Getting Civil Aviation Ready for the Post Quantum Age with LDACS

Daniel M. Mielke, Nils Mäurer, Thomas Gräupl, Miguel A. Bellido-Manganel

Deutsches Luft- und Raumfahrtzentrum e. V.

Digitisation has finally arrived in civil aviation: A new, feature rich communication, navigation, and surveillance system called LDACS is going to be deployed. An important aspect of LDACS is its cyber-security features. Since aeronautical equipment is used for long times, possibly decades, it is important to take future risks into account – including quantum computer driven cyberattacks. This article describes the first in-flight demonstration of Post-Quantum Cryptography in aviation on the basis of LDACS.

1 Introduction

Digital communications became a part of people's everyday life during the last years. However, in aviation, many communication tasks are still performed using analog voice radio – with all the disadvantages analog systems have. This includes comparatively low bandwidth efficiency, low sound quality (leading to potentially dangerous misunderstandings), and the lack of encryption and authenticity checks based on cryptography.

Although the intense growth of the aviation sector has been interrupted by the worldwide measures against the coronavirus, the trend to more modern aircraft collecting and exchanging more and more data is not stopped.

The L-band Digital Aeronautical Communications System (LDACS) is a digital system designed to bring aeronautical Communication, Navigation and Surveillance (CNS) into the 21st century. Especially on the physical layer, it makes use of modern communication techniques as they are used in established wireless communication systems like IEEE 802.11 ("Wifi") and the 4G phone network. LDACS will only be used for "operational" aeronautical communication i.e. it will be used for digital flight guidance, but not for passenger entertainment.

One critical aspect in operational aeronautical communications is security: How can it be ensured that confidential information is only received by authorised parties? How can the origin of a received message be verified? How is it guaranteed that a message has not been modified during transmission? While the first question addresses the cryptographic task of encryption, the second question addresses authentication, and the last question addresses integrity. These three properties are of high importance in a communication system whose messages directly affect flight guidance – especially in an environment where an increasing number of tasks is automated. This increasing level of automation is not the only ongoing development that motivates research on security in aeronautical communications: The broad availability of powerful computers and Software Defined Radios (SDRs) extends the circle of potential attackers on wireless systems in general and on the communication infrastructure of civil aviation in particular. This makes state-of-the-art cyber-security a must for digital aviation.

However, it has been shown that many widely used crypto-systems cannot be considered safe anymore, once quantum computers with a sufficient amount of qubits become available. Hence, there is ongoing research on the topic of post-quantum security, i.e. cryptographic algorithms that are "immune" against quantum computer driven attacks.

Luckily, the breakthrough in quantum computation enabling massive attacks on current encryption schemes is not expected to happen tomorrow. Nevertheless, the development of post-quantum secure crypto-systems is already of high relevance – especially for systems used in environments with long technology life spans like civil aviation. Since LDACS is expected to be used for decades, there is a high chance, that sophisticated quantum computers may become available during its life time. Thus, before deploying a

Figure 1: The result of a successful inflight McEliece encapsulated AES-256 key exchange shown on the terminal of the control computer aboard DLR's Falcon 20E research aircraft.

communication system that is used for critical infrastructure, it must be ensured that it can be operated securely for this duration.

2 Digital Flight Guidance with LDACS

LDACS is one of the radio access technologies realising the future aeronautical communications infrastructure that will allow aircraft to be digitally connected to the aeronautical telecommunications network (ATN) during all phases of flight [1]. Specifically, LDACS shall connect aircraft operating in the continental airspace by deploying a network of ground stations, each one of them covering a part of the airspace. An aircraft carrying an LDACS radio will then be able to connect to the ATN by communicating with the LDACS ground station covering its current location. In this way, it is similar to cellular mobile communication networks.

Technically, LDACS is a cellular broadband system based on Orthogonal Frequency-Division Multiplexing (OFDM) technology and supports quality-of-service while taking the requirements of aeronautical services into account [2]. It shares many technical features with 4G wireless communications systems. In addition to communication, LDACS supports navigation with its built-in ranging functionality.

