APPLICATION OF AVK AND SELECTIVE ENCRYPTION IN IMPROVING PERFORMANCE OF QUANTUM CRYPTOGRAPHY AND NETWORKS

C.T. Bhunia
Haldia Institute of Technology, PO: HIT, 721657, East Midnapore, West Bengal, India
and
The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Abstract

The subject of quantum cryptography has emerged as an important area of research. Reported theoretical and practical investigations have conclusively established the reliable quantum key distribution (QKD) protocols with a higher level of security. For perfect security, the implementation of a time variant key is essential. The nature of cost and operation involved in quantum key distribution to distribute a time variant key from session to session/message to message has yet to be addressed from an implementation angle, yet it is understood to be hard with current available technology. Besides, the disadvantages of the subject quantum cryptanalysis, in the name of “quantum cheating” and quantum error are demonstrated in the literature. This calls for an investigation for an affordable hybrid solution using QKD with conventional classical methods of key distribution to implement a time variant key. The paper proposes a hybrid solution towards this investigation. The solutions suggested will improve the performance of computer networks for secure transport of data in general.

MIRAMARE – TRIESTE
July 2006

1 Senior Associate of ICTP. ctbhunia@vsnl.com
INTRODUCTION

In his authoritative work[1,2], Shannon showed that the perfect secrecy in symmetric or secret cryptography is achievable only when the shared key of users is made to vary from session to session /message to message. This solution of time variant key in realizing perfect secrecy faces the well established problem known as the key distribution/transportation problem[3,4]. This great theory of Shannon is believed to be realizable with QKD as reported recent in researches[5-10]. In quantum mechanics one cannot measure something without causing noise to other related parameter. For examples Hysenberg's uncertainty principle states that $\Delta x . \Delta m = \text{constant}$. Thus if $\Delta x$ is changed, $\Delta m$ is bound to change. An ideal quantum channel supports transportation of the single photon. Thus a single photon can represent a bit – 0 (zero) or 1(one). The phase or state of polarization of photon may be used for identifying the 0 or 1. For example, Photons with 0° and 90° of polarization may therefore be treated as bit 0; and photons with 45° and 135° (also known as – 45°) of polarization may be assumed as bit1. Data security through quantum channel is under active research in the UK and USA. Some positive breakthroughs have been made by Charles Bennet of IBM Research at Yorktown Heights, New York, and by Gilles Brassard at the University of Montreal[11,12]. If Alice wants to send Bob the secret key, she can send the key, say of N bits, through quantum channels. Bob will be instructed by Alice to detect the photons (bits) from the quantum channel starting from a given time. There may be some transmission loss, and Bob may be able to detect some fraction of photons or bits. Bob will have to inform Alice via a telephone as to which photon he has seen. In this way, they may share both a common and variable key. For instance, if Alice sends 11100000 as the key, and Bob replies that he has seen the first, seventh and eighth photons (starting from the leftmost bit), then their common key shall be 100.

Alice can send data haphazardly using different polarized photons. Alice can do so (fig 1) either on a rectilinear basis:

When a horizontal polarized photon represents a 0 and a vertical polarization represents a 1

Or on a diagonal basis:

When a - 45° polarized photon represents a 0 and a + 45° polarized photon represents a 1.

Alice haphazardly uses both to send qubits (fig 2). Bob will haphazardly try to filter out the qubits. For the purpose of qubits detection Bob will use a polarization beam splitter. The polarization beam splitter is a device that allows the photons of orthogonal polarization to pass through but shunts the photon of other polarizations. The quantum nature dictates that: a) the same basis beam splitter will pass the received same basis polarized photons, but b) the rectilinear beam splitter will pass the received diagonally polarized photons either as vertical or horizontal polarization with equal probability and the diagonal beam splitter will pass the received rectilinear polarized photons either as vertical or horizontal polarized photons with equal probability. This will provide the different combinations of Alice’s sent photons and Bob’s detected photons. Therefore when both Alice and Bob use the splitter on the same basis they with correctly communicate qubits, but when they use the splitter on a different basis, the chance of matching between sent and received qubits is 50%. Bob now tells Alice (via conventional method, say telephone, as there is no need to keep secret these) how he
used the beam splitter to detect received qubits. Assume Bob’s choice was as rectilinear, rectilinear, diagonal, rectilinear, diagonal (fig 1). Bob does not announce the results of detection. Alice replies publicly (meaning via conventional method as there is no need to keep this secret) Bob the instants her choices of base match with Bob’s choices. Then they use the qubits of those instants when they use same base (in those instant they correctly communicate the bits), and ignore the bits of other instants. The matching bits (fig 2) generate the secret key for the session.

