

VARIATIONS ON KAK'S THREE STAGE QUANTUM CRYPTOGRAPHY PROTOCOL

JAMES HAROLD THOMAS

ABSTRACT. This paper introduces a variation on Kak's three-stage quantum key distribution protocol which allows for defence against the man in the middle attack. In addition, we introduce a new protocol, which also offers similar resilience against such an attack.

1. INTRODUCTION

In the relatively new field of quantum information science, there have been limited numbers of true breakthroughs. The quantum computer remains a machine on paper only, for a working realization has proved elusive. For one of the most powerful tools that the quantum computer would provide, namely the reduction of the factorization problem to polynomial time by Shor's algorithm, the most successful implementation to date has been to factor the number 15 into 3 times 5 [1].

The quantum computer might remain unrealized for years to come. Indeed, Kak has suggested that the current quantum circuit model for quantum computers is fundamentally flawed and new models must be developed to tackle the problem [2].

While there have been limited strides in some areas of quantum information science, one area in particular has produced realizable solutions in the field of cryptography. Quantum key distribution protocols have been successfully implemented and have produced commercially available products.

In this paper, we will discuss a new protocol proposed by Kak called the "Three Stage Protocol." To Kak's protocol, we will introduce a modification which allows for greater security against man in the middle attacks. In addition, we introduce a new single stage protocol which similarly allows for security against such attacks.

2. QUANTUM KEY DISTRIBUTION

The usefulness of quantum key distribution lies in the properties of the qubit, the quantum unit of information. Since a qubit is an object representing a quantum superposition state, the qubit cannot be copied. This is commonly called the no-cloning theorem [3]. This property ensures that during qubit data transmission, it is impossible for an eavesdropper (Eve) to simply make copies of the qubits being sent, and thus manipulate these copied qubits to obtain the message. This useful property allows quantum data transmission to be used effectively in key distribution protocols as shown in [3].

When a private key can be transmitted securely along a quantum channel, then secure classical communication between the two parties (Alice and Bob) can be achieved using the private key (Figure 1). One private key cryptosystem in use today is the Vernam cipher, also called the one time pad. According to Nielsen and Chuang, the security of the private key used in the Vernam cipher is sometimes

ensured by transmitting it via such low-tech solutions as clandestine meetings or trusted couriers. The need for better transmission protocols is obvious.

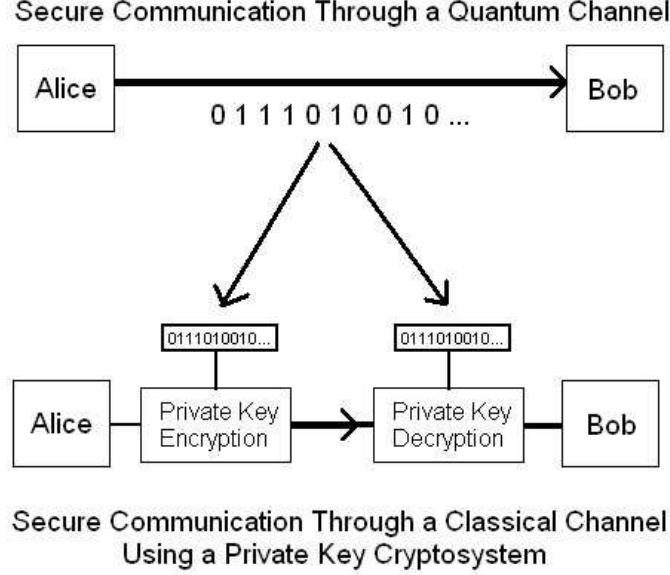


FIGURE 1. Quantum Key Distribution

3. KAK'S THREE-STAGE PROTOCOL

In [4], S. Kak proposed a new quantum key distribution protocol based on secret unitary transformations (Figure 2). His protocol, like BB84, has three stages, but unlike BB84, it remains quantum across all three stages. In the first stage, Alice manipulates the message X , which is simply one of two orthogonal states (e.g. $\alpha|0\rangle + \beta|1\rangle$ and $\beta|0\rangle - \alpha|1\rangle$) by means of a unitary transformation U_A , known only to her. Bob receives the new state, and in the second stage, applies his own secret transformation U_B , which is both a unitary transformation, and one that commutes with U_A , and sends the result back to Alice. In the third stage, Alice applies the Hermitian conjugate of her transformation, U_A^\dagger , and sends the result back to Bob. Since $U_A^\dagger U_B U_A(X) = U_B(X)$, Bob simply applies U_B^\dagger and obtains the previously unknown state, X .

