JAIST Repository
https://dspace.jaist.ac.jp/

Title	n-state quantum coin flipping protocol
Author(s)	Waseda, A.; Soshi, M.; Miyaji, A.
Citation	Proceedings of the International Conference on Information Technology: Coding and Computing, 2005. ITCC 2005.: 776-777
Issue Date	2005-04
Type	Conference Paper
Text version	publisher
URL	http://hdl.handle.net/10119/4388
Rights	Copyright (c)2005.IEEE. Reprinted from Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), Vol. II(2005), 776-777. This material is posted here with permission of the IEEE. Such permission of the IEEE does not in any way imply IEEE endorsement of any of JAIST's products or services. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE by writing to pubs-permissions@ieee.org. By choosing to view this document, you agree to all provisions of the copyright laws protecting it.
Description	

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

n-state quantum coin flipping protocol

Atsushi Waseda, Masakazu Soshi and Atsuko Miyaji
School of Information Science
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY
1, 1 Asahidai, Nomi, Isikawa, Japan
{a-waseda, soshi, miyaji}@jaist.ac.jp

Abstract

We propose the n-state quantum coin flipping protocol by generalizing the three states protocol proposed by Ambainis [2]. Furthermore, we conduct security analysis on our protocol and show that in our protocol we can reduce the bias of one player arbitrarily, but at the cost of increase of the bias of the other.

1 Introduction

Quantum cryptography, which is based on the principles of quantum physics, has been investigated extensively. In connection with this, many studies have so far been made on a *quantum coin flipping protocol*. This is because it is one of the most important cryptographic primitives to construct more general secure protocols. As sated above, most cryptographic primitives of modern cryptography could be invalidated in a future with the advent of computer systems with vast computational powers. Therefore it is of critical importance to develop their quantum versions.

When two players execute a *quantum coin flipping protocol* to reach an agreement on a value c, if one of them is dishonest, then $Prob(c = 0) \leq \frac{1}{2} + \epsilon$ and $Prob(c = 1) \leq \frac{1}{2} + \epsilon$. The value ϵ is called a *bias*. Lo and Chau show that it is impossible to construct quantum protocols with $\epsilon = 0$ [5]. An example of the quantum coin flipping is a protocol proposed by Ambainis [2]. The bias of the protocol of Ambainis is $\epsilon = 0.25$.

Therefore, we propose the n-state quantum coin flipping protocol by generalizing the three states protocol proposed by Ambainis [2]. Furthermore, we conduct security analysis on our protocol and show that our protocol can reduce the bias of one player arbitrarily, but at the cost of increase of the bias of the other. Thus, our protocol makes it possible to provide security suitable for various situations.

Now we describe the organization of this paper. In section 2, we define how to assign n states and propose the n-state quantum coin flipping protocol. In section 3, we evaluate the bias of dishonest Alice or Bob. In section 4, we discuss several aspects of our proposed protocol. Finally we conclude this paper in section 5.

2 Our Proposal

We propose the n-state quantum coin flipping protocol. First, we start by constructing a binary tree, which describes how quantum states in our protocol are constituted. Next we present our proposed coin flipping protocol.

2.1 Construction of quantum states

Now we propose a general method to construct quantum states in n-state qubits for quantum coin flipping protocols.

1. $t \in \{0, \ldots, n\}$ is chosen at random under the condition $n - t \equiv 0 \pmod 2$.
2. Form a binary tree whose height is $s = t + \frac{n-t}{2}$. Each leaf of the binary tree represents a distinct sequence of bits $b, x_1, \ldots, x_{s-1}$.
3. One of n states $|0\rangle$, $|1\rangle$, ..., $|n-1\rangle$, or its negative is assigned as a label to each vertex (except for the root) of the tree, depending on the level (i.e., distance from the root) of the vertex.
   (a) Level 1.
      i. If $t = 0$, $|0\rangle$ is assigned to the vertex and $|1\rangle$ to the other.
      ii. Otherwise, $|0\rangle$ is assigned to both.
   (b) Level $2 \leq \ell \leq t$. $|\ell - 1\rangle$ is assigned to the vertex, and $-|\ell - 1\rangle$ to its sibling (the other vertex of the same parent of the vertex.).
   (c) Level $t < \ell \leq s$. If the vertex resides in the right half of the tree, $|t+2(\ell-t-1)\rangle$ is assigned to the vertex, and $-|t+2(\ell-t-1)\rangle$ to its sibling. And

Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05)
0-7695-2315-3/05 $ 20.00 **IEEE**

IEEE COMPUTER SOCIETY

in the left half of the tree, $|t+2(\ell-t-1)+1\rangle$ is assigned to the vertex, and $-|t+2(\ell-t-1)+1\rangle$ to its sibling.