Safety and security are deeply interrelated in aviation and flight guidance [3, 4]. For this reason, LDACS has been designed with a security architecture relying on state-of-the-art cryptography [5, 6, 7]. However, as we alluded to, this might not be good enough, if recent developments in Post-Quantum Cryptography (PQC) are not taken into account.

3 Post Quantum Cryptography

In general cryptography is "the mathematical science that deals with transforming data to render its meaning unintelligible, prevent its undetected alteration, or prevent its unauthorized use" [8], or in simpler terms: "Cryptography is loosely the science of encrypting and decrypting secret codes" [9]. Before we go into

depth about "Post-Quantum Cryptography (PQC)", we would like to introduce some basic cryptographic operations and terms: First we want to introduce our two communication partners, Alice and Bob¹. If Alice and Bob want to communicate securely with each other, Alice and Bob can encrypt a message and Bob can decrypt that message. If they want to use a symmetric crypto-system (e.g. Advanced Encryption Standard (AES) [10]), they first have to agree on such a shared secret. A symmetric crypto-system means, Alice and Bob use the same secret as the key to encrypt and decrypt messages. Agreeing on a shared secret over an insecure communication channel is hard and for that purpose key exchange protocols exist, e.g. Diffie-Hellman Key Exchange (DHKE) [11].

In asymmetric crypto-systems, like Rivest–Shamir–Adleman (RSA) [12], both Alice and Bob have each a public key and a private key. Thus Alice knows Bob's public key and Bob knows Alice' public key. If Alice wants to encrypt a message for Bob, she encrypts that message with Bob's public key and sends that message to Bob. Since Bob is the only person, that knows his private key, only he can decrypt that message.

Another important use of asymmetric crypto-systems are signatures, which can be used to digitally sign messages (e.g. via Digital Signature Algorithm (DSA) [12]) by one of the communication partners. If Alice wants to make sure, that Bob really believes, that she sent a message, she signs that message with her private key. Bob, and everyone else in possession of Alice's public key, can now verify that this message was actually sent by Alice.

The term "Post-Quantum Cryptography (PQC)" is used in the context of cryptography to describe the idea that an attacker has access to a quantum-computer, which can calculate the underlying mathematical problems much more efficiently than a classical computer [13]. Thus cryptographers divide cryptographic security levels in pre-quantum (no practical quantum-computer exists) and post-quantum (a practical quantum-computer does exist). The implication being, that some of today's most relevant cryptographic systems, that are secure in a pre-quantum world,

¹ Alice and Bob are generic names traditionally used to designate cryptographic communication partners.

Figure 2: LDACS flight trials using four LDACS ground stations deployed in southern Germany and one LDACS airborne station carried by a Dassault Falcon 20E aircraft. Copyright of background map: Map data ©2020 GeoBasis-DE/BKG (©2009), Google. [22]

are no longer secure in a post-quantum world. The reason is, that these cryptographic systems' security is based on mathematical problems, that cannot be solved within a reasonable amount of time using a classical computer. One famous example is the factorization of large integers that cannot be solved by non-quantum computers in any practical way. Thus, cryptographic systems making use of this property, like the RSA public-key system, are considered safe (assuming a sufficient key length) while no quantum computers are available.

However, in 1994, Shor [14] introduced Shor's algorithm, which is a fast quantum algorithm to find the prime factorization of any positive integer [15]. Shor's algorithm applied to RSA and combined with a large enough quantum-computer would break RSA. Other cryptographic operations, such as the DHKE key exchange or the DSA signature scheme, or the elliptic curve variations of these schemes would be broken, as well [15].

In 1996, Grover introduced Grover's algorithm [16], which speeds up searching in unordered data-structures of size N from N operations to $\sqrt{N}$. Again applied with a large enough quantum computer, Grover's algorithm reduces the security level of the symmetric crypto-system AES with a key length of 128bit to 64bit in a post quantum world, thus effectively halving security levels.