4. THE MAN IN THE MIDDLE ATTACK

The Suceptability of both BB84 and Kak's three-stage protocol to man in the middle attacks has been documented [e.g. 5,6], and various methods to counter these attacks have been proposed [e.g. 7,8]. In such an attack, the eavesdropper, Eve, can attempt to thwart the communication between Alice and Bob in one of the following ways (Figure 3).

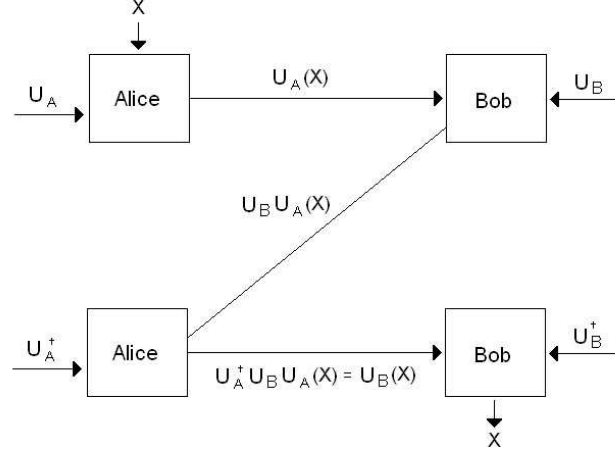


FIGURE 2. Kak's Three-Stage Protocol

- (1) Eve receives the message from Alice by impersonating Bob. Eve then decodes Alice's message, and, now impersonating Alice, duplicates this message to Bob. In this scenario, both Eve and Bob obtain the secret message.
- (2) Eve impersonates Bob and decodes Alice's message as in scenario 1, but instead of relaying the actual message to Bob, Eve relays a different message of her own choosing. In this scenario, only Eve obtains the secret message.
- (3) Eve impersonates Bob, but is not able to decode Alice's message. Instead, she impersonates Alice and sends her own message to Bob. In this scenario, communication between Alice and Bob is blocked, but no secret message is compromised.

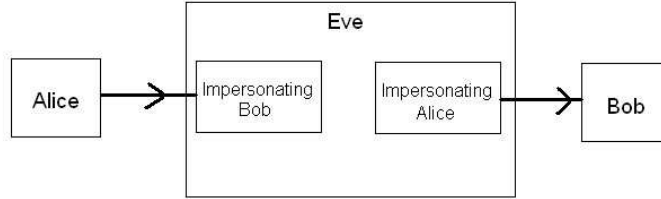


FIGURE 3. Man in the Middle Attack

5. A VARIATION ON KAK'S THREE STAGE PROTOCOL

In Kak's paper [4], he suggests using secret real valued orthogonal transformations to encrypt the qubits. Under orthogonal transformations of the same form (see below), the selection of the angles θ and ϕ by Alice and Bob respectively does

not affect the outcome of the protocol. Furthermore, both Alice and Bob do not need to know what each other's angle selection is.

The reason that a man in the middle attack can be carried out is that when U_A is assumed to be real valued, it is very easy for Eve to find another unitary transformation, U_E , which commutes with U_A . This is the underlying assumption by both Perkins [5], and Basuchowdhuri [7]. Indeed, for a 2x2 real valued unitary transformation (i.e. an orthogonal transformation), there is a limitation on its form.

Consider a 2x2 transformation:

$$\mathbf{U}_A = \begin{bmatrix} w & x \\ y & z \end{bmatrix}, w, x, y, z \in \mathbb{R}$$

Then, for U_A to be orthogonal (unitary), $U_A U_A = I$. This gives rise to the following equations:

$$\begin{cases} w^2 + y^2 = 1 \\ x^2 + z^2 = 1 \\ wx + yz = 0 \end{cases}$$

These equations are satisfied only when U_A has one of the two following forms:

$$\mathbf{U}_1(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix},$$

a rotation, as Kak proposed, or

$$\mathbf{U}_2(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix},$$

a reflection across the line $\frac{\theta}{2}$.

The three-stage protocol demands that while Bob doesn't know the value of θ that Alice is using, he must know which of the two above forms of U_A that Alice chooses. The reason for this is that while $U_1(\theta)$ commutes with $U_1(\phi)$ for any θ and ϕ , and $U_2(\theta)$ commutes with $U_2(\phi)$ for any θ and ϕ , $U_1(\theta)$ does not commute with $U_2(\phi)$ in general. So we will consider the choice of the form of U_A to be public information. Once this information is known, Bob simply needs to choose his own angle ϕ , and his transformation U_B will be of the same form as U_A .

$$U_B = \begin{cases} U_1(\phi), U_A = U_1(\theta) \\ U_2(\phi), U_A = U_2(\theta) \end{cases}.$$

It is easy to see that when the same form is used, U_A and U_B commute (i.e. $U_A U_B = U_B U_A$).

