_j |M_0\rangle \simeq U|M_0\rangle \tag{9}$$

for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$. This implies that the receiver can forge at least one quantum messages and their signatures although all other quantum message-signature pairs cannot be forged. Here, a quantum message satisfying Eq. (9) is said to be *forgeable* in the AQS scheme with an assistant unitary operator W.

In this paper, we show that there does not exist such an AQS scheme which does not include any forgeable quantum message, that is, for every known AQS scheme with the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ and the quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$ as in Eq. (5), there always exists at least one forgeable quantum messages. In this situation, one question naturally arises, such as whether one can construct an AQS scheme without any forgeable quantum message. In this paper, we present an AQS scheme which is a slightly modified version of the above AQS scheme, and numerically show that there exists no forgeable quantum message in our scheme.

II. FORGEABLE MESSAGES IN AQS SCHEMES

Without loss of generality, we may assume that an assistant unitary operator W has the following representation [11]:

$$W = w_0\sigma_0 + iw_1\sigma_1 - iw_2\sigma_2 + iw_3\sigma_3, \tag{10}$$

where $w_j \in \mathbb{R}$, $w_0 \geq 0$ and $\sum_{j\in\mathbb{Z}_4} w_j^2 = 1$. Let

$$\begin{aligned} \alpha &= \frac{1}{2}\left(w_0^2 + w_1^2 - w_2^2 - w_3^2\right) \\ &= w_0^2 + w_1^2 - \frac{1}{2} \\ &= \frac{1}{2} - w_2^2 - w_3^2, \\ \beta &= w_0 w_2 + w_1 w_3, \\ \gamma &= w_0 w_3 - w_1 w_2. \end{aligned} \tag{11}$$

If $\beta = 0$ then it can readily be obtained that

$$\begin{aligned} \sigma_1 W^\dagger \sigma_1 W \sigma_1 |0\rangle &= 2(\alpha - i\gamma)|1\rangle \\ &\simeq -2(\alpha + i\gamma)|1\rangle \\ &= \sigma_3 W^\dagger \sigma_1 W \sigma_3 |0\rangle, \end{aligned} \tag{12}$$

which implies

$$R_j^\dagger W^\dagger \sigma_k \sigma_1 \sigma_k W R_j |0\rangle \simeq \sigma_1 W^\dagger \sigma_1 W \sigma_1 |0\rangle, \tag{13}$$

for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$, since it is clear that

$$\begin{aligned} \sigma_1 W^\dagger \sigma_1 W \sigma_1 &\simeq \sigma_1 W^\dagger \sigma_k \sigma_1 \sigma_k W \sigma_1, \\ \sigma_3 W^\dagger \sigma_1 W \sigma_3 &\simeq \sigma_3 W^\dagger \sigma_k \sigma_1 \sigma_k W \sigma_3, \end{aligned} \tag{14}$$

for all $k \in \mathbb{Z}_4$. Since if we take $Q = \sigma_1$ and $U = \sigma_1 W^\dagger \sigma_1 W \sigma_1$ then Eq. (13) is equivalent to the forgeability condition in Eq. (9), we can say that the qubit message $|0\rangle$ is forgeable in AQS schemes with the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ and a quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$ whose assistant unitary operator W satisfies $\beta = 0$.

We now assume that $\beta \neq 0$, and let $|M_0\rangle$ be a qubit message defined as

$$|M_0\rangle = \frac{1}{\sqrt{\mu^2+1}}\left(\mu|0\rangle + |1\rangle\right), \tag{15}$$

where

$$\mu = \frac{\alpha + \sqrt{\alpha^2+\beta^2}}{\beta}. \tag{16}$$

Then it follows from tedious but straightforward calculation that

$$\sigma_1 W^\dagger \sigma_1 W \sigma_1 |M_0\rangle \simeq \sigma_3 W^\dagger \sigma_1 W \sigma_3 |M_0\rangle, \tag{17}$$

and therefore it can be seen from Eqs. (14) that, for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$,

$$R_j^\dagger W^\dagger \sigma_k \sigma_1 \sigma_k W R_j |M_0\rangle \simeq \sigma_1 W^\dagger \sigma_1 W \sigma_1 |M_0\rangle. \tag{18}$$

This implies that the following theorem holds.