(a) Alice sends qubits to Bob randomly (we have taken only 5 qubits for illustration)

(b) Bob measures the received photons using a random polarization basis

(c) Alice and Bob communicate and identify locations where they correctly used the polarization base. COMPARE (a) with (b). BUT THEY KEEP SECRET THE POLARIZATION OF SENT OR RECEIVED PHOTONS.

(d) Correct bits are taken for key. Bits of other positions are ignored. So the key in this example is 111.

Fig 2. Key exchange between Alice and Bob

Should any eavesdropper attempt to intercept photon transmission; there shall be garbage with the key accepted by Alice and Bob. This is because the quantum theory ensures that, without changing the phase of the photon, an intercepted photon cannot be retransmitted. Therefore, a change in the polarity of the photon will let Alice and Bob immediately know of an interception. The scheme of sending information at the one-photon-per bit level as proposed by IBM research and the research of University of Montreal reported that “to send the key, the transmitter (Alice) tells the receiver (Bob) the plans to send n bits (photons) starting at a given time. Alice then sends the bits by randomly
switching the phase in the transmitter between 0° to 180°; this switches the output in the receiver between "0" and "1". Although transmission and detection losses mean that Bob will only see a small classical communication channel (the telephone, for example) to tell Alice which photons he has seen - but not which detector he has seen. This allows Alice and Bob to share the same random number. For example, Alice uses ten photons to send the random number 1001011101; Bob replies that he only received the second, fifth and last photon; therefore they have shared the random number 001.

However, it is conceivable that a eavesdropper could intercept the signal, copy Alice's message, and send it on to Bob without either Alice or Bob realizing. One way to overcome this, and ensure absolute security, is for both the transmitter and receiver to use non-orthogonal measurement bases. In other words, Alice sends parts of the message by switching the transmitter phase between 90° and 270°, say, and other parts by switching between 0° and 180°. When Bob and Alice are using the same base, the system works as before. However, if Alice is using 0°/180° and Bob is using 90°/270° (or vice versa), the message is meaningless - a photon that Alice sends as a "0" has a 50% chance of being received as a "1" and vice versa. Therefore when Bob tells Alice which photons he has received, he also says which base he was using and Alice must tell him if that is a valid photon (i.e. one which was sent and received when they were both using the same base). Paul Townsend of British Telecom, working with the Malvern group, recently demonstrated self-interference of short light pulses, "containing on average 0.1 photons, down 10 km of standard communications fiber using the technique."

There is another technique to minimize the hacking by Eve. This is to reduce Eve's information. The technique is known as privacy amplification protocol. In the protocol, Alice randomly chooses pairs of bits from the key they have got over quantum channel. Then she performs XOR on the pairs. She then tells publicly to Bob on which bits the XOR operation was made but not the results. Bob then performs the XOR operation on the bits that Alice informed him. Alice and Bob then replace the pair with XOR results to design the new key. This is illustrated as below:

a) Alice and Bob have the secret key 111 as in fig (2)

b) Alice chooses the first and second bit as a pair and informs these to Bob publicly. She gets the XOR result 1 ⊕ 1 = 0 and keeps it secret.

c) Bob performs XOR on the informed bits and gets the result 1 ⊕ 1 = 0.

d) Alice and Bob both replace the pair by the XOR result. So their new key is 01.

e) Note that even if Eve definitely knows one bit of the chosen pair, until and unless she gets the result of XOR (which Alice and Bob never communicate) she cannot replace the pair for hacking the key.

The active research in the quantum cryptography has made many other protocols for quantum key distribution (QKD): Ekert protocol, B92 protocol, six state protocol and QKD protocols with higher dimensional quantum states. Ekert protocol aims to provide a secret random key to users (Alice and Bob) using entanglement. B92 protocol aims to provide a secret key to the users using two non orthogonal quantum states. The six states protocol proposes to use six non orthogonal quantum states to provide a secret key to the users. The higher dimensional QKD protocol proposes to use d dimensional non orthogonal quantum states to provide a secret key. It is believed that as a number of non orthogonal states increases the level of security confidence will increase. It is generally verified that higher dimensions allow Eve less information than qubits.

