PMAKE: Physical Unclonable Function-based Mutual Authentication Key Exchange Scheme for Digital Aeronautical Communications

Nils Mäurer and Thomas Gräupl
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{nils.maeurer, thomas.graeupl}@dlr.de

Corinna Schmitt and Gabi Dreo Rodosek
Research Institute CODE
Universität der Bundeswehr München
Neubiberg, Germany
{corinna.schmitt, dreo}@unibw.de

***Abstract*—Growth of civil air traffic and new entrants into the air transportation sector such as Unmanned Aeronautical Vehicles (UAV) pose a great challenge for air traffic management and its supporting Communication, Navigation and Surveillance (CNS) infrastructure. Analogue systems have to be replaced by digital systems to optimize spectrum efficiency, and automation needs to be introduced to support human decision making at scale. As safety and security are strongly intertwined in aviation, cybersecurity is one key enabler for digitalization in civil aviation. However, few deployed digital aeronautical communications systems incorporate dedicated cybersecurity measures. Link requirements of low latency, low bandwidth, and long range make aeronautical datalinks especially challenging in terms of security design. Further, challenging are the nature of wireless communication itself and the political boundaries in international air transportation concerning unique communication participant identification. Thus, this paper proposes a concept for a challenge-response (CR) based Physical Unclonable Function (PUF) Mutual Authentication Key Exchange scheme, short PMAKE, binding communication identity and radio device together. Initial evaluations show its suitability for the digital aeronautical communications system LDACS.**

***Index Terms*—Cybersecurity, Mutual Authentication and Key Exchange (MAKE), Physical Unclonable Function (PUF), L-band Digital Aeronautical Communications System (LDACS)**

I. Introduction

The ongoing digitization process nowadays has also spillovers in the civil aeronautical industry, especially affecting Communication, Navigation and Surveillance (CNS) infrastructure. The Single European Sky Air Traffic Management Research (SESAR)[1] program in the European Union (EU) and NextGEN[2] in the US have been tasked with the development of new technologies to create an aeronautical, digital Future Communications Infrastructure (FCI). Wireless technology candidates for the FCI are the Aeronautical Mobile Airport Communication System (AeroMACS) for airport communications, the satellite communications for oceanic, polar and remote domains, and the L-band Digital Aeronautical Communication System (LDACS) for long-range terrestrial aeronautical communications [30]. In this paper we focus on LDACS.

As safety and security are strongly interrelated in aviation, strong cybersecurity is the foundation and precondition for digitization in aviation [15], [33], [34]. However, cybersecurity for CNS is unfortunately not realized in most deployed systems [10], [28], [36]. One of the few systems in the ecosystem, which has a dedicated cybersecurity architecture is the FCI candidate for airport communications, AeroMACS. The system is majorly based on the IEEE 802.16 WiMAX standard [20], which has a security sub-layer integrated in its protocol stack. Central to the security of AeroMACS lies its Public Key Infrastructure (PKI) building a chain of trust originating from a root Certificate Authority (CA) [22]. This turned out to be problematic, since a root of trust has to be declared that all states worldwide, affected by civil aviation, can trust directly or via cross certification. Security infrastructure becomes therefore entangled with the political reality of aviation, which is, a small number of dominant state actors are capable of securing critical infrastructure and have limited trust towards others. For these others a PKI becomes a less attractive solution for an aeronautical trust framework. AeroMACS is therefore not widely deployed. Besides the mentioned situation with AeroMACS, we also have to consider the technical requirements for aeronautical datalinks representing the highest challenges for security support in aeronautic: (1) The low additional security latency and (2) the low additional security overhead. This is prompted by the long communication range (200NM) of terrestrial aeronautical communications and limited, dedicated spectrum for civil aviation communications. Further, political boundaries in international transportation concerning unique communication participant identification must be respected.