Theorem 1. *Assume that an AQS scheme consists of the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ and a quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$ with an assistant unitary operator W. Then there exist at least one forgeable qubit messages $|M_0\rangle$, that is, there exist a qubit message $|M_0\rangle$ and forgery unitary operators Q and U satisfying Eq. (9) for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$.*

We remark that all qubit messages are forgeable in AQS schemes with the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ and a quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$ whose assistant unitary operator W satisfies $\gamma = 0$ in Eqs. (11), as follows. Let us assume that W is an assistant unitary operator with $\gamma = 0$, then it can easily be shown that

$$\begin{aligned}\sigma_1 W^\dagger \sigma_1 W \sigma_1 &= 2\alpha\sigma_1 - 2\beta\sigma_3 \\ &\simeq \sigma_3 W^\dagger \sigma_1 W \sigma_3. \end{aligned} \tag{19}$$

Thus it turns out that

$$R_j^\dagger W^\dagger \sigma_k \sigma_1 \sigma_k W R_j \simeq \sigma_1 W^\dagger \sigma_1 W \sigma_1, \tag{20}$$

for all $j \in \mathbb{Z}_2$ and $k \in \mathbb{Z}_4$.

III. AQS WITHOUT FORGEABLE MESSAGES

We have shown that, for every assistant unitary operator W, there exist at least one forgeable qubit messages in the AQS scheme with the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ and a quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$. However, we here present an AQS scheme without forgeable qubit messages by slightly modifying the random rotation and selecting a suitable assistant unitary operator, as follows.

In order to get rid of forgeable quantum messages, we first point out that the random rotation $\{R_j\}_{j\in\mathbb{Z}_2}$ in the known AQS schemes is biased, and the biased random rotation may be one of reasons why there exists a forgeable quantum message. Thus we here use an AQS scheme with an unbiased random rotation $\{\tilde{R}_j\}_{j\in\mathbb{Z}_4}$, where $\tilde{R}_j = \sigma_j$ for each $j \in \mathbb{Z}_4$.

We now find one of the most suitable assistant unitary operators which we can consider. In order to find it, we begin with observing one simple case, such as the case that all quantum messages are forgeable in a given AQS scheme with its random rotation $\{\tilde{R}_j\}_{j\in\mathbb{Z}_4}$ and quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$.

In particular, TABLE I shows us what assistant unitary operators W can make all qubit messages forgeable in the AQS scheme, when a forgery attack operator Q, which is in Eq. (6), is one of the Pauli matrices. For example, if $Q = \sigma_1$ then all qubit messages become forgeable when the operator W satisfies two of the three equations, $\alpha = 0$, $\beta = 0$ and $\gamma = 0$, since

$$\begin{aligned}\alpha &= w_0^2 + w_1^2 - \frac{1}{2}, \\ \beta &= w_0 w_2 + w_1 w_3, \\ \gamma &= w_0 w_3 - w_1 w_2, \end{aligned} \tag{21}$$

as seen in Eqs. (11).

If an assistant unitary operator W has at most two non-zero w_j's, then such an operator W satisfies at least one of nine pairs of equations in w_j's which appear in TABLE I, and thus all qubit messages are forgeable in the AQS scheme. Hence we note that at least three w_j's should be non-zero, in order for all qubit messages not to be forgeable. This means that a good candidate for an assistant unitary operator would be an operator far from the identity operator σ_0 (or $e^{i\theta}\sigma_0$) among operators W with at least three non-zero w_j's. Therefore, we regard an operator T defined by

$$T = \frac{i}{\sqrt{3}}\left(\sigma_1 - \sigma_2 + \sigma_3\right) \tag{22}$$

as our best candidate for a suitable assistant unitary operator, since the operator T among those operators is one of the farthest ones from σ_0 with respect to the trace distance.