**RESEARCH IDEAS**

Research findings reported in literature have established the superiority of QKD over classical approaches. The superiority is mainly due to the application of laws of physics in QKD rather than unproven mathematical assumptions used in classical methods. The cost and operational issues of using a quantum channel for key distribution from session to session/ message to message are yet to be addressed as to make it applicable in a general sense, neither it appears to be easy task. We
propose two solutions to apply QKD in implementing one time pad key. The proposed solutions are: hybrid use of QKD and AVK, and QKD+ AVK +Selective Encryption

**Automatic Variable Key**
Recently AVK was proposed as a time variant key[22]. The proposed AVK is illustrated in table 1 for a session between Alice and Bob whereby they respectively exchange data 345 and 789. In AVK, the key is made variable with data. The key is proposed to be variable, and after every transmission it changes dynamically such that:

\[ K_0 = \text{initial secret data} \]
\[ K_i = K_{i-1} \text{ XOR } D_i \text{ for all } i > 0 \]

The variable key as suggested, if implemented, will not only provide a time variant key but it will provide security confidence against differential attack[23]. AVK will prevent the repetition of patterns in cipher for the same input data blocks unlike in conventional cryptosystems. The experimental results in table 2 duly confirm it. We propose that QKD may be used for the first time to share the secret key using a costly quantum channel. Thereafter the AVK may be used to vary the shared key for which a classical channel will suffice. This hybrid solution will definitely overcome the quantum error problem. In the proposed scheme the quantum channel is used only for the first key.

**Selective Encryption**
The performance of any cryptosystem is measured by two parameters: Level of security and Speed of encryption. It is undoubtedly established that a hybrid operation of QKD with AVK will provide a very high level of security confidence. Therefore it is proposed to use the selective encryption with QKD and AVK. The recently introduced AES (Advanced Encryption Standard) is supposed to replace DES. AES suffers from the error propagation problem[24-25] that causes the speed of encryption to go down. The selective encryption[26-27] is proposed to overcome the problem.

<table>
<thead>
<tr>
<th>Session slots</th>
<th>Alice Sends</th>
<th>Bob Receives</th>
<th>Bob Sends</th>
<th>Alice receives</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A secret key say 2</td>
<td>2</td>
<td>A secret key say 6</td>
<td>6</td>
<td>For next slot, Alice will use 6 as key and Bob 2 as key for transmitting data</td>
</tr>
<tr>
<td></td>
<td>Alice sends his first data(3) as: 3 XOR 6</td>
<td>Bob gets back original data (3 XOR 6 XOR 6) = 3</td>
<td>Bob sends first data (7) as: 7 XOR 2</td>
<td>Alice gets back original data (7 XOR 2 XOR 2) = 7</td>
<td>Alice will create new key 7 XOR 6 for next slot. Bob will create new key 2 XOR 3 for the purpose of transmission.</td>
</tr>
<tr>
<td>2</td>
<td>Alice sends next data (4) as: 4 XOR 6 XOR 7</td>
<td>Bob recovers original data (4 XOR 6 XOR 7 XOR 6 XOR 7) = 4</td>
<td>Bob sends next data (8) as: 8 XOR 2 XOR 3</td>
<td>Alice recovers original data (8 XOR 2 XOR 3 XOR 2 XOR 3) = 8</td>
<td>Alice computes new key 3 XOR 4 and Bob computes new key 7 XOR 8 for transmitting next data.</td>
</tr>
</tbody>
</table>
TABLE 2: Experimental verification of superiority RSA AVK over conventional RSA

Original Message: Blue colored data are repeated data bytes as we have used ASCII code

financial bid=Rs 3700 for modem
financial bid=Rs 5000 for printer

Encrypted Message under Conventional RSA (Blue colored are repeated encrypted bytes/ 32768 is for blank space the repetition is present in cipher as in original; this to differential cryptanalysis)


Encrypted message under RSA with AVK (no repeated encrypted byte even for blank space for repeated bytes in original message; no way differential cryptanalysis is possible)


For the purpose of tackling the error propagation of AES and thereby the lower speed of encryption the selective encryption in fig 3 may be employed. The selective encryption lowers the security level, but with the application of QKD with AVK the level is guaranteed.
QUANTUM Channel…………….to transport key for the first time

Classical Channel for subsequent operation under AVK and Selective encryption

![Diagram: Selective AES with AVK plus QKD](image)

The viability of the idea revolves around the choice of \( r \). We propose the following algorithm I for the selection of those blocks of the message that require encryption.