4. Let $|y_i\rangle$ be labels of vertices on the path from the root to leaf $b, x_1, \ldots, x_{s-1}$. The quantum state $|\phi_{b,x_1,\ldots,x_{s-1}}\rangle$ is expressed as

$$|\phi_{b,x_1,\ldots,x_{s-1}}\rangle = \frac{1}{\sqrt{s}} \sum_{i=1}^{s} |y_i\rangle. \quad (1)$$

2.2 The protocol

Now, our n state quantum coin flipping protocol is given as follows.

1. Alice selects $b, x_1, \ldots, x_{s-1} \in \{0,1\}$ in a uniformly random manner and sends $|\phi_{b,x_1,\ldots,x_{s-1}}\rangle$ to Bob.
2. Bob picks a uniformly random $b' \in \{0,1\}$ and sends b' to Alice.
3. Alice sends $b, x_1, \ldots, x_{s-1}$ to Bob.
4. Bob verifies if the state that he received from Alice in the first step is $|\phi_{b,x_1,\ldots,x_{s-1}}\rangle$. If the result of the measurement is not $|\phi_{b,x_1,\ldots,x_{s-1}}\rangle$, he considers that Alice has cheated and aborts the protocol.
5. Otherwise, the outcome of the flipping is $c = b \oplus b'$.

3 Security Analysis

We evaluate the probability of dishonest player obtaining $c = 0$. The attack model is the same as that of [2].

If Alice chooses $b = 0$, she sends a mixed state ρ^0 that is equal to every state $|\phi_{0,x_1,\ldots,x_{s-1}}\rangle$ with probability $\frac{1}{2^{s-1}}$. Otherwise (Alice choose $b = 1$), she sends ρ^1 that is equal to every state $|\phi_{1,x_1,\ldots,x_{s-1}}\rangle$ with probability $\frac{1}{2^{s-1}}$. We define $X = \frac{t}{n}$, and analyze our protocol using X. X means the measure of nonorthogonal between ρ_0 and ρ_1.

First, we estimate the probability of dishonest Bob achieving $b \oplus b' = 0$.

Lemma 1 *The bias for Bob is* $\epsilon_{Bob} = \frac{1}{4} - (\frac{3}{4} - \frac{1}{1+X})$.

Furthermore, since either of ρ^0 or ρ^1 is transmitted for the coin of Alice, the accessible information m should not be greater than 1 [4]. But by Lemma 2, the value of m obtained in the equation above satisfies this requirement.

Lemma 2 *The accessible information* m *of* ρ *which is transmitted by Alice is bounded by* $m \leq \frac{1-X}{1+X} \leq 1$.

Secondly, we bound the probability of dishonest Alice achieving $b \oplus b' = 0$.

Lemma 3 *The bias for Alice is* $\epsilon_{Alice} = \frac{1}{4} + (\frac{3}{4} - \frac{1}{1+X})$.

4 Discussion

In our protocol, we can choose n and t arbitrarily and give any values of biases to Alice or Bob. In particular, we can reduce the bias of one player arbitrarily, but at the cost of increase of the bias of the other. Typical cases of X, ϵ_{Alice} and ϵ_{Bob} are summarized in Table 1.

Table 1. Biases in typical cases

X	0	$\frac{1}{3}$	1
ϵ_{Alice}	0	$\frac{1}{4}$	$\frac{1}{2}$
ϵ_{Bob}	$\frac{1}{2}$	$\frac{1}{4}$	0

For example, if $X = \frac{1}{3}$, then ϵ_{Alice} and ϵ_{Bob} become the same, i.e., $\frac{1}{4}$. This is exactly the case Ambainis considers. Needless to say, our generalized n-state protocol can express it as a special case.

5 Conclusion

We propose the n-state quantum coin flipping protocol. The biases of Alice and Bob are $\epsilon_{Alice} = \frac{1}{4} + (\frac{3}{4} - \frac{1}{1+X})$ and $\epsilon_{Bob} = \frac{1}{4} - (\frac{3}{4} - \frac{1}{1+X})$, respectively. This means that our protocol can reduce the bias of one player arbitrarily, but at the cost of increase of the bias of the other. Thus, our generalized n-state quantum protocol makes it possible to provide security suitable for various situations.

6 Acknowledgment

This research is conducted as a program for the "21st Century COE Program" and the "Fostering Talent in Emergent Research Fields" in Special Coordination Funds for Promoting Science and Technology by Ministry of Education, Culture, Sports, Science and Technology.

References

[1] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao. Quantum bit escrow. In *Proceedings of STOC'00*, pages 705–714, 2000.
[2] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. quant-ph/0204022.
[3] A. Ambainis, N. Buhrman, Y. Dodis, and H. Röhrig. Multiparty quantum coin flipping. quant-ph/0304112.
[4] A. Kent. Quantum bit string commitment. *Phy. Rev. Lett.*, 90(237901), 2003.
[5] H. Lo and H. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177–187, 1998.

IEEE COMPUTER SOCIETY