Q	$W = w_0\sigma_0 + iw_1\sigma_1 - iw_2\sigma_2 + iw_3\sigma_3$
σ_1	$w_0^2 + w_1^2 - 1/2 = w_0w_3 - w_1w_2 = 0$
	$w_0^2 + w_1^2 - 1/2 = w_0w_2 + w_1w_3 = 0$
	$w_0w_3 - w_1w_2 = w_0w_2 + w_1w_3 = 0$
σ_2	$w_0^2 + w_2^2 - 1/2 = w_0w_1 - w_2w_3 = 0$
	$w_0^2 + w_2^2 - 1/2 = w_0w_3 + w_1w_2 = 0$
	$w_0w_1 - w_2w_3 = w_0w_3 + w_1w_2 = 0$
σ_3	$w_0^2 + w_3^2 - 1/2 = w_0w_2 - w_1w_3 = 0$
	$w_0^2 + w_3^2 - 1/2 = w_0w_1 + w_2w_3 = 0$
	$w_0w_2 - w_1w_3 = w_0w_1 + w_2w_3 = 0$

TABLE I: Characaterization of assistant unitary operators W which make all qubit messages forgeable in AQS schemes with its random rotation $\{\tilde{R}_j\}_{j\in\mathbb{Z}_4}$ and quantum encryption $\{\sigma_k W\}_{k\in\mathbb{Z}_4}$ when a given forgery attack Q is one of the Pauli matrices: For each forgery attack σ_j, if an assistant unitary operator W satisfies one of the three pairs of equations in w_j's then all qubit messages become forgeable.

From now on, we numerically investigate the forgeability of our AQS scheme with its random rotation $\{\tilde{R}_j\}_{j\in\mathbb{Z}_4}$ and quantum encryption $\{\sigma_k T\}_{k\in\mathbb{Z}_4}$.

Let Q be an arbitrary forgery attack operator defined as

$$Q = q_0\sigma_0 + iq_1\sigma_1 - iq_2\sigma_2 + iq_3\sigma_3, \tag{23}$$

where q_j are real numbers with $q_0 \geq 0$ and $\sum_{j\in\mathbb{Z}_4} q_j^2 = 1$, and let d_Q be its trace distance from the identity operator σ_0, that is,

$$d_Q = \|\sigma_0 - Q\|_1 = |1 - q_0| + |q_1| + |q_2| + |q_3|, \tag{24}$$

where $\|\cdot\|_1 = \mathrm{tr}|\cdot|$ is the trace norm. For each qubit message $|M\rangle$, let $P_{Q,|M\rangle}$ be the probability with which a forgery attack can be detected by using the swap test once, then it follows from Ref. [10] that

$$P_{Q,|M\rangle} = 1 - \frac{1}{2^9}\sum_{j,k,j',k'\in\mathbb{Z}_4}\left(1 + |\langle M|\Delta_{jkj'k'}|M\rangle|^2\right), \tag{25}$$

where

$$\Delta_{jkj'k'} = \sigma_j T^\dagger \sigma_k Q^\dagger \sigma_k T \sigma_j \sigma_{j'} T^\dagger \sigma_{k'} Q \sigma_{k'} T \sigma_{j'}, \tag{26}$$

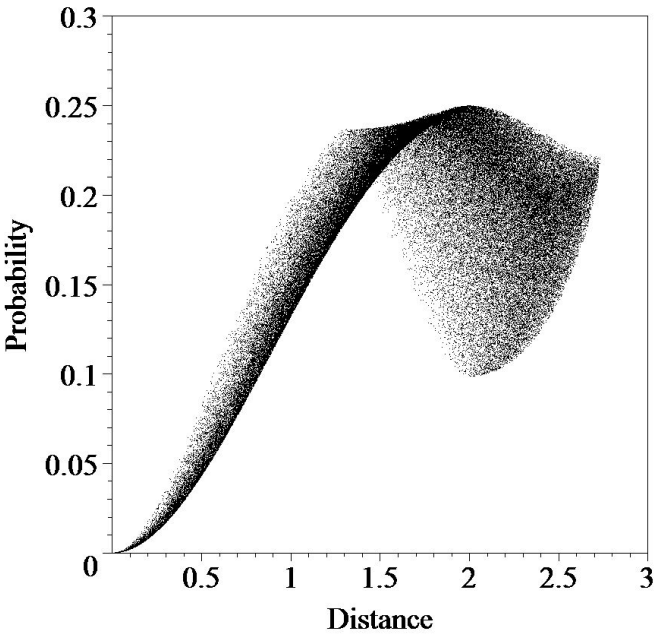

FIG. 1: The minimal probability to detect the forgery attack among all qubit messages by exploiting the swap test once, plotted against the distance from the identity operator σ_0 for 100,000 randomly chosen unitary operators Q in Eq. (23): When the distance is 2, that is, when the operator is one of the Pauli matrices, the minimal probability to detect a forgery attack, $P_{\min}$, has a local minimum.