Both attacks would require thousands logical and, due to faulty-behavior of qubits, millions of physical qubits [17]. To put this into perspective: In 2021 the IBM Quantum Eagle processor will launch with 127-qubits and IBM plans for a 1121-qubit IBM Quantum Condor processor in 2023 [18]. Both machines would be the most powerful public quantum-computers to date. With that, a million qubit machine could well be decades away [18].

In order to begin defending against the possible threat that quantum-computers pose to the world's most used crypto-systems, post-quantum robust crypto-systems are, however, currently being developed and standardised. Post-quantum crypto-systems are based on mathematical problems that are equally impractical to be solved by quantum computers and classical computers. The

National Institute of Standards and Technology (NIST) started its standardisation work in

2017, in search for the most promising post-quantum crypto-systems in a series of three rounds [19]. One of the most promising candidates and finalist for public-key crypto-systems and key establishment algorithms is the McEliece crypto-system, that has been invented in 1978 [20].

Every computer and practically all digital communication systems use error correction codes to provide highly reliable services. A straightforward example is a repetition code, where every bit is sent three times to allow the correction of a single bit-flip during transmission (e.g. 0 1 $\rightarrow$ 000 111). There exist many other (and way more efficient) error correction codes like Reed-Solomon Codes, Convolutional Codes or Goppa Codes. The latter code class is an example for a code that is not only used for error correction, but that can also be used for encryption. This is called code-based cryptography. The security of the McEliece crypto-system is based on the NP-hard problem of decoding a general linear code like the Goppa Code. Currently, the major drawback of McEliece is its very large key size. For example, to reach a similar security level as AES-128, McEliece requires a key size of roughly 1MB. Encryption and decryption, however, are faster than with RSA [19].

In our flight trials, we used McEliece keys, that strongly benefited from advancements in key size reduction in recent years [21]. The key size could be reduced to 200kB. A successful key exchange is shown in Figure 1.

4 Flight Trials

After years of development and tests in the laboratory and thorough computer simulations, LDACS was ready to be demonstrated in flight trials in 2019. Within the German national project MICONAV², the German Aerospace Center (DLR), together with its project partners³, conducted the first in-flight LDACS

² Migration towards Integrated COM/NAV Avionics

³ Rohde & Schwarz GmbH & Co. KG, Bögl & Partner Systemtechnik GmbH, iAd – Gesellschaft für Informatik, Automatisierung und Datenverarbeitung GmbH, Technical University of Munich

Figure 3: Overview of ground and airborne LDACS equipment. [23]

demonstration in March and April 2019 in Germany [22]. We employed four experimental LDACS ground stations and one experimental LDACS airborne station. In order to recreate the expected cellular deployment of LDACS, the four LDACS ground stations were distributed in the south-west of Germany, as it can be seen in Figure 2.

Figures 3a to 3c show the LDACS ground station located in the DLR premises in Oberpfaffenhofen and the LDACS airborne station, respectively. The airborne station was installed into the Dassault Falcon 20E DLR research aircraft shown in Figure 4.

The flight trials, which consisted of six flights over two consecutive weeks, allowed us to conduct numerous experiments addressing the communication, navigation, and surveillance capabilities of LDACS. Through these experiments, we were able to demonstrate that LDACS can support applications relevant to air traffic management, such as Controller–Pilot Data Link Communications

(CPDLC) communications, audio streaming, as well as general-purpose data transmission and broadcast. Basically, data were generated by the different applications running on laptops connected to either the ground station or the airborne station. The generated data were transmitted over LDACS to its counterpart station, therefore enabling the applications to communicate with each other and to recreate future ATM procedures.

5 Post-Quantum Aeronautical Communication

The cryptographic protocol used in the MICONAV project follows the common approach of using a combination of an asymmetric and a symmetric crypto-system. The applied proof-of-concept consists of three parts:

- The exchange of public keys between Ground Station (GS) and

Aircraft Station (AS), denoted by PubKeyGS and PubKeyAS, respectively.

- The (asymmetrically encrypted) sharing of a secret session key KAES.
- The confirmation of this session key.

