Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Quantum Key Agreement through Information Reconciliation and Privacy Amplification

Ajit Singh[1]
[1]*CSE, SES, BPSMV, Khanpur Kalan, Sonepat*
ghanghas_ajit@rediffmail.com

Swati Aggarwal[2]
[2]*CSE, SES, BPSMV, Khanpur Kalan, Sonepat*
swati.aggarwal@rocketmail.com

***Abstract*— This paper considers the problem of security in practical implementation of Quantum Key Agreement applying the concept of Information Reconciliation and Privacy Amplification targeted towards the computer science community. Firstly, a scheme is proposed which is operable in presence of noise using procedure called 'entanglement purification' on Bell states to detect presence of adversary and then a protocol that minimizes the entropy loss and thus increasing the length of shared key between two communicating parties in presence of active computationally unbounded adversary.**

***Keywords*— Quantum Key Distribution, Entanglement purification, Bell states, Privacy amplification, Entropy loss**

I. INTRODUCTION

To carry out Quantum key distribution[4] in Quantum cryptography[1-3] between two communicating parties, Alice and Bob, *Quantum privacy algorithm*(QPA) which is iterative in nature and based on Bell's Theorem[4,5] is presented which is secure in presence of both noise and eavesdropping using an element 'entanglement purification' procedure. Earlier existing protocols are inoperable in presence of noise and transmission is suspended whenever eavesdropper is detected. There was no way of distinguishing entanglement with an eavesdropper from entanglement with environmental noise.QPA can be performed by Alice and Bob by a sequence of local operations over a public channel at distant locations. It imparts small bound on adversary, Eve, information which can be extracted from string. QPA allows Alice and Bob to generate a pair of qubits in a state which is close to pure, maximally entangled $|\phi^+\rangle$ and entanglement with environment is arbitrarily low where:

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

These are called Bell states described by density operators form basis for state space of qubit pair or entangled photons. Then, a second approach is considered in which both parties share same weak secret w(which is not a uniform random key) and Eve has some partial information about w, so it is assumed that w has some entropy[7,8] from Eve's view. Now, goal is to convert this non-uniform w to uniform shared secret R but still there is the requirement to increase its length to impose difficulty for adversary by reducing entropy loss which is the difference between the entropy of w and the length of R. So, entropy loss should be small because entropy in R can only come from w and if more entropy loss will occur then randomness in R will be less.

II. METHODOLOGY

A. *First approach*

Scenario is such that Eve in addition of interacting with all qubits used by Alice and Bob for communication, can also prepare qubit pairs and send one qubit from each pair to communicating parties.

Iterative quantum algorithm [5] starts with collection of qubit pairs in mixed state and if performed with accuracy, some will be discarded and some will be selected which then converged to $|\phi^+\rangle\langle\phi^+|$ using density matrix. Before proving the purity of qubit pairs, it is necessary to mention that Alice and Bob use two rotations and quantum controlled-not operation in which CNOT gate flips second(target) qubit if and only if first qubit (control qubit) =1.That is, .

Table I
CNOT gate operation

Before		After	
Control	Target	Control	Target
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

.

1) *Rotation Operation:* Now, consider $\rho^{\wedge}$ and $\rho^{\wedge}$' be density operators of two qubit pairs and Alice performs a unitary operation using Hadamard gate[6] which operates on single qubit at a time.

$$H(|0\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

$$H(|1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|1\rangle - i|0\rangle)$$

On each qubit pair Bob performs inverse operation.

$$H(|0\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

$$H(|1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|1\rangle + i|0\rangle)$$

And if considering that computation basis are eigen values of z components of spins and the qubit spin is ½ particles, then both above operations corresponds to rotations π /2 and - π /2 about x axis respectively.

2) CNOT Operation: After this rotation operation, Alice and Bob both perform two instances of CNOT operation

control target control target

$|a\rangle \quad |b\rangle \rightarrow |a\rangle \quad |a * b\rangle \quad (a, b) \in \{0, 1\}$,

When one $\hat{\rho}$ comprise two control qubits and $\hat{\rho}$, comprises two target qubits then Alice and Bob measure target qubits in z components of target spins. If results coincide, control pairs will be accepted and it will be kept for next round and target bits will be omitted. And, otherwise, if outcomes do not coincide, discard both pairs.