**Algorithm: I**

1. Input Key Words for the message of \( N \) words (say, \( n \) numbers of keywords are given). Find the frequency of occurrence of each keyword in whole of the message, \( f_i \) (\( i=1 \) to \( n \)).
2. [Say, the AES encrypts blocks each of \( M \) words (\( M<N \)). So there are \( k \) blocks where \( k=N/M \). Find the frequency of occurrence of each keyword in each block, \( F_{ij} \) (\( i=1 \) to \( n \), \( j=1 \) to \( k \)).
3. If \( F_{ij} \geq \{f_i(1/k)\} \) for any one, more or all keywords, i.e., \( i=1 \) to \( n \), the \( j \)th block will be encrypted in AES with redundancy based technique, otherwise not.
4. Repeat (3) for all blocks, \( j=1 \) to \( k \). When \( j=k \), the proposed scheme of encryption is complete.

**Simple Analysis**

If \( P \) is the probability of the failure of encryption of a block due to error, the speed factor for encryption under the proposed scheme will be:

\[
\text{Speed up factor } (s) = \frac{1}{r + (1-r)(1-P)}
\]

This provides a throughput gain for the proposed scheme over the conventional scheme as:

\[
gain = (s-1) \times 100\% \quad (1)
\]

**An estimation of the value of \( r \) in case of random distribution**

We assume that the key words are randomly distributed with \( \alpha_i \) as the probability of occurrence of \( i \)th key word in any application or service. Assume that the same application generates a message of \( N \) words. Then

\[
f_i = N \alpha_i
\]

The probability that the \( j \)th block will be encrypted is

\[
P_j = \left[ \sum_{i=M}^{M} \binom{M}{i} \left( \alpha_i \right)^i (1-\alpha_i)^{M-i} \right]
\]
where $M$ is the block size; and number of blocks, $k=N/M$.

Thus the probability of $j$th block being selected for encryption is $p_{hj}$ where:

$$p_{hj} = \text{highest value of all } p_{ji} \text{ for all key words (i=1 to n)}.$$  

Let us assume that $p_{hj}(=p)$ is same for all the key words. Then the probability that $r$ number of blocks will be selected out of $k$ blocks is

$$p_{rs} = \binom{k}{r} p^r (1-p)^{k-r}$$

This suggests a value of $r$ as $r_{\text{random}}$ where:

$$r_{\text{random}} = \left[ \sum_{i=1}^{k} \binom{k}{i} \right] \times \left( \frac{1}{k} \right)$$ (2)

The numerical results (with $i=1$ and $\alpha_i=\alpha$) based on eqs.(1-2) are shown in fig 4. It is found that:

(i) As expected when $\alpha=1$, $r$ becomes 1 (100%);
(ii) As $M$ increases, $r$ decreases. As $M$ increases, block size increases resulting in a higher probability of the block to be encrypted. Again as $M$ increases, $k$ decreases. Thus minor number of blocks will meet the criterion of being encrypted. These are the reasons behind such results.
(iii) As expected with the lower value of $\alpha$, the value of $r$ goes down. This is due to the fact that with lower $\alpha$, the probability of any block to be encrypted goes down
(iv) As gain depends on both $r$ and $P$, the variation of gain has been shown in fig 3 for different sets of $r$ and $P$. As expected the gain decreases with the increase of $r$ and decrease of $P$. As expected, both gain and loss are 0, when $r=1$.

![Graph](image)

Fig 4. Variation of $r$ with $\alpha$ [Note: the results are given only for $N=16$ because if $N$ is high, the computation using the binomial formula becomes unmanageable. In that case, Laplace approximation has to be used]

We have illustrated a selective AES that will increase the speed of encryption which normally goes down with the error propagation effect of AES. The selective encryption will cause security level to fall. To maintain the desired security level, QKD plus AVK may be employed with the technique. We find that the proposed technique will be effective at high value of $P$ and low value of $r$, i.e. when the system running the AES has a high probability of bit error, and the plain text has a low probability of occurrence of key words. We propose a few other algorithms for selective encryption with AVK and QKD.
Algorithm II
The study made above on the proposed technique shows it has to compromise with security level. The algorithm I proposed for the selection of blocks to be encrypted has inherently compromised the level of security. The algorithm proposes to encrypt when the block contains a minimum of \( \left\lfloor \frac{f_i}{(1/k)} \right\rfloor \) key words. If the keyword is the parameter of secrecy, logically a block should be encrypted if the block has even a single keyword. Secondly algorithm I is applicable only when the whole of message is available prior to encryption. When the message is being generated and being processed for encryption on stream, the proposed algorithm I will not work. Thus algorithm I may be modified as in algorithm II to provide a higher level of security confidence and to make it applicable to any message coming as a stream.