With these challenges in place, it is clear that traditional certificate-based authenticated key exchange schemes might be too expensive in terms of political issues, security overhead,

[1] https://www.sesarju.eu/, Oct. 14, 2020

[2] https://www.faa.gov/nextgen/, Oct. 14, 2020

978-3-903176-32-4 © 2021 IFIP

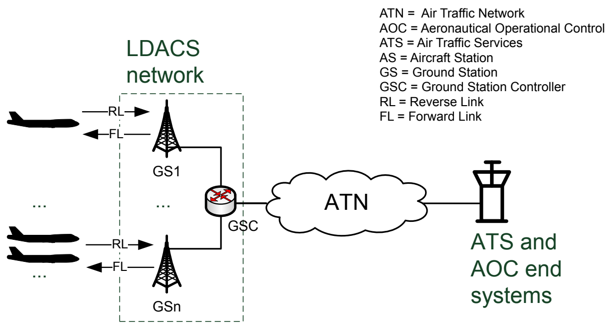


Fig. 1. Network architecture of LDACS [23]

and maintenance expense on digital aeronautical links [3]. Tackling the issue of certificates, trust, and low security data overhead, the Internet of Things (IoT) sector and solutions like Physical Unclonable Function (PUF)-based Challenge-Response (CR) authentication or Mutual Authentication and Key Exchange (MAKE) schemes [6], [8], [9], [19] come into focus. However, all these schemes only offer authentication, require a pre-stored, shared secret, prior to the setup phase of the protocols, or are simply impractical for the aeronautical communications requirements.

Thus, the objective of this paper is to investigate the combination of PUF, key exchange methods such as Diffie-Hellman Key Exchange (DHKE) and CR-based mutual authentication protocol for application in the aeronautical domain. The outcomes lead us to our proposed PUF-based Mutual Authentication Key Exchange scheme called PMAKE.

The paper is structured as follow: Section II presents insides to LDACS together with its frame structure, PUF theory, and DHKE theory. Security assumptions and detailed objectives are presented in Section III. PMAKE itself is discussed in detail in Section IV followed by the respective evaluation in Section V. Finally, the paper is concluded in Section VI.

II. Background and Related Work

Before diving into the solution we present here background information to make our taken design and implementation decisions (cf. Section IV) understandable and lay out important related work.

A. LDACS Theory

LDACS is a ground-based digital communications system for flight guidance and communications related to the safety and regularity of flight [30], [31]. It has been developed in Europe and is currently under standardization by ICAO [14], [16]. It covers current Air Traffic Services (ATS), Aeronautical Operational Control (AOC) data and also future applications, enables new concepts (e.g., sectorless Air Traffic Management (ATM)) and has at least an order of magnitude more net capacity than the currently used terrestrial links like the VHF Digital Link Mode 2 (VDLm2) system [14].

Fig. 1 depicts involved components and communication links. Up to 512 Aircraft Station (AS) communicate to an LDACS Ground Station (GS) in the Reverse Link (Reverse Link (RL)), GS communicate to AS in the Forward Link (Forward Link (FL)). GSs are controlled by a Ground Station Controller (GSC). The GSC connects the LDACS sub-network to the global Air Traffic Network (Air Traffic Network (ATN)) to which the corresponding Air Traffic Services (ATS) and Aeronautical Operational Control (AOC) end systems are attached. As we will need a detailed understanding of LDACS frame structure design in the evaluation Section V, we will briefly discuss this here.

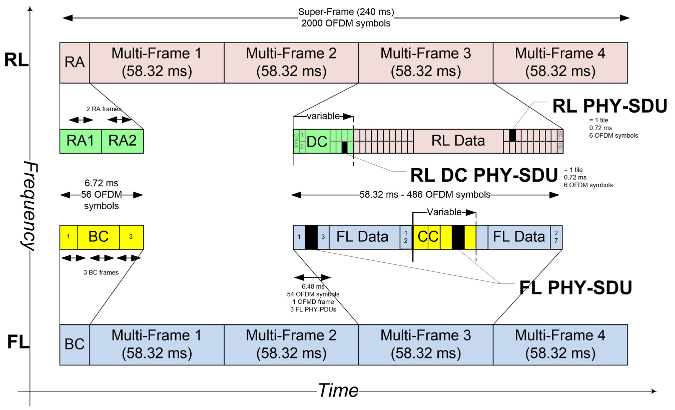


Fig. 2. Frame structure of LDACS [14]