3) Special Case: Now, a special case is considered as in [16] where each pair is in state $\hat{\rho}$ and joint state of two pairs is simple product $\hat{\rho} * \hat{\rho}$. To map above stated operators consider them in density matrices form as below:

$$\begin{pmatrix} A, 0, 0, 0 \\ 0, B, 0, 0 \\ 0, 0, C, 0 \\ 0, 0, 0, D \end{pmatrix} \Rightarrow \begin{pmatrix} (A^2+B^2)/N, 0, 0, 0 \\ 0, 2CD/N, 0, 0 \\ 0, 0, (C^2+D^2)/N, 0 \\ 0, 0, 0, 2AB/N \end{pmatrix}$$

Figure 1: Mapping of density matrices

So, if control qubits are returned, their density operator $\hat{\rho}$ will have diagonal elements of $\hat{\rho}$, then

$$A = \frac{A^2+B^2}{N}$$

$$B = \frac{2CD}{N}$$

$$C = \frac{C^2+D^2}{N}$$

$$D = \frac{2AB}{N}$$

where, $N = (A + B)^2 + (C + D)^2$, (probability that Alice and

Bob obtain coinciding results in target pair measurement).If above matrix is written in Bell states then diagonal elements:

$$A=\langle\phi^+|\hat{\rho}|\phi^+\rangle$$
$$B=\langle\psi^-|\hat{\rho}|\psi^-\rangle$$
$$C=\langle\psi^+|\hat{\rho}|\psi^+\rangle$$
$$D=\langle\phi^-|\hat{\rho}|\phi^-\rangle$$

So, this procedure uses two rotations and CNOT operation as stated above.

Here, diagonal element A is called the "fidelity" which is the probability that qubit will pass a test for being in state $|\phi^+\rangle$ (desired result).Since this is a pure state and none of the surviving pairs are entangled with any other system in the environment. Thus, it is required to drive the fidelity to 1 i.e.; other three diagonal elements are 0.So, if procedure is performed iteratively on an ensemble of these pairs of pairs, then A□ ,B□ ,C□ ,D□ give average diagonal entries of surviving pairs. Thus, surviving pairs will converge to pure state $|\phi^+\rangle\langle\phi^+|$ if average A□ is driven to 1. Therefore, by iterating QPA map, pair approaches to pure state $|\phi^+\rangle$.

If however, input pairs have different matrices or states i.e.; $\hat{\rho}$ and $\hat{\rho}$' will be different. $\hat{\rho}$ corresponds to {A,B,C,D} and $\hat{\rho}$' corresponds to{A □ ,B □ ,C □D □ }.Then, diagonal elements of retained control pairs will on average are:

$$A = \frac{AA' + BB'}{N}$$

$$B = \frac{CD + CD'}{N}$$

$$C = \frac{CC' + DD'}{N}$$

$$D = \frac{AB' + AB}{N}$$

where N = (A+ B)(A'+B') + (C+D)(C'+D').

This technique is rather wasteful in terms of eliminating particles i.e.; at least one half of particles are lost at every iteration.

If в is denoted as a class of pure, maximally entangled states, then condition that $\hat{\rho}$ can be purified using QPA procedure is $\max_{\phi\in B}\langle\phi|\hat{\rho}|\phi\rangle > \frac{1}{2}$.

B. Second Approach:

The above stated method is to detect presence of Eve in transmission of key. That is, if convergence is not obtained then it is concluded that there presence of eavesdropper and communication is aborted. Suppose, if Eve provides entangled pairs then the QPA procedure may or may not converge to pure states $|\phi^+\rangle < \phi^+|$. So, the above method could be made more reliable if now let Alice and Bob already share same secret key w through information reconciliation process[9] and active computationally unbounded adversary Eve have partial i.e.; incomplete knowledge about w, so it is assumed that w has entropy from Eve view. The goal for Alice and Bob is to distil highly random shared secret key from partial R about which Eve has no information. That is, to convert non uniform secret w into a uniformly distributed string R (shared key) of maximum length. As no computational assumptions are made, so entropy in R can only come from w. And entropy (called Shannon entropy) is a measure of uncertainty of random variable and takes its maximum if and only if random variable has uniform distribution. So, security of privacy amplification [10, 11] is proved by showing Shannon entropy of final key conditioned on Eve's information is maximal except for small loss. So, entropy loss should be small during execution which leads R to be of maximum length. Best previous results have entropy loss of $\Theta(k^2)$, k is security parameter, but now entropy loss, linear in security parameter has been obtained.