and let P_Q be the minimum of $P_{Q,|M\rangle}$ taken over all qubit messages $|M\rangle$, then the value of P_Q can efficiently be calculated for a given Q. For 100,000 randomly chosen Q, the points (d_Q, P_Q) are plotted in FIG. 1.

For each $0 \leq d \leq 1 + \sqrt{3}$ [12], let $P_{\min}(d)$ be the minimum of P_Q's taken over all unitary operators Q with $d_Q = d$, then $P_{\min}(d)$ can be represented as the greatest lower bound of the points (d_Q, P_Q) in FIG. 1, from which we can furthermore see that $d = 0$ if and only if $P_{\min}(d) = 0$, that is, a forgery attack operator is not the identity operator up to global phase if and only if its detection probability is strictly positive. This directly implies that there does not exist any forgeable messages in this AQS scheme.

In addition, we can see from FIG. 1 that, for a forgery attack operator with distance less than 3/2, the minimal probability to detect the attack is small if and only if the operator is close to the identity operator. Therefore, we can obtain that since, by performing sufficiently large number n of swap tests for $n + 1$ copies of the message-signature pairs, the maximal probability not to detect a forgery attack, $(1 - P_{\min}(d))^n$, exponentially tends to zero, one can detect any forgery attack to arbitrary precision in our AQS scheme.

IV. CONCLUSION

We have considered forgeable quantum messages in AQS schemes, and have shown that there exists at least one forgeable quantum message-signature pairs for all known AQS schemes. Moreover, we have presented our AQS scheme with the random rotation $\{\tilde{R}_j\}_{j\in\mathbb{Z}_4}$ and quantum encryption $\{\sigma_k T\}_{k\in\mathbb{Z}_4}$, and have numerically shown that there does not exist any forgeable quantum messages in our AQS scheme.

However, since our scheme uses more random rotation operators than the previous ones, it needs users' more key strings shared in advance, and plenty of copies of the message-signature pairs should be required, in order to detect a forgery attack operator quite close to the identity operator. This means that our scheme demands quite a few both classical and quantum resources. In addition, other security problems including the non-repudiation has not been analyzed. Hence, we cannot say that our scheme is practically useful.

Nevertheless, we can still say that our AQS scheme is helpful to improve theoretical works related to AQS, since one can at least show the existence of AQS schemes without forgeable quantum messages by means of our scheme. Therefore, our result could be a basic reference for both theoretical and practical applications of AQS, such as finding a practically useful AQS scheme without forgeable messages, and would also be helpful to strengthen theories in quantum cryptography.

Acknowledgments

This work was supported by the IT R&D program of the Ministry of Knowledge Economy [Development of Privacy Enhancing Cryptography on Ubiquitous Computing Environment]. T.K. was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2012-0006691), and S.L. was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2012-003441).

[1] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02), pp. 449–458, 2002.

[2] D. Gottesman and I. L. Chuang, quant-ph/0105032.

[3] G. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002).

[4] Q. Li, W. H. Chan, and D.-Y. Long, Phys. Rev. A **79**, 054307 (2009).

[5] X. Zou and D. Qiu, Phys. Rev. A **82**, 042325 (2010).

[6] J. W. Choi, K.-Y. Chang, and D. Hong, Phys. Rev. A **84**, 062330 (2011).

[7] K. Zhang, D. Li, and Q. Su, Phys. Scr. **89**, 015102 (2014).

[8] P. O. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).

[9] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, Phys. Rev. A **84**, 022344 (2011).

[10] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[11] Any 2×2 unitary operator can be expressed as the form of Eq. (10) up to global phase.

[12] We note that $\max_Q \|\sigma_0 - Q\|_1 = \|\sigma_0 - T\|_1 = 1 + \sqrt{3}$, where the maximum is taken over all Q's in Eq. (23).