In the FL direction, each Super Frame (SF) starts with a Broadcast (BC) slot, where the GS announces its existence to the AS and sends physical parameters for link establishment. The rest of the FL SF is split into four Multi Frames (MFs), each containing nine Orthogonal Frequency-Division Multiplexing (OFDM) frames and each frame comprises three FL Physical Layer Service Data Units (PHY-SDUs). Every FL PHY-SDU can be used to transmit FL user data or Common Control (CC) data, in which GS can allocate resources to an AS. In the RL, a SF starts with a Random Access (RA) slot, where AS can request access to an LDACS cell, and continues with four MFs. Each RL MF is constructed from 162 RL PHY-SDUs equivalent to Orthogonal Frequency-Division Multiple Access (OFDMA) tiles. They are used for two purposes, namely (1) to transmit Dedicated Control (DC) data, which are used by an AS to request the allocation for resources allowing them to send on the RL and (2) to transmit RL user data. Those details are depicted in Fig. 2.

In order to address the problem of low data rates of aeronautical systems, due to limited dedicated spectrum for civil aviation, we recommend

1) to reduce security message exchanges between GSC, GS and AS,
2) to eliminate the need of the integration of a PKI into the LDACS security framework, and
3) to uniquely bind identification and radio device, respectively the actual physical aircraft.

These three recommendations are followed by our proposed PMAKE scheme and is presented in Sections IV and V.

B. PUF's Theory

A silicon PUF is a mapping $f : \{0,1\}^n \rightarrow \{0,1\}^m$ with n challenge bits and m response bits. The response is derived when applying the n challenge bit onto the intractably complex instance-specific unique system behaviour [35]. PUFs use device unique random patterns, which are introduced in the manufacturing process to differentiate chips and make them uniquely identifiable. Hence, a PUF can be interpreted as a unique device's fingerprint, an enabler to create a unique set of CR pairs and a strong random number generator.

Thus the PUF can be combined with an arbitrary amount of arbitrary challenges to produce an arbitrary amount of device unique responses without the responses being available and accessible to an adversary when the chip is powered down. This capability will be used in the proposed PMAKE solution in Section IV.

C. DHKE's Theory

The original DHKE was first published in 1976 and is based on the discrete logarithm or Diffie-Hellman problem [11]. Due to the possibility of Man-in-the-Middle attacks [4], authenticated DHKE schemes (e.g., Station to Station (STS), Internet Key Exchange (IKE) and IKE version 2 (IKEv2) protocols [5] were invented.

Elliptic curve cryptography [21] enabled smaller key sizes, resulting in the the Elliptic Curve Diffie-Hellman (ECDH) protocol [2]. Based on the conjectured difficulty of finding isogenies between supersingular elliptic curves [29], Supersingular Isogeny Diffie–Hellman (SIDH) finally represents a post-quantum robust version of the DHKE [17], [18].

For our PMAKE scheme we will use the basic principle of any of the three previously mentioned DHKE (i.e., classic DHKE, ECDH, SIDH). We assume that each communicating party chooses a secret key and performs any DHKE type specific mathematical operation to derive a public key to be used in further message exchanges. This allows the Physical Unclonable Function based Mutual Authentication Key Exchange (PMAKE) scheme to use different DHKE types, depending on the situation.

D. Related Work

This work follows in line with several publications about LDACS and its cybersecurity design. First investigations were undertaken by conducting a threat- and risk analysis in [23], resulting in the draft of a cybersecurity architecture for LDACS in [26]. Several evaluations of that proposal followed [24], [25], until it became apparent that the MAKE procedure for LDACS will have to differ from MAKE procedures of other wireless communication links, such as Long Term Evolution (LTE) [1] or even AeroMACS [12], [22]. Before evaluating several MAKE procedures for LDACS, a suitable latency and data model was required, which was already published for LDACS in [13]. The first work on one possible MAKE procedure was published in [27], where an identity based variation of the STS protocol with different DHKE types was introduced and its suitability evaluated (based on [13]) for LDACS. As digitization goes onward and attackers become more inventive the defense strategies and protocols need to improve further. Thus, in this paper, we combine PUF and DHKE methods with each other into the PMAKE scheme, presented in Section IV and evaluate it based on the same evaluation methodology [13] as done in [27].

