Quantum in Aviation Security: ADS-B Protection with QKD

Brady Phelps
Honors Tutorial College
Ohio University
Athens, Ohio, United States
bp309420@ohio.edu

Zion Klinger-Neviska
School of EECS
Ohio University
Athens, Ohio, United States
zk250618@ohio.edu

Chad Mourning
School of EECS
Ohio University
Athens, Ohio, United States
mourning@ohio.edu

Michael Braasch
School of EECS
Ohio University
Athens, Ohio, United States
braaschm@ohio.edu

2024 Integrated Communications, Navigation and Surveillance Conference (ICNS) | 979-8-3503-9309-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICNS60906.2024.10550471

***Abstract*—Automatic Dependent Surveillance Broadcast (ADS-B) is the standard for aircraft surveillance and has been required on almost all aircraft within the National Airspace System since 2020. Data transmissions from ADS-B transponders are non-encrypted and, as a result, pose a variety of safety and security risks. Prior research has been conducted that provides solutions for retrofitting ADS-B systems with FPE (format-preserving encryption) algorithms. These require safe key distribution protocols to create the keys between parties. Classical key distribution protocols have been proposed and recently tested with some promise. However, with the rise of quantum computing, there is also a need for protection from future quantum threats. This paper explores the implementation of a quantum key distribution (QKD) protocol for the key generation of ADS-B transmissions using an FPE encryption algorithm with both free-space and optical links for air and ground distribution. This creates a level of security bounded by the laws of physics, as opposed to proposed key distribution methods, which are vulnerable to being hacked by both quantum and classical algorithms. Coupled with creating the protocol, a simulation is created to visualize the approach. This research stands to benefit all aircraft, national and international, that implement the ADS-B system, creating an increased sense of security, safety, and order in the air.**

***Index Terms*—ADS-B, QKD, Security, Aviation, Avionics**

I. Introduction

A. Vulnerability

Automatic Dependent Surveillance-Broadcast (ADS-B) is a critical surveillance technology used in aviation, allowing aircraft to broadcast their position to enhance situational awareness and safety. ADS-B plays a crucial role in preventing collisions and improving air travel safety. However, security is a significant concern since ADS-B transmissions are non-encrypted and lack authentication, making it vulnerable to unauthorized access and spoofing.

In March of 2014, researchers at the Air Force Institute of Technology conducted a project in which they evaluated encryption methods capable of running on ADS-B as suggested by the National Institute of Standards and Technology (NIST) [6]. The paper concluded that a type of symmetric key algorithm, known as FPE (format-preserving encryption) [10], are capable for retrofitting encryption to ADS-B. However, due to the nature of symmetric key algorithms, which require both parties to share a key, there is a need for safe key distribution and generation because, without secure keys, the encryption is worthless. Agbeyibor [6] suggests an initial scheme to share the key offline or create variations of existing schemes, such as the distribution scheme used in IFF (Identification friend or foe) transponders. Additionally, in a paper published in 2015 by a group of researchers from George Mason University created a protocol for classical key distribution for ADS-B systems [17]. Recently, another paper was released by the Air Force Institute of Technology, which covered a potential key distribution scheme for the FPE algorithms utilizing uni-directional cryptography [12]. This work presents a feasible solution for ADS-B encryption with the addition of a secure software module to parse Mode-S packets [33]. This work was then realized through experimentation, when Air Force researchers tested the protocol and found it feasible [11].

The primary contribution of this paper is an alternative solution that utilizes quantum technology for the creation of a secure quantum key distribution (QKD) protocol that suits the needs of ADS-B for now and in the future. This paper explores applications of quantum key distribution schemes in modern-day applications. The work conducted provides solutions to modern and future communications security flaws. The key exchange shown will generate a secure key for encrypted ADS-B and protect against malicious parties gathering information about some of the government's most high-risk assets, e.g. Air Force One. The work stands to expand on the utility of quantum key distribution in aviation and prepare aviation security for a post-quantum era. The findings here relate directly to ADS-B; however, the key distribution apparatus is independent of the ADS-B transmitter and could be utilized for key swapping for other needs.

B. Layout

The remainder of this paper is laid out as follows: Section II provides necessary background on ADS-B, Quantum Information, and the BB84 Protocol; Section III analyzes the capabilities of ADS-B, and how we can utilize ADS-B specifications to send encrypted information; Section IV dives into the key generation protocol, and how the BB84 protocol [9] is implemented for secure key exchange; Section V covers noise considerations and how noise will affect hardware considerations and protocol reliability; Section VI

Choose Ohio First Scholarship Program.

showcases features of the simulation used to illustrate the effectiveness of the protocol; Section VII concludes the paper with key takeaways; Section VIII previews potential future work and research in this field.