The distilled random string through extractor or by hash function should have min-entropy H_∞. [7]

Definition 1: A random variable X has min entropy k, denoted $H_\infty(X) = k$, if

$$\max \Pr[X=x] = 2^{-k}$$

Strong extractors produce outputs of almost maximal min-entropy. So, R should be statistically close to uniform where 2^{-k} is considered as the statistical distance between distribution of R and uniform distribution.

1) Earlier Protocol: In [12] authentication protocol was explained through interactive version of robust fuzzy

extractor which generalizes authentication in Renner and Wolf [13].Authentication protocol of [12] works by authenticating bits of message m one by one from Alice to Bob. Steps are:

- For each bit of m, Bob sends Alice, a random extractor seed as a kind of catalyst.
- Then Alice using Bob's seed on input w responds by sending extractor output if bit=1 received in m. And, in addition to extractor output also sends seed of her own.
- Then, Bob responds by applying extractor to w using Alice seed without concerning value of m Now, 1-bit of extractor output results in $\Theta(k)$ entropy loss and each extractor output is k bits long so overall entropy loss is $\Theta(k^2)$.

For security reasons, in this protocol it is required that Eve has to respond with at least one extractor output on her own without any interaction to both communicating parties. As extractor output is a nearly-uniform k-bit string, Eve cannot succeed with probability much higher than 2^{-k}.

2) *Analysis:* Intuition for the security of above protocol lies in knowledge of Bob about the length of message λ_m as well as wt(m) and if Eve were to insert 0 bits or modify 1 as 0 bit, then she have to either have to remove 0 bits or insert 1 bits. And this procedure of removal or addition requires answering a random challenge of Alice (Bob) which Eve cannot perform with probability $>2^k$.Also, entropy loss is $\Theta(\lambda_m k)$ in authentication protocol and $\Theta(k^2)$ in [12].

As in [12],the extractor output is MAC key, and it requires to shorten this length to be a constant number of bits as, then only $\Theta(1)$ bits of entropy for every bit of m will be lost and $\Theta(k)$ entropy loss will be obtained. And also, probability of success of Eve is constant.

3) Improved Version: If it could be ensured that Eve must respond with several extractor [14, 15] outputs on her own, then it could be shown that success probability is 2^{-k} which can be obtained by encoding message m in special error-detecting code of distance $\Theta(k)$.Also, now for Eve to avoid detection she must introduce $\Theta(k)$ errors and so it is required from Eve side to come up with $\Theta(k)$ extractor output on her own. The code required is to be a polynomial-time encodable and not necessarily polynomial-time decodable. For message m of length λ_m and if there are two strings c and c' of length λ_c, let EditDis(c, c □) denote edit distance between c and c' i.e.; number of single bit insert and delete operations required to change string c to c'[16].

Definition 2: *Let m* ϵ $\{0, 1\}^{\lambda m}$. For some constant $0<e_A<1$, a function Edit(·):$\{0,1\}^{\lambda m} \rightarrow \{0,1\}^{\lambda c}$, is a ($\lambda_m$, e_A, ρ)-error-detecting code for edit errors, if $\rho\lambda_c = \lambda_m$ and satisfies following properties:

- c = Edit(m) can be computed in polynomial (in λ_m)time, given m, for all m $\in \{0,1\}^{\lambda m;}$
- For any m, m' $\in \{0, 1\}^{\lambda m}$ with m ≠ m', EditDis (c', c) > $e_A \lambda_c$, where c = Edit (m) and c'=Edit (m').

And, $\rho = \frac{\lambda m}{\lambda c}$ called rate of code.

It is required that Alice first encode m in an error-detecting code for 4*k* edit errors instead of authenticating the bits of m as in [12,13] because authentication of bits is done bit-by-bit and Eve can change m by insertion, deletion or modification of individual bits from 0 to 1 or from 1 to 0 but it is required from Eve side to guess an extractor output on a fresh random seed because as stated in[12] length of m and number of 1s in m are known already to both Alice and Bob before starting communication. So, Eve can create edit errors in message but at least a quarter of errors must be introduced. Also, the length of codeword must still remain linear in the length of m.