### Algorithm: II

1. Input Key Words for the message of N words (say, n number of keywords are given).
2. [Say, the AES encrypts blocks each of M words (M<N). So there are k blocks where k=N/M]. If it occurs, encrypt the block otherwise not.
3. Repeat (2) for all blocks, j=1 to k. When j=k, the proposed scheme of encryption is complete.

---

Fig 5: Comparison of variation of r with the probability of occurrence of key words for algorithm I & II.

The results ‘r’ for algorithm I and algorithm II are compared in fig 5. It is found that:

i) As expected the value of r is higher in the case of algorithm II thereby ensuring a higher level of security which was the aim for algorithm II

ii) There is a nominal difference in the values of ‘r’ in two cases. The difference is higher when M is lower. This suggests that for low M, algorithm II may be used, and for high M,
algorithm I may be employed. The better response of algorithm I for higher M was established in fig 5 above.

\[
\begin{align*}
\text{Algorithm III} \\
\text{To further increase the level of security and to make the scheme applicable to a message generating as a number of streams, we propose algorithm III. Algorithm III fits the geometric distribution model.}
\end{align*}
\]

\[
\begin{align*}
\text{Algorithm: III} \\
1. \quad \text{Input Key Words for the message of N words} \\
\text{Message is divided into K parts each of k blocks. Each block is of M words} \\
2. \quad \text{Find the occurrence of any keyword in the blocks, starting with the first block in the first part. If it occurs, encrypt that block and all the blocks thereafter in the part} \\
3. \quad \text{Repeat (1-2) for all parts, j=1 to K. When j=K, the proposed scheme of encryption is complete.}
\end{align*}
\]

We assume a single keyword that has a probability of occurrence in the message as \( \beta \). Thus the probability, \( Q \) that a block of M words be selected for encryption is given as:

\[
Q = \left[ \sum_{i=1}^{M} \binom{M}{i} \alpha_i^i (1-\alpha)^{M-i} \right] 
\]  
(3)

The probability, \( Q_i \) that the last \( i \)th block out of \( i \) sequential stream blocks, will be encrypted is then:

\[
Q_i = Q (1-Q)^{i-1} 
\]  
(4)
Thus the value of $r$ will be obtained as:

$$r = \frac{1}{k} \sum_{i=1}^{k} k - i + 1 \cdot Q_i$$  \hspace{1cm} (5)$$

The value of $r$ under algorithm III is given in Fig 6. We find that the variation is similar to that of binomial distribution, but $r$ is higher in geometric distribution confirming better security.

![Graph: % of blocks to be encrypted versus stream size (N) with Geometric Distribution with M=8](image)

**Fig 7. Variation of $r$ with respect to $N$ under algorithm III**

We have studied the variation of $r$ under algorithm III with message size, $N$. It was not done for the cases of algorithms I and II for computational problems with binomial co-efficient. We find in Fig 7:

i) With $N$, $r$ increases as expected, thereby increasing the security level.

ii) As expected with the probability of occurrence of keywords $S$ in the message, $r$ increases.

**CONCLUSION**

Quantum cryptography is very promising. As it matures as an independent technology, a hybrid application of quantum key distribution with AVK and selective encryption may be an alternative viable proposition. In the paper we have illustrated a number of possible means of realizing the hybrid techniques. Performance studies and comparison are made. In their coexistence phase, the proposed ideas of 1) QKD with AVK and 2) Selective encryption with QKD & AVK will be interesting and effective applications in secure communication.

**Acknowledgments**: This work was done within the framework of the Associateship Scheme of the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.
REFERENCES

3. C T Bhunia, IT, Network & Internet, New Age International Publishers, New Delhi, 2005
7. N Datta, Quantum Entropy and Information, School on Theory and Technology in Quantum Information, Communication, Communication and cryptography, 12-16 June’2006
18. H Bechmann Pasqulucci et al, Physics review, A59, 4238, 1999
22. C T Bhunia Application of Automatic Variable Key in ECB with DES and in RSA”, pp135-143 in “ it++ the nest generation”, CSI Annual Convention McGrawhill, New Delhi, 2004
25. C T Bhunia et al, Project Work on AES Error Propagation, ISM, Deemed University, India, June’2004