II. Background

A. ADS-B

Automatic Dependent Surveillance-Broadcast (ADS-B) is a surveillance technology that allows aircraft to broadcast their position [5]. This information is received by both air traffic control (ATC) and other aircraft as a means to share positions for situational awareness and safety when flying. This system helps avoid collisions and provides a degree of safety in the air. This technology is in the process of being adopted by aviation agencies across the world. In 2020 [4], the FAA issued a mandate with the requirement of an ADS-B Out transmission for almost all aircraft within the National Airspace System flying as outlined in 14 CFR 91.215 [30]. The technology stands as an alternative to secondary surveillance radar, with benefits such as real-time precision positional tracking and improved safety. However, ADS-B has a major security vulnerability, as its transmissions are neither encrypted nor authenticated; this means anyone can read information sent out through ADS-B. This can be seen from services like adsbexchange.com [1] and radarbox.com [2], where non-government entities have access to information regarding all aircraft with an ADS-B transponder. This allows a given person to accurately locate aircraft of importance, such as Air Force One, on any given day by logging into one of these public websites. This tracking has recently been a controversial topic in the news, with celebrities such as Taylor Swift and Elon Musk complaining about personal safety concerns from their private jets being tracked [16], [25].

With this lack of authentication, it is also possible for outside parties to spoof ADS-B transmissions [18]. This means outside parties can create false signals to create the illusion of an aircraft being in areas where there are actually no aircraft. Spoofing ADS-B can lead to heightened levels danger for all involved. These flaws call for a solution, in which privacy preservation encryption is included without hindering current ADS-B functionality, to return safety and security to the forefront of air navigation.

B. Quantum Information

Quantum information is a growing field with major implications for the future of security and networks throughout the world. In May 2022, President Biden announced two executive directives involving the advancement of quantum technologies [3]. This has brought more attention to the field and showcased the importance of the field in securing one of the world's leading governments. Many QKD (Quantum Key Distribution) protocols have been developed for secure quantum networks and communications [20]. These protocols outperform modern classical protocols in several respects, as they are protected by the laws of physics as opposed to classical protocols, which have the potential to be solved, for instance, Quantum algorithms, such as Shor's Algorithm for factoring large number [27], have shown the potential to break modern encryption and key distribution methods like RSA [24]. QKD protocols can maintain a higher level of security due to the quantum phenomena of entanglement and superposition [7]. These phenomena allow for information to exist in multiple states at the same time and allow seemingly unrelated pieces of data to define each other. These unique properties are the fundamental principles of quantum encryption and will serve as stepping stones for the protocol developed in this paper.

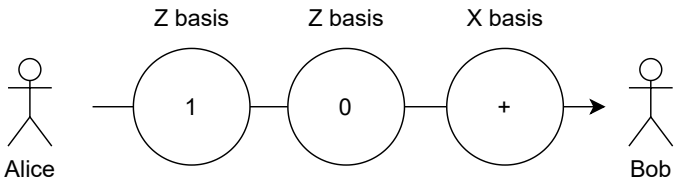

Fig. 1. Alice prepares a series of qubits in a randomly chosen basis. She then sends these qubits to Bob.

We have seen the rise of potential quantum key distribution applications within the field of aviation in recent years. Researchers at Ludwig Maximilian University experimentally proved quantum key distribution between aircraft and ground [19], while researchers in Canada also experimentally proved QKD between ground and aircraft [33]. With the security vulnerabilities found in aircraft systems such as ADS-B and the rise of quantum threats, it is important for the United States and other governments to explore quantum-backed communication within aircraft.

C. BB84 Protocol

The *BB84 protocol* is a *prepare and measure* quantum key exchange protocol [9]. The BB84 protocol has been proven to work in both plane-to-ground and ground-to-plane transmissions [19], [22]. For rigorous background information on quantum key distribution, consider the survey conducted by researchers at the University of Connecticut titled "An Introduction to Practical Quantum Key Distribution" [7].

In brief, the following describes the BB84 protocol:

- Alice (one can think of Alice as our ATC) attempts to create a shared secret key pair with Bob (one can think of Bob as an aircraft). Eve (one can think of Eve an an illicit actor) attempts to eavesdrop and collect their key.
- Alice prepares a series of qubits, or quantum bits, utilizing one of two bases: the X basis or the Z basis. Each basis represents an orthogonal set of polarizations. Within each basis, there are two potential states a qubit can exist in, these states are orthogonal. In the Z basis, the polarizations are denoted as 1 and 0. In the X basis, the polarizations can exist in either + or -. When the parties send information, they essentially encrypt a binary 1 or 0 into one of these four polarizations. See figure 1 for details.