THEOREM 1: Let k be the security parameter. Let Edit (·) be a (4(k + 1), e_A, ρ) error-detecting code for constants $0 < e_A, \rho < 1$. Let Ext be a (h_w, t, τ, $2^{-\tau}$)-strong extractor with $\tau = \frac{\rho}{eA} + 1$.Then there exists an efficient (h_w, k)-interactive authentication protocol for messages of length 4(k + 1) with entropy loss $\frac{8\tau(k+1)}{\rho}$. The protocol works as long $h_w \geq \frac{8\tau(k+1)}{\rho} + t + k + 1$.

Given e_A, ρ and τ are constants and using the results of [12], the message authentication protocol is converted to privacy amplification protocol, hence obtaining the corollary to Theorem stated above.

COROLLARY 1: There exists an efficient (h_W, λ_k, 2^{-k}, ϵ) privacy amplification protocol with entropy loss O (k).The length of the extracted key $\lambda_k = h_W - 2\log\frac{1}{\epsilon} - O(k)$.

4) Improved Authentication Protocol: If Eve must respond to many ($\Theta(k)$) fresh random challenges translating success probability to 2^{-k},then Alice have to transmit message c=Edit(m) which is verified by Bob to be a valid codeword.

For protocol let:

K = security parameter

h_W = min entropy

m=message m $\in \{0, 1\}^{\lambda m}$.

λ_w = Alice and Bob share λ_w -bit secret w $\in$ W with h_W.

Ext= average–case (λ_w, t, τ, $2^{-\tau}$) strong extractor with seed length q bits for some constant t and τ.

Edit (·) = be a (λ_m, e_A, ρ) error-detecting code for constants $0< e_A,\rho<1$,such that Hamming weight of all code words is the same(let wt(c)).

Protocol NewAuth (w, m):

1. Alice sends Bob the message m. Let the message received by Bob be m'.
2. For all responses received, Alice and Bob execute protocol Auth(w,c) where c=Edit(m),using average-case strong extractor Ext taking seed as input.
3. Bob computes Edit(m').Let c' be string received by Bob. And if,

   c'≠ Edit(m')

   Then Bob rejects. Otherwise, Bob accepts m' as the message received.

Instead of proving this error detecting code technique through induction argument[12] because in this if Eve is successful in changing any bit of the message send to Bob by Alice, then Eve has to respond to a random challenge on her own but here it is required to keep track of how

many random challenges Eve can respond. As it is needed to precisely characterize how many extractor outputs Eve must have taken in relation to the number of bits modified, so here the entire protocol transcript is viewed as a string of literals from Eve point of view in which each literal represent an interaction of Eve with either Alice or Bob.

In this string representation, two message interactions happen occurring between Alice and Eve or between Bob and Eve as a roundtrip. In any round i, Eve's interaction with any Alice (Bob) consists of Eve's sending challenges and extractor output in response to challenge issued by Alice or Bob in previous rounds. Then Alice (Bob) sends Eve a challenge and response to received challenge in previous rounds. Let these roundtrips be denoted by two literals a and b between (Alice and Eve) and (Bob and Eve) respectively. Any literal is called costly literal if in real run of the protocol Eve would have to respond a fresh random challenge on her own in the round trip corresponding to the costly literal. This string representation is necessary to stress on points in protocol where Eve would have to respond to a fresh random challenge. It allows capturing all the information including the order in which Eve interacted with the honest parties. Now consider the following to obtain the desired results:

THEOREM 2: Let E be a string consisting of a_0, b_0, a_1, b_1 literals holding property that number of times each literal appears in string E should be same. Also let E' be new string and number of costly literals in E be at most L .Then the edit distance between E and E' is at most 4L.

COROLLARY 2: Let Alice and Bob execute protocol Auth in the presence of an active adversary Eve. Let m_A denote the message sent by Alice and let m_B denote the message received by Bob. Let the edit distance between m_A and m_B be at least 4L. Then Eve must have responded to at least L fresh random challenges on her own.

LEMMA1: Assume $H_{\infty}(w \mid Tr_{\mu}) \geq k + 1 + t$. Then, Pr [Eve successfully responds to μ fresh random challenges] $\leq 2^{(-\mu(\lambda r-1)} + 2^{-(k+1)}$.