For Form 1:

$$\begin{aligned} U_A U_B &= \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{bmatrix} = \\ &\begin{bmatrix} \cos(\theta)\cos(\phi) - \sin(\theta)\sin(\phi) & -\cos(\theta)\sin(\phi) - \cos(\phi)\sin(\theta) \\ \cos(\phi)\sin(\theta) + \cos(\theta)\sin(\phi) & -\sin(\theta)\sin(\phi) + \cos(\theta)\cos(\phi) \end{bmatrix} \end{aligned}$$

Applying trigonometric identities,

$$U_A U_B = \begin{bmatrix} \cos(\theta + \phi) & -\sin(\theta + \phi) \\ \sin(\theta + \phi) & \cos(\theta + \phi) \end{bmatrix}.$$

Since U_A and U_B have the same form, it is clear that they commute.

For form 2:

$$\begin{aligned} U_A U_B &= \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(\phi) & \sin(\phi) \\ \sin(\phi) & -\cos(\phi) \end{bmatrix} = \\ &= \begin{bmatrix} \cos(\theta)\cos(\phi) + \sin(\theta)\sin(\phi) & \cos(\theta)\sin(\phi) - \cos(\phi)\sin(\theta) \\ \cos(\phi)\sin(\theta) - \cos(\theta)\sin(\phi) & \sin(\theta)\sin(\phi) + \cos(\theta)\cos(\phi) \end{bmatrix}. \end{aligned}$$

Again, applying trigonometric identities,

$$U_A U_B = \begin{bmatrix} \cos(\theta + \phi) & \sin(\phi - \theta) \\ \sin(\theta - \phi) & \cos(\theta + \phi) \end{bmatrix}$$

Since U_A and U_B always commute given the same form, then for Eve to impersonate Bob and obtain Alice's secret message, she only needs to select any angle ψ and use it in her own transformation U_E where U_E is of the same form as U_A . Using U_E , Eve can obtain the secret state X in the exact same way that Bob can obtain it. In addition, Eve can relay a message to Bob using her own U_E transformation. Since Bob doesn't know what Alice's U_A transformation is, Eve's U_E is a valid substitution.

Suppose now instead of a orthogonal (i.e. unitary and real value) transformation, Alice chooses a more general complex valued unitary transformation,

$$U_A(\theta) = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\theta} & e^{-i\theta} \\ ie^{i\theta} & -ie^{-i\theta} \end{bmatrix}, \theta \in [0, 2\pi).$$

When Alice chooses a U_A of this form, it is more difficult for Bob to find another transform, U_B which commutes. We see that when

$$U_B(\phi) = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\phi} & e^{-i\phi} \\ ie^{i\phi} & -ie^{-i\phi} \end{bmatrix}, \theta \in [0, 2\pi),$$

then

$$U_A U_B = \begin{bmatrix} e^{i(\theta+\phi)} + ie^{i(\phi-\theta)} & e^{i(\theta-\phi)} - ie^{-i(\theta+\phi)} \\ ie^{i(\theta+\phi)} + e^{i(\phi-\theta)} & ie^{i(\theta-\phi)} - e^{-i(\theta+\phi)} \end{bmatrix}$$

and

$$U_B U_A = \begin{bmatrix} e^{i(\phi+\theta)} + ie^{i(\theta-\phi)} & e^{i(\phi-\theta)} - ie^{-i(\phi+\theta)} \\ ie^{i(\phi+\theta)} + e^{i(\theta-\phi)} & ie^{i(\phi-\theta)} - e^{-i(\phi+\theta)} \end{bmatrix}.$$

These transformations commute only when $\phi = \theta + \pi$ (or any 2π multiple). For Bob to decode Alice's message, he must have more information than simply the form of her transformation. He must know also the value of θ that she has chosen.

While this might seem to be a hindrance to the protocol, it allows for much greater security against a man in the middle attack. Eve attempts to intercept Alice's message to Bob by choosing a U_E to impersonate Bob's U_B . As we saw earlier, when U_A is real valued, Eve can simply pick any angle ψ and generate a transformation U_E that commutes. But with a complex valued U_A , Eve cannot guarantee a commuting transformation without knowing the value of θ . Consider Eve's choice of a ψ without knowledge of θ . Then, $U_A^\dagger U_E U_A \neq U_E$.