- For each qubit Alice prepares, she will send the qubit to Bob **without** telling him the basis she prepared it in. This means that when Bob receives the qubit he will not know the preparation basis.
- If Alice were to send the classical value 1 in the Z basis, she would send a $|1\rangle$ qubit, whereas if she were to send the value 1 in the X basis, she would send a $|+\rangle$ qubit. This notation, known as dirac notation [14], represents the quantum state of our qubit.
- When Bob receives these values, he will randomly choose the Z or X basis to measure. If he chooses the correct basis, he will measure the correct classical bit Alice sent. See Figure 2. If Bob measures Alice's $|1\rangle$ bit in the Z basis, he will measure a 1, and if he measures Alice's $|+\rangle$ bit in the X basis, he will measure a 1. If he happens to measure in a mismatched basis, he will receive a random 1 or 0, which cannot be used for the key.
- Once every bit has been sent, Alice will publicly announce her prepared states, and Bob will announce his chosen measurement bases. See Figure 3.
- If the state Alice prepared matches the state Bob chose to measure, they should have the same readings and will have a secured bit. If there is a mismatched basis, that bit will simply be discarded. We can share these choices publicly because measurement choice does not tell Eve the value of the qubit, just the basis at which it was prepared.
- Alice and Bob will then choose a subset of their bits that match to announce publicly. If all shared bits match, they will know with confidence proportional to the number of shared bits that their communications line was safe. If the bits do not match, we will know someone has been snooping on our channel, the reason for this is introduced later in this section. The publicly announced bits are spoiled and provide no additional security and are discarded, not to be used in the final key. See figure 4.
- For additional security they will then undergo information reconciliation [9] and privacy amplification [8] under classical channels to securely generate their key using their shared bits. This process involves using a randomly selected hash function to further scramble the key to reduce any possible risks.

This protocol is provably secure [28]. Due to the nature of qubits, if Eve measures a bit, the bit will collapse onto the state of the measurement (see Figure 5); therefore if an eavesdropper (Eve) is attempting to steal part or all of the key, Alice and Bob will be aware because their supposedly matching bits will have a high statistical likelihood of not matching (see Equation 1). Unlike traditional man-in-the-middle attacks [13], due to the no-cloning theorem [31], which states it is impossible to clone a given qubit, Eve cannot capture, copy, and re-transmit any of the qubit information as it is being sent from Alice to Bob. If Eve wishes to steal information, she must measure the bit in the correct basis and

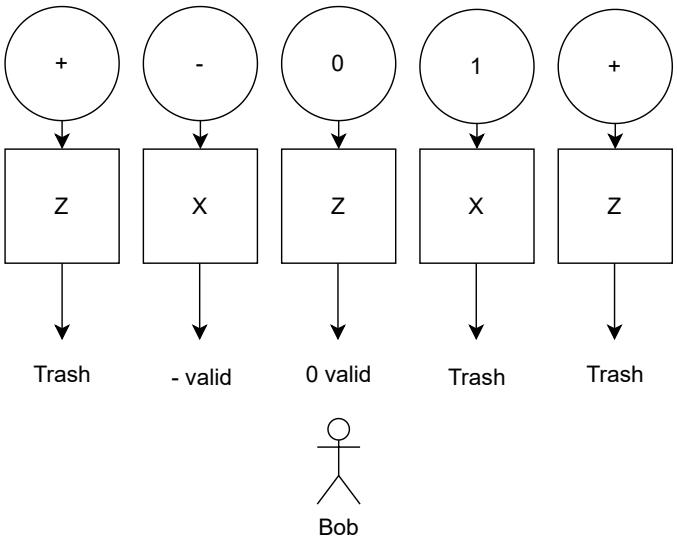

Fig. 2. Bob measures all passed qubits in a randomly chosen basis. As you can see in the picture, if Bob chooses to measure in the same basis Alice prepares in, he will receive a valid bit.

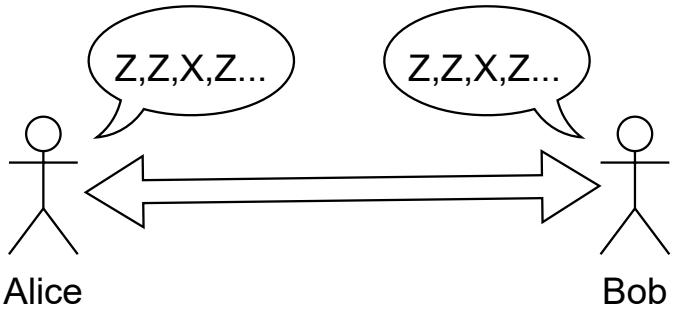

Fig. 3. Bob and Alice share their prepare and measurement choices. They will be throwing away all mismatching choices from their remaining key. At the end of this step, they will have each have a bit string containing the bits from their identical prepare and measure choices.

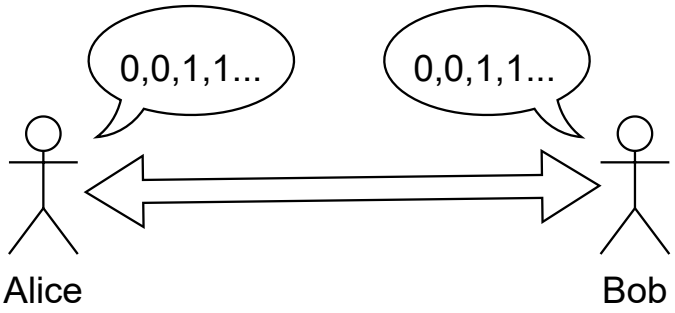

Fig. 4. Bob and Alice share K bits from their secure values. At this step, all of their shared bits should match. The more bits shared, the more confident we can be that all of our bits match.

