Forgeable quantum messages in arbitrated quantum signature schemes

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

[1] Institute of Mathematical Sciences,
Ewha Womans University, Seoul 120-750, Korea

[2] Fusion 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

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 [3–13], and the signature schemes are called the arbitrated quantum signature schemes.

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 work, we consider one situation, which is slightly different from the forgery problem, that we check whether at least one quantum message with signature can be forged in a given scheme, although all the messages cannot be forged. If there exist only a finite number of forgeable quantum messages in the scheme then the scheme can be secure against the forgery attack by not sending the forgeable quantum messages, and so our situation does not directly imply that we check whether the scheme is secure against the attack. But, if users run a given scheme without any consideration of forgeable quantum messages then a sender might transmit such forgeable messages to a receiver, and an attacker can forge the messages if the attacker knows them in such a case. Thus it is important and necessary to look into forgeable quantum messages.

We here show that there always exists such a forgeable quantum message-signature pair for every known scheme with quantum encryption and rotation, and show that there exists an arbitrated quantum signature scheme without any forgeable quantum message-signature pairs.

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

[2] Gottesman D and Chuang I L 2001 arXiv:quant-ph/0105032

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

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

[5] Cao Z and Markowitch O 2009 Int. J. Quantum Inform. **07** 1205

[6] Zou X and Qiu D 2010 Phys. Rev. A **82** 042325

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

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

[9] Li Q, Li C, Wen Z, Zhao W and Chan W H 2013 J. Phys. A: Math. Theor. **46** 015307

[10] Zhang K -J, Zhang W -W and Li D 2013 Quantum Inform. Proc. **12** 2655

[11] Su Q and Li W -M 2013 Int. J. Theor. Phys. **52** 3343

[12] Zhang K -J, Qin S -J, Sun Y, Song T -T and Su Q 2013 Quantum Inform. Proc. **12** 3127

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