5) Analysis To calculate entropy loss, message c of length $\frac{4(k+1}{\rho}$ needs to be authenticated. Authentication of 0 bit requires Eve to face 1 extractor response and authenticating 1 bit needs two extractor responses. And length of each extractor response is τ so entropy loss will be at most $2\times \frac{4(k+1)}{\rho} \times \tau = \frac{8\tau (k+1)}{\rho}$ proving theorem. To break this security, if Eve have to make Bob accept a message m'≠ m, then from Definition 2, she must make Bob accept a message c'≠ c in Auth(w, c) where edit distance between c' and c is greater than $e_A\lambda_c = \frac{4eA(k+1)}{\rho}$. Also, from Corollary 2, Eve must have to respond to more than $\frac{eA(k+1)}{\rho}$ fresh random challenges with probability of at most $p = 2^{\frac{-eA(k+1)}{\rho}(\tau+1)} + 2^{-(k+1)}$ from Lemma 1.So, $\tau=\frac{\rho}{eA}+1$ and $p< 2^{-k}$ is achieved.

III. CONCLUSIONS

This paper is presented to find the efficient method of distributing the quantum key between two parties securely by using entanglement purification procedure based on Bell states in which

$$\max_{\phi \in B} \langle \phi | \hat{\rho} | \phi \rangle \frac{1}{2}.$$

condition should be met for the state $\hat{\rho}$ to be purified by QPA procedure.

And, also to minimize the entropy loss through edit distance codes and hence increasing the length of shared random key. Thus, extracted key length achieved is m-Θ(k) if shared secret key has m entropy round complexity is Θ(k) with optimal entropy loss.

REFERENCES

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984 (IEEE, New York, 1984), p. 175.

[2] [2] A. K. Eckert, Phys. Rev. Lett. **67**, 661 (1991).

[3] [3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)

[4] [4] Hanif Bayat Movahed, Quantum Key distribution and Privacy amplification, #0248243,University of Guelph, Project for QIP course

[5] [5] David, Artur, Richard , Chiara , Sandu, Anna , Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*Clarendon Laboratory, Department of Physics, University of Oxford , Oxford OX1 3PU, United Kingdom, School of Mathematics and Statistics, University of Plymouth,, United Kingdom, Department of Electrical, Computer and Systems Engineering, Boston University,*

[6] [6] Anders Tipsmark, Ruifang Dong, Amin Laghaout, Petr Marek, Miroslav Jezek, Ulrik L. Andersen, Experimental demonstration of a Hadamard gate for coherent state qubits.

[7] [7] Leonid Reyzin. Some Notions of Entropy for Cryptography. Boston University Computer Sciencehttp://www.cs.bu.edu/~reyzin

[8] [8] Renato Renner and Stefan Wolf. Simple and Tight Bounds for Information Reconciliation and Privacy Amplification. Computer Science Department, ETH Zurich, Switzerland.renner@inf.ethz.ch., Department d'Informatique et R.O., Universite de Montreal, QC, Canada.wolf@iro.umontreal.ca

[9] [9] Anastase Nakassis, Joshua Bienfang, Carl Williams, Expeditious Reconciliation for Practical Quantum Key Distribution, NIST, 100 Bureau Drive, Gaithersburg, MD 20899-8423

[10] [10] C. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210-229, 1988

[11] [11]C. H. Bennett, G. Brassard, C. Crepeau, and U. Maurer, Generalized privacy amplification, IEEE Transactions on Information Theory, Vol. 41, No. 6, 1915–1923, 1995.

[12] [12]B. Kanukurthi and L. Reyzin. Key agreement from close secrets over unsecured channels. In A. Joux, editor, *Advances in Cryptology|EUROCRYPT 2009*, volume 5479 of *LNCS*. Springer, 2009.

[13] [13]R. Renner and S. Wolf. Unconditional authenticity and privacy from arbitrarily weak secret. In Dan Boneh, editor, Advances in Cryptology| CRYPTO 2003, volume 2729 of LNCS, pages 78{95. Springer-Verlag , 2003

[14] [14]B. Kanukurthi and L. Reyzin. An improved robust fuzzy extractor. In R. Ostrovsky, R. D. Y

[15] [15]Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing, 38(1):97{139, 2008. arXiv:cs/0602007.

[16] [16]N. Chandran, B. Kanukurthi, R. Ostrovsky, and L.Reyzin. Privacy amplification with asymptotically optimal entropy loss

[17] Q. A. Turchette, C. J. Hood, W. Lange, H.Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).