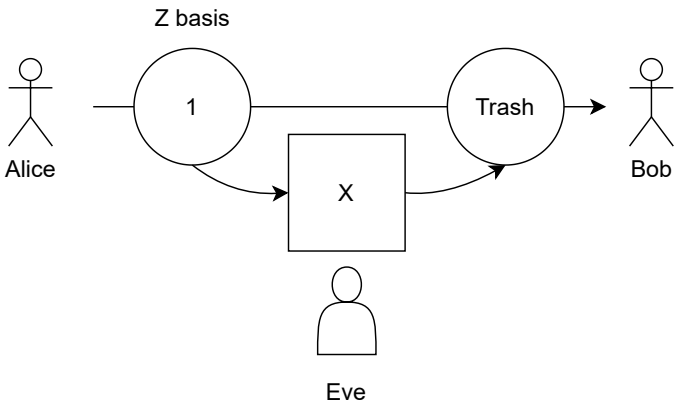

Fig. 5. Eve attempts to snoop on the communications channel and collapses the state. Whenever Eve attempts to steal a bit, there is a 1/4 probability she will collapse the state and be detected per bit.

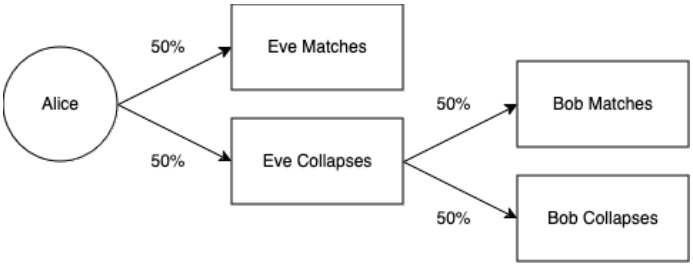

Fig. 6. The diagram shows the reasoning behind the probability Eve gets detected (Equation 1). If there is a 50% chance Eve corrupts the bit, there is another 50% chance that Bob measures in the correct basis. If Eve corrupts the bit and Bob measures in the correct basis, that is when we can detect Eves presence (25% of the time).

pass along the collapsed qubit.

Since Eve does not know which basis Alice prepares in, she has a 50% chance of measuring in the correct basis. Over a large number of bits, this risk of measuring in the incorrect basis grows for Eve, and the protocol quickly becomes secure. Equation 1 provides the probability of Eve going undetected, given a number of measured bits.

$$P(\text{undetected}) = \left(\frac{3}{4}\right)^n \quad \text{Where } n \text{ is the number of bits} \tag{1}$$

We then suggest further privacy amplification, but it is often seen as optional as the raw key is already extremely secure. There is a possibility that Eve could have secretly stolen a few bits from the key and gone undetected, so one can further secure this breach of information via privacy amplification.

Privacy Amplification involves selecting a random universal hashing function from a publicly known set of functions. The function will take a binary string equal to the length of the current key and output a key of some length shorter than the original key. The amount by which one shortens the key is most often proportional to the amount of suspected information Eve could have stolen. This means that even if Eve steals a few bits, they will not know the location of those bits in the final key or if the final key has the stolen bits at all. This process has been shown to work, even when Eve had a quantum memory [23].

III. Analyzing ADS-B Capabilities

This section describes the format of the ADS-B messages to be secured, as well as the encryption protocol to be used in the ADS-B messages.

A. ADS-B Messages

ADS-B messages come in several downlink formats (DFs). An ADS-B squitter is 112 bits wide and 120 μs long with an 8 μs preamble. These messages are transmitted at 1090 Mhz. Figure 7 showcases the contents of the multiple downlink formats updated as they will be utilized in the protocol. As you will notice, the DF-15 ME field is encrypted, this field will be encrypted using our protocol.

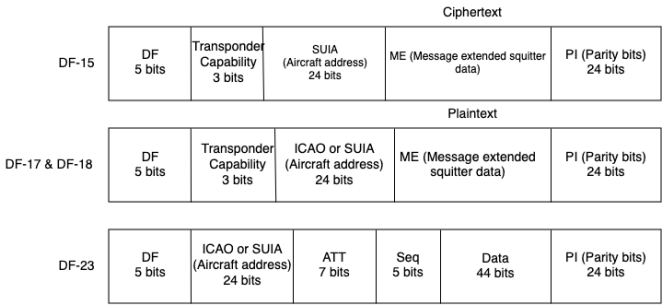

Fig. 7. ADS-B squitter message diagram for all downlink formats.

For the proposed encryption scheme, we will closely follow the method created by the AFIT team [12] and only encrypt the "Message Extended Squitter" field (ME) portion of the messages. This is done so the system can encrypt based on message types. Encryption of the ME data will be done using an FPE encryption method.