6. THE SINGLE STAGE QUANTUM CRYPTOGRAPHY PROTOCOL

When, as in the variation to Kak's protocol described above, Bob knows the value of θ that Alice has chosen for her transformation U_A (assuming as above that the form of U_A is public information), then he has full knowledge of U_A . In this situation, Alice and Bob can forego the second two stages of the protocol and let Bob perform the transform U_A^\dagger to obtain the unknown state X (Figure 4). We have simply, $U_A^\dagger U_A(X) = X$. In this situation, there is no need for U_A to be complex valued. We can have, as Kak proposed in [4],

$$U_A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

So for Eve to intercept the message X and properly decode it, she would have to know the value of θ . The strength of this protocol is dependent on keeping the value of θ a secret known only to Alice and Bob. We enhance the security of our protocol by allowing for θ to change, which blocks any attempt by Eve at a statistical analysis of the qubits. We assume that before secure transmission may begin, there is some other secure protocol that Alice may use to transmit her initial value of θ to Bob. One example is Perkins' protocol which uses trusted certificates [6].

Suppose we restrict θ to the upper half plane of the unit circle. After l qubits are successfully transmitted from Alice to Bob, the qubits $l+1$ to $l+k$ will be used to obtain the new value of θ . The k data bits selected by Alice for these k qubits will represent an integer N such that if b_n is the n th bit transmitted ($b_n \in \{0, 1\}$), then $N = b_{l+1} + 2b_{l+2} + 4b_{l+3} + \dots + 2^k b_{l+k}$. When these four qubits are received by Bob and decoded, Alice and Bob adjust their transformations U_A and U_A^\dagger respectively such that

$$U_A = \begin{bmatrix} \cos(\theta_N) & -\sin(\theta_N) \\ \sin(\theta_N) & \cos(\theta_N) \end{bmatrix}, \theta_N = \frac{N\pi}{2^k}.$$

After this, Alice transmits l more qubits to Bob before again changing the value of θ . In this fashion, any attempt by Eve to obtain the value of θ with no prior knowledge would be extremely difficult.

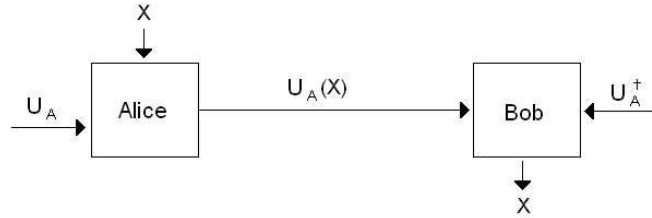


FIGURE 4. The Single Stage Quantum Cryptography Protocol

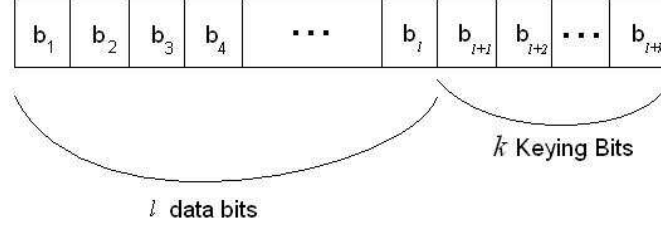


FIGURE 5. Framing on the Single Stage Protocol

ACKNOWLEDGEMENTS

The author thanks the Louisiana Board of Regents, BoRSF, under agreement NASA/LEQSF(2005-2010)-LaSPACE and NASA/LaSPACE under grant NNG05GH22H for support during this project.

REFERENCES

- [1] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, I.L. Chuang, Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* 414, 883-887 (20 Dec 2001). arXiv:quant-ph/0112176v1
- [2] S. Kak, Are Quantum Computing Models Realistic? *ACM Ubiquity*, 7 (11): 1-9, 2006. arXiv:quant-ph/0110040v5
- [3] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [4] S. Kak, A Three-Stage Quantum Cryptography Protocol. *Foundations of Physics Letters* 19 (2006), 293-296. arXiv:quant-ph/0503027v2
- [5] G. Gilbert, M. Hamrick (MITRE), Constraints on Eavesdropping on the BB84 Protocol. arXiv:quant-ph/0106034v2
- [6] W. Perkins, Trusted Certificates in Quantum Cryptography. arXiv:cs/0603046v1 [cs.CR]
- [7] K. Svozil, Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography. *International Journal of Quantum Information*, Vol. 3, No. 4 (2005) 649-654. arXiv:quant-ph/0501062v4
- [8] P. Basuchowdhuri, Classical Authentication Aided Three-Stage Quantum Protocol. arXiv:cs/0605083v1

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING, LOUISIANA STATE UNIVERSITY, BATON ROUGE, LOUISIANA, 70803, USA