CSCM38: Advanced Topics: AI and Cyber Security – Report

Luke Hengstenberg

878876

Table of Contents

Part A

Task 1

In the paper, Thomas (2007) provides an insight into a quantum cryptography protocol called the "Three Stage Protocol" proposed by Kak, introducing a modification to address security concerns, and proposing a new single stage protocol. The paper begins by explaining the usefulness of quantum key distribution due to the properties of qubits preventing cloning. The paper references the Vernam cipher and suggests that security concerns with current cryptosystems create a need for better transmission protocols. To develop the readers understanding of the topic area the paper details the three stages of Kak's protocol based on secret unitary transformations. A step by step explanation of Man-in-the-middle attacks is then provided, ensuring the reader understands the security concern the paper is addressing.

Following this, the paper sheds light on the reason Kak's three stage protocol is susceptible to MiTM attacks. The paper identifies a limitation in the application of orthogonal transformations that would allow Eve (attacker) to use her own transformation to impersonate Bob (victim), gaining access to Alice's (victim) secret message. The paper addresses this limitation by proposing a variation to the three-stage protocol that uses more general complex valued unitary transformation instead of orthogonal (unitary and real value) transformation. The security of this modification is reinforced by demonstrating how the same attack would now prove unsuccessful. Finally, the paper proposes a single stage quantum cryptography protocol that would also be resistant to MiTM attacks. This protocol allows Bob to perform a single transformation, skipping the second two stages of Kak's protocol. The paper explains the requirement of some other secure protocol to transmit an initial value. The paper demonstrates how the protocol would work by contributing formulas and justifies how it is resistant to MiTM attacks.

Task 2

Classical key distribution (CKD) can be accomplished by: two parties physically meeting, establishing a trusted courier, or using a public key cipher such as RSA and Diffie-Hellman. The RSA asymmetric encryption protocol is a commonly used method that makes use of the factorization problem, which consists of generating a key based on the multiplication of two large prime numbers [2]. The security of CKD relies purely on the computational difficulty of calculating the key. To break RSA every combination of the two prime numbers would have to be tested until those used for key generation are found. A traditional computer does not have the necessary processing power to accomplish this. However, a quantum computer is much more powerful and may therefore be able to solve the mathematical problems public key ciphers are based on by running a specific algorithm such as Shor's algorithm, rendering CKD unsecure.

Quantum Key Distribution (QKD) uses components of quantum mechanics to create secure communication channels between two parties for safe key exchange. Unlike CKD, the properties of QKD are based on the laws of physics making it resistant to increasing computational power, eavesdroppers, attack algorithms, and quantum computers [4]. QKD provides a truly secure channel for key exchange which produces detectable anomalies if an eavesdropper attempts to measure the key. QKD is a solution to the issues present in CKD by providing secure key distribution and prevention from attacks. However, in its current form

QKD has several technical weaknesses that are not present in CKD, such as quantum channels only working at short distances, slow transfer of information, and high cost of infrastructure to support it.

Task 3

The original algorithm "Kak's three-stage protocol" encrypts qubits using secret real valued orthogonal transformations. The first stage of the algorithm uses an orthogonal transformation U_A chosen by Alice which is assumed to be public knowledge, to manipulate a message X. U_A has one of two forms: $U_1(\theta)$ as a rotation or $U_2(\theta)$ as a reflection across line $\frac{\theta}{2}$. This means the protocol relies on Bob knowing which of the two forms Alice has chosen as $U_1(\theta)$ can commute with $U_1(\phi)$ for any chosen angles (θ, ϕ), but not $U_2(\phi)$. In the second stage Bob applies an orthogonal transformation U_B which commutes with U_A so that $U_AU_B = U_BU_A$, sending the result to Alice. In the third stage Alice applies the "Hermitian conjugate" $U^t{}_A$, sending the result back to Bob who can then apply $U^t{}_B$ to obtain state X. The issue with this protocol is due to U_A and U_B always commuting, Eve can impersonate Bob by creating her own transformation U_E with any angle ψ which is of the same form as U_A, therefore acting as a valid substitution in the preceding stages to obtain state X.

Thomas (2007) addresses this issue by modifying the protocol so that instead of a real valued orthogonal transformation for U_A Alice chooses a more general complex valued unitary transformation. This change makes it harder for Bob to choose a transformation U_B that commutes as it will only commute when ϕ is equal to $\theta + \pi$ or any 2π multiple. This means to get X, Bob needs to know the value Alice chose as θ as well as the form. This variation provides an extra level of security against MiTM attacks because Eve can no longer impersonate U_B by choosing a transformation U_E with any angle ψ and the same form as U_A. Without Eve having knowledge of θ, we would see that $U^t{}_AU_EU_A$ would not be equal to U_E in the third stage of the protocol, and would therefore fail in acquiring secret state X.

Thomas (2007) also proposes an alternative single stage quantum cryptography protocol that addresses this issue. As in Kak's protocol, a real valued orthogonal transformation is chosen as U_A instead of a complex valued unitary transformation used in the modified version. Much like the previously seen variation, this protocol relies on knowledge of the value θ used in U_A. The protocol eliminates the need for three stages by allowing Bob to obtain secret state X by using θ to perform the transformation $U^t{}_A$ such that $U^t{}_AU_A(X)$ is equal to X. Due to the secrecy of θ, this variation also provides security against MiTM attacks if Eve does not have knowledge of value θ, as well as having the benefit of being less computationally expensive. Both the variation and the new protocol face the issue of Alice safely transmitting an initial value for θ before secure transmission can begin. Thomas (2007) proposes the use of some other secure protocol such as the Perkin's protocol to combat this.