B. Format Preserving Encryption

FPE, or Format Preserving Encryption, is a form of encryption where the plain text shares the same format as the cipher text. In this protocol, we utilize FPE due to its ability to combine AES security with the capability to handle legacy data formats of variable length. Since NIST recommends the use of the FF1 block cipher for ADS-B [15] and AFIT researchers have conducted positive experiments utilizing FF1; therefore, this is the encryption method that is adopted in this paper as well. However, unlike previous papers, the protocol does not call for an SUIA (Session Unique ICAO Address) or session key to be generated and sent using DF-23 packets on ADS-B to communicate unidirectional key exchanges with home ATC. This method has been shown to work through experiment, but this method uses public unidirectional encryption, which tends to be slower than symmetric key encryption and lacks of protection against future quantum threats. In this protocol, we will perform a direct key exchange between the aircraft and

ATC using quantum and classical channels to establish a set of keys to be used for secure communications and to safely utilize FF1 encryption in ADS-B. This allows us to utilize symmetric key encryption when encrypting the ME messages. This method is faster, and through quantum channels, is more secure than public uni-directional encryption.

IV. Key Generation and Exchange

A. Setup

1) Hardware Apparatus Requirements: To realize this protocol, certain hardware requirements must be met to properly establish the quantum connections to create the keys. In Figure 8, you can see both a quantum and classical connection are needed. A classical connection can be accomplished by any number of modern communications techniques, as this channel does not need to be encrypted. However, the quantum channel does need encrypted, and also needs special hardware.

On the ground station, one will need the quantum transmitter. In a quantum connection, the source and transmitter comprise of an attenuated laser capable of sending single photons to the receiver in a variety of polarizations. For free-space connections, this has been realized through different work, – most notably, a paper titled "Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links" [32], details a configuration for assembling an apparatus suitable for QKD exchange.

Along with a photon source, a receiver is required to receive the photons. The receiver will be on the aircraft and will have a detector that will be able to receive and measure the photons sent from the ground station.

By contrast, when implementing ground links, one can use optic fiber cables to transmit qubits bi-directionally between sources. With this approach, one does not need most of the hardware required for a free-space connection, but there is the additional requirement of optic fiber cables running from the ATC to a ground hookup for the aircraft as well as a hardware module capable of sending and receiving qubits. Figure 9 illustrates a fiber connection.

2) Software Requirements: For software requirements, the ATC will require a classical secure software module capable of using the established key to decrypt the packets using the symmetric key encryption. The ATC will also require software capable of controlling the classical and quantum channels utilized in the key exchange. This will require a single program that can communicate on the classical channels to properly convey information with the aircraft regarding the current states of the protocol, and the functionality for the program to signal to the quantum source when to prepare and send qubits.

Additionally, software will need to be installed on the aircraft to properly communicate classically with the ATC, and to signal to the quantum receiver how to measure the received qubits from the ATC.

B. Key Generation Protocol

To generate the key, one will use the previously explained BB84 protocol [9] (Section II). With the ATC serving as Alice and the aircraft serving as Bob, one can follow the steps of the BB84 protocol to securely generate a shared key between both parties. This step will utilize the hardware setup to establish a quantum connection, and then undergo the BB84 protocol. This means first, the ATC will send randomly polarized qubits to the aircraft (Figure 10). Then, the aircraft will measure each of these qubits in a random basis (Figure 11). After this, the two parties will reveal their basis choices, and keep the matching choices in their secret key (Figure 12). Then, the two parties will publicly exchange parts of their secret key and check to make sure the revealed bits match (Figure 13). If the exchanged bits do not match (within expected noise ranges) we can determine someone is snooping on the communications channel.

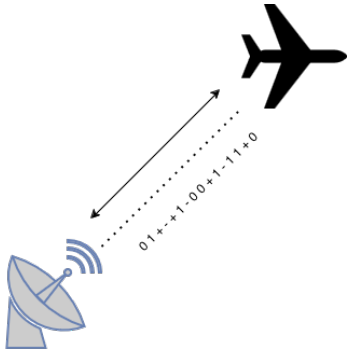

Fig. 8. Diagram of free space connection. Here, the classical communication is modelled by the solid arrow line. Over this channel, nothing needs to be encrypted. The dotted line represents the quantum channel, it is this channel where the ground station uses its photon transmitter as the source for the BB-84 protocol. The numbers represent the potential values being sent by each photon. The plane will have a receiver attached to its underside that will catch and measure the photons.

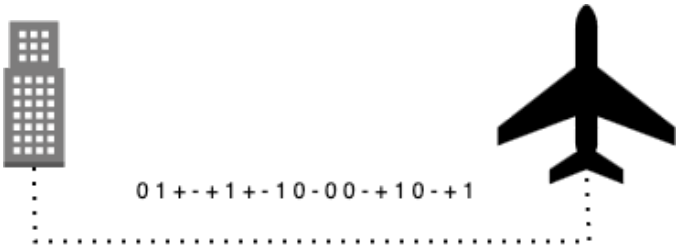

Fig. 9. Diagram of optic fiber connection. Optic fiber cables will transmit photons from our ground station to our aircraft for secure key generation while the aircraft is still grounded.