The first two parts of the protocol are visualized in Figure 5 in more detail. The mutual exchange of the public keys is performed in step 1) and 2): Both communication partners, i.e. GS and AS, generate their respective McEliece key pair (one private key and one public key) before they send their public key to the other partner. In step 3), the AS generates a random key of length 256bit called session key KAES. This key is then encrypted with the public key of the GS using the McEliece scheme as shown in step 4). Then, the encrypted session key is sent to the GS. Step 5) shows how the GS receives the encrypted key and decrypts it using its private key PrivKeyGS. Finally, the GS stores the decrypted session key KAES. Both communication partners share a secret KAES although this secret has never been transmit in clear-text.

Additionally, we have also implemented a confirmation protocol which guarantees that both parties use the same key [24]. The protocol is based on using a randomly generated number-usedonce "nonce" and a timestamp that are encrypted using the KAES. By mutually exchanging this information, both communication partners can verify that the same session key is used. From now on, all data exchanged between AS and GS can be symmetrically encrypted using the session key KAES. In MICONAV, the AES crypto-system was used for this purpose using a key length of 256bit.

The described implementation is a first proof-of-concept and not ready for deployment yet. The key exchange as shown in Figure 5 is vulnerable to Man-in-the-Middle (MITM) attacks: Imagine, an attacker would infiltrate all communication between GS and AS starting from the very first step by acting as the AS with respect to the actual GS while acting as the GS with respect

Figure 4: DLR's research aircraft Dassault Falcon 20E (D-CMET) used in the experiments. [23]

to the actual AS. In the current setup, neither the actual AS nor the actual GS have a chance to realize this MITM attack and the attacker has access to the symmetric keys – and consequently to all messages encrypted using these keys. This vulnerability can be addressed by performing a signed key exchange; however this requires at least some pre-shared information like certificates. Another option would be to perform the exchange of the public keys in advance via a secure side channel, e.g. smart cards. This would also simplify the protocol in Figure 5, since the first two steps could be skipped.

6 Summary

Critical communication systems like the L-band Digital Aeronautical Communications System (LDACS) discussed in this article are potentially used for decades. It is important to take foreseeable cyber-security threats into account that may arise in this time. A particular threat that is expected to materialise within the next decade, is the threat of quantum computers rendering many state-of-the-art cryptography systems vulnerable. We strive therefore to introduce post-quantum secure cryptography into aviation.

In a first step of getting civil aviation ready for the post-quantum age, we demonstrated McEliece cryptography for aeronautical communications in flight. The flights performed in the MICONAV project were the first time that an LDACS demonstrator was flown aboard an aircraft, confirming the expected performance of LDACS, and demonstrating post-quantum cryptography in aviation for the first time.

Clearly, the results presented in this article are just the first step in realising our vision of postquantum secure aviation, and much work remains to be done. However, our results demonstrate that if recent advances in cryptography and aeronautical communication systems are combined, the goal is already within reach.

Abbreviations

AES	Advanced Encryption Standard
AS	Aircraft Station
CNS	Communication, Navigation and Surveillance
CPDLC	Controller–Pilot Data Link Communications
DHKE	Diffie-Hellman Key Exchange
DSA	Digital Signature Algorithm
GS	Ground Station
LDACS	L-band Digital Aeronautical Communications System
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
RSA	Rivest–Shamir–Adleman
SDR	Software Defined Radio