Although the single stage protocol requires less computation, one may argue that it is less secure than the previously explored variation as it relies purely on the secrecy of θ instead of a chosen form and θ. If the same value for θ is used throughout then Eve could perform statistical analysis on the qubits to calculate θ. To address this issue the protocol allows the value for θ to change after a set number of qubits have been successfully transmitted, with Alice and Bob adjusting their transformations based on the new value. This means any attempt to acquire θ would be extremely difficult without prior knowledge of the value and formula used.

Part B

Task 4

The first paper this report compares is titled “Understanding the Strategic and Technical Significance of Technology for Security – Implications of Quantum Computing within the Cybersecurity Domain” [2]. The paper provides a broad overview of the long-term potential of quantum technology and investigates two methods to achieve quantum proof cryptography: Post-quantum cryptography (PQC) and Quantum Key Distribution (QKD). Much like [1], this paper recognises the viability of using a quantum computer to apply Shor’s algorithm to break classical encryption. However, the paper stresses a sense of urgency not present in [1], which reflects the 12-year difference between their publication.

The paper refers to QKD as sending individual quantum particles from sender to receiver that when combined make up the encryption key. This shows that the applications of the protocol’s introduced by [1] go further than QKD, as direct encryption of data is performed meaning messages can be sent as well as keys. The paper lists a critical feature of QKD as ensuring the key transfer cannot be intercepted. This supports the overall contribution of [1] as both the three-stage variation and single stage protocol have been reported as following the no-cloning theorem and have been designed to prevent MiTM attacks. Another critical feature listed by the paper is QKD operating based on the laws of physics rather than computational complexity. This highlights an issue with the three-stage variation in [1] because although it operates based on the laws of physics it still relies on computational complexity with a fixed value for θ, meaning it is not future proof as θ could be calculated after encryption. The single stage protocol satisfies this as the value for θ is designed to change and is calculated using the qubits, therefore being future proof and based on physics. Overall, the paper gives credibility to the single stage protocol introduced by [1] but discredits the three-stage variation.

The second paper this report compares is titled “Quantum Key Distribution: from Principles to Practicalities” [3]. The paper reviews several quantum key distribution protocols, breaking down their structure and security. As with the previously explored papers, this paper also recognises the viability of using Shor’s algorithm to break classical encryption. The paper introduces three main classes of QKD protocols which are BB84, Ekert scheme, and Goldenberg/Vaidman class. These protocols are predecessors to those discussed in [1], and like Kak’s Three-stage protocol clear security flaws are identified. The variations of BB84 show similarities to the three-stage protocol due to Alice choosing between several states and Bob selecting based on the form. Much like [1], the paper references MiTM security concerns with these protocols. This supports the usefulness of the findings presented in [1] as both protocols have been designed to combat this issue.

The Ekert scheme and Goldenberg/Vaidman class also give credibility to the findings of [1] due to vulnerabilities in their reliance on states. However, both introduce methods to prevent eavesdropping which were not detailed in [1]. The Ekert scheme makes use of runs where different directions can be used to test the Bell inequality for interference. Error detection techniques to monitor interference were not discussed in [1], identifying a lack of research in how the protocols would detect an eavesdropper. The Goldenberg/Vaidman class sends wave packets at random times along two channels, stopping the eavesdropper from monitoring the transmission. Although the single stage protocol in [1] uses a method to change the θ value there is no reference to a randomisation element, pointing to a possible weakness in its design. Overall, when compared the protocols introduced by [1] appear to be more advanced in many aspects, especially in the prevention of MiTM attacks, but there is a clear lack of research into handling other security concerns and error monitoring.

Task 5

The first paper by HSD [2] was selected to provide a broad overview of quantum computing and QKD features in the modern world. The paper allowed a comparison to be made between papers written 12 years apart and enabled a review of [1]'s usefulness when compared with current research. The second paper by Bruss and Lutkenhaus [3] was selected to conduct a focused cross-examination of the technical aspects of the protocols presented by both papers. The paper allowed strengths and weaknesses to be identified by investigating issues present in [3] that were addressed by [1], and limitations in [1] that were addressed by [3].

The contribution of [1] has limited relevance as a standalone piece of research in 2019 but may provide relevance theoretically to other research. The concepts introduced by the paper are novel in addressing the specific issue of MiTM attacks but offer no applications as working quantum cryptography protocols. Although the three-stage variation offers added security against MiTM attacks it still has security issues due to the use of a fixed θ value, making its application limited. Both protocols require some distribution protocol for the value of θ, defeating the purpose of secure QKD as the protocols rely on another communication channel. [1] offers no research into the practical implementation of the suggested protocols, lacking important design features such as error monitoring which are necessary in detecting eavesdroppers. However, despite its limitations the contribution of [1] can still prove relevant in the design of modern quantum cryptography protocols as a reference point for preventing MiTM attacks.

References

[1] Thomas, J. H. Variations on Kak's Three Stage Quantum Cryptography Protocol. CoRR abs/0706.2888 (2007).

[2] HSD (The Hague Security Delta). Understanding the Strategic and Technical Significance of Technology for Security – Implications of Quantum Computing within the Cybersecurity Domain. https://blackboard.swan.ac.uk/bbcswebdav/pid-3498687-dt-content-rid-3684244_2/courses/1920_CSCM38/presentations2019/HSD-Rapport-Quantum.pdf (2019).

[3] Bruss, D & Lutkenhaus, N. Quantum Key Distribution: from Principles to Practicalities. https://blackboard.swan.ac.uk/bbcswebdav/pid-3498687-dt-content-rid-3684240_2/courses/1920_CSCM38/presentations2019/9901061.pdf (2008).

[4] CSA (Cloud Security Alliance). What is Quantum Key Distribution?. https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf (2015).