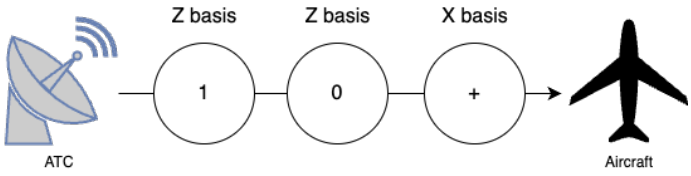

Fig. 10. The home ATC uses its photon transmitter to establish a free-space connection with the aircraft and uses this connection to send photons in either the X or Z basis at random.

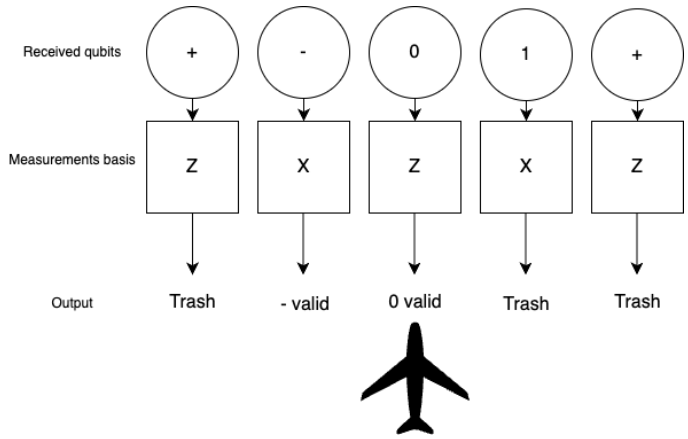

Fig. 11. The aircraft will then measure in a randomly selected X or Z basis. These measurements will result in either a 0 or 1 classical bit.

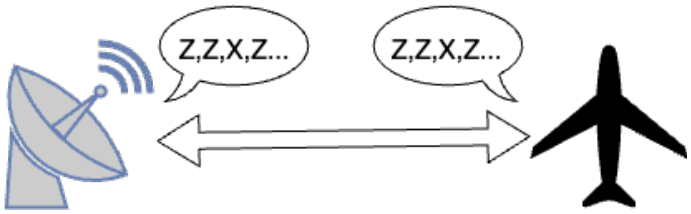

Fig. 12. The home ATC will then publicly announce the basis it prepared in, and the aircraft will announce the basis it measured in. They will keep the bits with matching prepare and measure basis.

After the initial key exchange is completed, one can undergo privacy amplification to further increase the security of our key. Once a secure random hash function is used to secure the key, there is now a shared secret key between aircraft and ATC. After this step, one can securely communicate ADS-B information with the shared key. The shared key is used by the aircraft to encrypt the ME section of the ADS-B packets using the FF1 encryption method, and the home ATC uses the shared key to decrypt these packets.

Algorithm 1 contains pseudo-code provided to further outline the steps of the protocol.

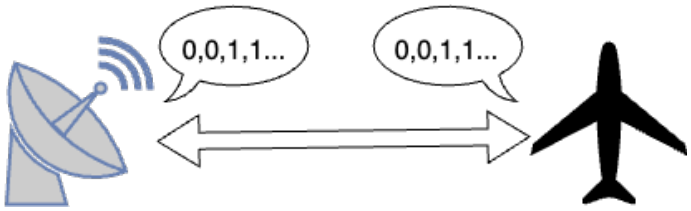

Fig. 13. The two parties will then select a subset of their matching values and publicly announce their classical bits at those values. If all goes well, the announced bits should match, and they can say with high confidence that the rest of the key is secure. They will throw out the publicly shared bits from their final key.

Algorithm 1: Secure Key Exchange and Encryption for ADSB Messages

Data: ADSB Message M, Key Length n
Result: Encrypted ADSB Message C
Input : ADSB Message M
Output: Encrypted ADSB Message C

// Key Exchange using BB84 Protocol;
Generate random bit string K_{sender} of length n;
Generate random bit string $K_{receiver}$ of length n;
Prepare qubits in random basis according to K_{sender};
Send qubits to receiver;
Receiver measures qubits according to $K_{receiver}$;
Communicate basis used for each qubit;
Detect eavesdropping using basis mismatches;
Establish secure key K_{shared} using matching basis measurements;

// Encryption using FF1 Encryption Protocol;
$C \leftarrow$ FF1Encrypt(K_{shared}, M);
return C;

V. Noise

In theory, quantum communication channels are perfect and do not have any error. However, with the limitations of current equipment, error rates are a hazard to many quantum communication systems. There are quantum error correcting codes [26] that limit the amount of error that noise may cause to a system, but this is still a constraint on modern systems and will be a particularly challenging feature for this protocol. In the case of optic fiber ground transmissions, QBER (quantum bit error rates) are less of a concern, as optic fiber communications channels have been proven and commercialized with success [29]; however, for the free space links, this becomes a larger problem. In the experimental realization of ground to plane BB84 key exchanges conducted by the University of Waterloo, noise generated by the moving plane and the environment presented issues [22]. Some mitigating adaptations can be made to improve results; for instance, the trials were only ran at night, due to the optical interference caused by the sun.