References: [1] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger. LDACS: Future Aeronautical Communications for Air-Traffic Management. *Communication Magazine*, 52(5):104–110, May 2014. [2] T. Gräupl, C. Rihacek, and B. Haindl. LDACS A/G Specification. SESAR2020 PJ14-02-01 D3.3.030, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, August 2019. [3] M. Slim, B. Mahmoud, A. Pirovano, and N. Larrieu. Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey. *Computer Science Review*, 1112:1–29, May 2014. [4] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. On perception and reality in wireless air traffic communication security. *IEEE transactions on intelligent transportation systems*, 18(6):1338–1357, 2016. [5] Mäurer, N. and Bilzhaue, A. A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS). In 37th Digital Avionics Systems Conference (DASC), pages 1–10, New York, NY, USA, Sept. 2018. IEEE. [6] N. Mäurer and C. Schmitt. Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis. In 19th Integrated Communications, Navigation and Surveillance Conference (ICNS), pages 1A2/1–1A2–13, New York, NY, USA, Apr. 2019. IEEE. [7] Mäurer, N., Gräupl, T. and Schmitt, C. Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS. In 39th Digital Avionics Systems Conference (DASC), pages 1–10, New York, NY, USA, Oct. 2020. IEEE. [8] Robert Shirey. RFC 4949 - Internet security glossary, version 2. Technical report, IETF, August 2007. [9] Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, and Gerhard Rosenberger. A course in mathematical cryptography. Walter de Gruyter GmbH & Co KG, 2015. [10] Daemen Joan and Rijmen Vincent. The design of rijndael: Aes-the advanced encryption standard. In *Information Security and Cryptography*. springer, 2002. [11] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976. [12] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. [13] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009. [14] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings*

Figure 5: Exchange of the session key K_{AES} secured by the McEliece scheme as implemented in MICONAV

35th annual symposium on foundations of computer science, pages 124–134. Ieee, 1994. [15] Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017. [16] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996. [17] Earl T Campbell, Barbara M Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, 2017. [18] Jay Gambetta. Ibm’s roadmap for scaling quantum technology, 2021. [Online]. Available: <https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/> [Accessed: January 15, 2021]. [19] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the nist post-quantum cryptography standardization process. US Department of Commerce, NIST, 2020. [20] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978. [21] Hannes Bartz and Gianluigi Liva. On decoding schemes for the mdpc-mceliece cryptosystem. In *SCC 2019; 12th International ITG Conference on Systems, Communications and Coding*, pages 1–6. VDE, 2019. [22] Miguel A. Bellido-Manganell, Thomas Gräupl, Oliver Heirich, Nils Mäurer, Alexandra FilipDhaubhadel, Daniel M. Mielke, Lukas Marcel Schalk, Dennis Becker, Nicolas Schneckenburger, and Michael Schnell. LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System. submitted to *IEEE Transactions on Aerospace and Electronic Systems*, 2021. [23] Nils Mäurer, Thomas Gräupl, Miguel A. Bellido-Manganell, Daniel M. Mielke, Alexandra Filip-Dhaubhadel, Oliver Heirich, Daniel Gerbeth, Michael Felix, Lukas Marcel Schalk, Dennis Becker, Nicolas Schneckenburger, and Michael Schnell. Flight Trial Demonstration of Secure GBAS via the L-band Digital Aeronautical Communication System (LDACS). *IEEE Aerospace and Electronic Systems Magazine*, pages 1–19, 2021. [24] M. Fischlin, F. Guenther, B. Schmidt, and B. Warinschi. Key confirmation in key exchange: A formal treatment and implications for tls 1.3. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 452–469, 2016.

Daniel M. Mielke M.Sc.

Daniel M. Mielke received his B.Sc./M.Sc. from University of Kiel in 2014/2016 and spent a term at the UBC in Vancouver. He joined DLR in 2016. His research interests are channel modeling and robust wireless communication systems in aviation. He is a PhD candidate at the University of Ulm.

Nils Mäurer M.Sc.

Nils Mäurer has been working as a cybersecurity researcher at the Institute of Communications and Navigation (KN) for the German Aerospace Center (DLR) since 2017. He is currently researching the cybersecurity design of LDACS, the datalink for future terrestrial aviation communications.

Dr. Thomas Gräupl

Thomas Gräupl received the Ph.D. degree in computer science from the University of Salzburg, Austria in 2011. He is a researcher with the institute of communications and navigation of the German Aerospace Center DLR.

Miguel A. Bellido-Manganell

Miguel A. Bellido-Manganell, in DLR since 2016, is contributing to the further development of LDACS and leading the LDACS Air-to-Air Mode design. His research interests include channel modelling, digital signal processing, spectrum compatibility, and medium access for aeronautical ad hoc networks.