Quantum error also presents a challenge when catching Eve. As mentioned before, in the BB84 protocol, Alice and Bob will share the values of some of their matching measurements, and if the values do not match, they know an eavesdropper exists. With this introduction of noise, this is no longer the case, as there will be a certain level of expected error. This creates a bound, which is different based on the security proof being used and the level of natural noise in a system. Using this bound, one can still confidently check against an attacker, however, if the attacker tries to steal one or two bits in a very long message, the attacker could hide in this natural noise. That is why it is important to undergo further privacy amplification to ensure the attacker has no idea where their stolen bits lie within the secure key (if the bits are even in the final key).

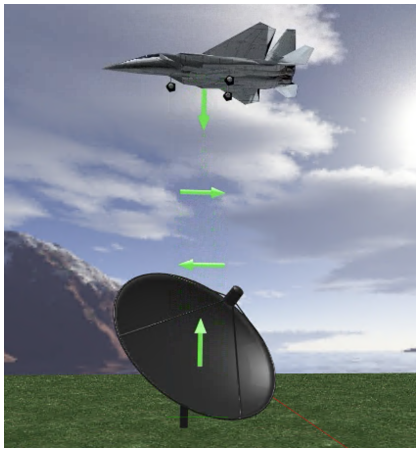

Fig. 14. The dish represents the ATC as it sends photons in a variety of polarizations to the aircraft.

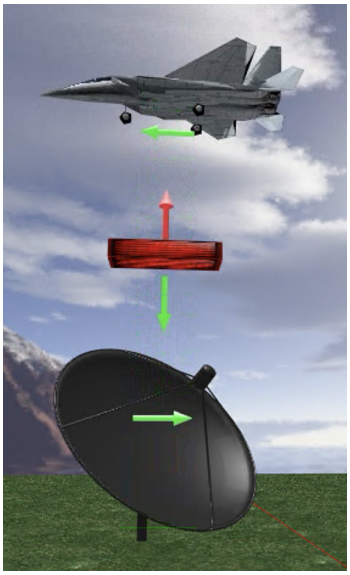

Fig. 15. The figure shows an eavesdropper, represented by the red block, interfere with the communications link. This corrupts our photon and turns it red, representing a collapsed qubit of the wrong basis.

VI. Simulation

Along with the protocol proposal, an educational simulation has been created. This simulation illustrates photons being sent from a ground station to aircraft. It also includes a live noise graph, and snooping capabilities. The simulation showcases the effectiveness of the protocol in securing against potential threats, and assists in explaining the methods of the protocol. See Figures 14, 15, and 16 for screen captures of the simulation.

VII. Conclusions

The protocol provided is suitable for the creation of a quantum-secured key to be used in ADS-B encryption. The scheme is also capable of creating quantum keys for other avionics systems and can be seen as a contemporary application for quantum technology. The protocol is currently not

Fig. 16. This figure shows the simulation with the simulator controller and noise graph. The simulation allows for varying link speeds and includes an interactive noise graph that aligns with the simulation.

feasible for mass deployment due to the nature, rarity, and expense of current quantum hardware; however, it is suitable for the creation of quantum keys during flight for aircraft that require a higher level of security, such as Air Force One. With the post-quantum era approaching, it is important to address modern security problems with solutions capable of surviving in the future, and quantum key distribution is a mode of key exchange that maintains protection in a post-quantum world.

VIII. Future Works

Possible areas of future work include: experimental realization of the quantum key exchange with the ADS-B transponder, further work on secure key applications within avionics systems, and extending the portfolio of key exchange mechanisms from terrestrial and airborne, to marine and orbital applications. In parallel to the work in this paper, the authors are working on other projects in the field of quantum computing educational simulations.

IX. Acknowledgements

This work was supported in part by Choose Ohio First program 19.38 [21].

References

[1] *adsbexchange*. http://adsbexchange.com. Accessed: 2023-10-04.
[2] *radarbox*. https://www.radarbox.com/. Accessed: 2023-10-04.
[3] 2022. Fact sheet for Biden Presidential Directives.
[4] *Airspace*.
[5] *Automatic Dependent Surveillance-Broadcast (ADS-B)*.
[6] R. C. Agbeyibor, *Secure ads-b: Towards airborne communications security in the federal aviation administration's next generation air transportation system*, (2014).
[7] O. Amer, V. Garg, and W. O. Krawec, *An introduction to practical quantum key distribution*, IEEE Aerospace and Electronic Systems Magazine, 36 (2021), pp. 30–55.
[8] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, *Generalized privacy amplification*, Information Theory, IEEE Transactions on, 41 (1995), pp. 1915 – 1923.
[9] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science, 560 (2014), pp. 7–11.

[10] J. BLACK AND P. ROGAWAY, *Ciphers with arbitrary finite domains*, in Topics in Cryptology — CT-RSA 2002, B. Preneel, ed., Berlin, Heidelberg, 2002, Springer Berlin Heidelberg, pp. 114–130.

[11] R. M. F. B. P. B. E. K. C. J. A. M. BRANDON C. BURFEIND, BRET M. CUNNINGHAM, *A limited demonstration of ads-b security*, tech. rep., United States Air Force, 2019.

[12] B. BURFEIND, R. MILLS, S. NYKL, J. A. BETANCES, AND C. SIELSKI, *Confidential ads-b*, in 2019 IEEE Aerospace Conference, 2019, pp. 1–11.

[13] F. CALLEGATI, W. CERRONI, AND M. RAMILLI, *Man-in-the-middle attack to the https protocol*, IEEE Security & Privacy, 7 (2009), pp. 78–81.

[14] P. A. M. DIRAC, *The Principles of Quantum Mechanics*, Clarendon Press, Oxford, 1927.

[15] M. DWORKIN, *NIST Special Publication 800-38G — Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*, Special Publication 800-38G, National Institute of Standards and Technology, 2016.

[16] S. HOLLISTER, *Elon musk's private jet tracker threads twitter bot*, The Verge, (2023).

[17] T. KACEM, D. WIJESEKERA, P. COSTA, J. CARVALHO, M. MONTEIRO, AND A. BARRETO, *Key distribution mechanism in secure ads-b networks*, in 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), 2015, pp. P3–1–P3–13.

[18] D. V. KOŽOVIĆ AND D. Ž. UREVIĆ, *Spoofing in aviation: Security threats on gps and ads-b systems*, Vojnotehnički glasnik/Military Technical Courier, 69 (2021), pp. 461–485.

[19] S. NAUERTH, F. MOLL, AND M. RAU, *Air to ground quantum key distribution*, Nature Photon, (2013).

[20] A. I. NURHADI AND N. R. SYAMBAS, *Quantum key distribution (qkd) protocols: A survey*, in 2018 4th International Conference on Wireless and Telematics (ICWT), 2018, pp. 1–5.

[21] OHIO DEPARTMENT OF HIGHER EDUCATION, *Choose Ohio First*. https://highered.ohio.gov/initiatives/affordability/choose-ohio-first, n.d. Accessed: February 18, 2024.

[22] C. J. PUGH, S. KAISER, J.-P. BOURGOIN, J. JIN, N. SULTANA, S. AGNE, E. ANISIMOVA, V. MAKAROV, E. CHOI, B. L. HIGGINS, AND T. JENNEWEIN, *Airborne demonstration of a quantum key distribution receiver payload*, Quantum Science and Technology, 2 (2017), p. 024009.

[23] R. RENNER, *Security of quantum key distribution*, International Journal of Quantum Information, 06 (2008), pp. 1–127.

[24] R. L. RIVEST, A. SHAMIR, AND L. ADLEMAN, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 21 (1978), pp. 120–126.

[25] ROLLING STONE, *Taylor swift's lawyers threaten student over private jet tracker*, Rolling Stone, (2022).

[26] P. W. SHOR, *Scheme for reducing decoherence in quantum computer memory*, Physical Review A, 52 (1995), p. R2493.

[27] P. W. SHOR, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing, 26 (1997), pp. 1484–1509.

[28] P. W. SHOR AND J. PRESKILL, *Simple proof of security of the bb84 quantum key distribution protocol*, Physical Review Letters, 85 (2000), p. 441–444.

[29] TOSHIBA, *Toshiba Quantum Key Distribution (QKD) Products*, n.d. Accessed: March 15, 2024.

[30] U.S. GOVERNMENT PUBLISHING OFFICE, *Title 14: Aeronautics and space, part 91: General operating and flight rules, subpart b: Flight rules, section 91.215: Atc transponder and altitude reporting equipment and use*, 2023. Electronic Code of Federal Regulations.

[31] Z. W. WOOTTERS, W., *A single quantum cannot be cloned.*, (1982), p. 802–803.

[32] Z. YAN, E. MEYER-SCOTT, J.-P. BOURGOIN, B. L. HIGGINS, N. GIGOV, A. MACDONALD, H. HUBEL, AND T. JENNEWEIN, *Novel high-speed polarization source for decoy-state bb84 quantum key distribution over free space and satellite links*, Journal of Lightwave Technology, 31 (2013), pp. 1399–1408.

[33] J. YIN, Y. CAO, Y.-H. LI, S.-K. LIAO, L. ZHANG, J.-G. REN, W.-Q. CAI, W.-Y. LIU, B. LI, H. DAI, G.-B. LI, Q.-M. LU, Y.-H. GONG, Y. XU, S.-L. LI, F.-Z. LI, Y.-Y. YIN, Z.-Q. JIANG, M. LI, J.-J. JIA, G. REN, D. HE, Y.-L. ZHOU, X.-X. ZHANG, N. WANG, X. CHANG, Z.-C. ZHU, N.-L. LIU, Y.-A. CHEN, C.-Y. LU, R. SHU, C.-Z. PENG, J.-Y. WANG, AND J.-W. PAN, *Satellite-based entanglement distribution over 1200 kilometers*, 2017.