III. LDACS Security Model, Security Assumptions and Objectives

As mentioned in Section II, an LDACS network consists of one GSC controlling several GS and up to 512 AS connecting to one GS (c.f., Fig. 1). In order to communicate with each other, all entities within the LDACS network need to mutually authenticate with one another. This ascertains that only trusted participants can use the system. Thus to anchor trust within the system, multiple strategies are currently considered:

1) PKI: An International Civil Aviation Organization (ICAO)-hosted root CA can serve as trust bridge with regional sub-CAs distributed around the world or one root CA is placed per geographic region (i.e., per continent/country) with all distributed root CAs performing cross-certification with each other [32].
2) PUF based Challenge-Response-Pair (CRP): This is the strategy, we want to propose in this paper. Given a secure database on ground, attached to the GSC, where CRP are stored and a PUF installed in every aircraft during a secure manufacturing process, PMAKE can be used for mutual authentication and key exchange.

Overall, the MAKE procedure in LDACS is deeply linked to the cell entry procedure. Thus once an aircraft is registered in a cell and basic physical parameters for communication have been established, a MAKE procedure must be performed to authorize communication.

Our proposed PMAKE scheme was influenced by following four **security assumptions** from [5], which uphold for the main phase of PMAKE:

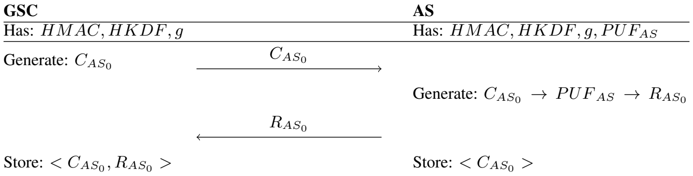
S1: The adversary is able to eavesdrop on all messages sent in a cryptographic protocol.

S2: The adversary is able to alter all messages sent in a cryptographic protocol using any information available.

S3: The adversary may be a legitimate protocol participant (an insider), or an external party (an outsider), or a combination of both.

S4: An adversary is able to obtain the value of the session key K_{AB} used in any sufficiently old previous run of the protocol.

Bilzhause et. al identified five objectives to secure LDACS [3]. These five objectives were later extended to nine objectives in the LDACS Standards and Recommended Practises (SARPS) endorsed by ICAO [16]. For the context of this work, the most important are (1) integrity, (2) authenticity for user and control plane messages in transit, provide (3) confidentiality for user plane messages in transit, provide



GSC
AS
Has: $HMAC, HKDF, g$
Has: $HMAC, HKDF, g, PUF_{AS}$
Generate: C_{AS_0}
C_{AS_0}
Generate: $C_{AS_0} \rightarrow PUF_{AS} \rightarrow R_{AS_0}$
R_{AS_0}
Store: $< C_{AS_0}, R_{AS_0} >$
Store: $< C_{AS_0} >$

Fig. 3. PMAKE's Setup Phase

(4) mutual entity authentication to (5) authorize explicitly permitted actions of users or entities.

Overall, to fulfill any of these objective, some key exchange and mutual authentication procedure must take place at the very beginning of connection establishment. The objective of the LDACS's PMAKE scheme is to establish a shared session key K between any two parties AS and GSC, in which they can have "mutual belief", following the definition of Boyd [5].

Summarizing this we define the following three **objectives O1-O3 for PMAKE**:

O1: *Mutual Authentication* means, both parties can be sure of each others identity and that both participated in this interaction.

O2: *Secure Key Agreement* assumes, both parties have established a shared session key that is fresh and can be use for a certain time between them only.

O3: *Perfect Forward Secrecy* means, the established session key remains secret, even when long term keys of the involved parties have been compromised after the session.

IV. The PMAKE Scheme

Assuming a verifier wants to authenticate i nodes using traditional PUF-based authentication protocols (e.g., A and B) he needs to store j numbers of k-bit long challenges and l-bit long corresponding responses, accumulating to a space complexity of $O((k+l) \times i \times j)$. Reducing this number, we loosely orient ourselves on the HMAC-based RFID PUF mutual authentication protocol (HPK), as it has already reduced space complexity to $O((k+l) \times i)$ [19]. This means, for every node only one CRP has to be maintained. With every protocol run a new CRP is securely exchanged, making the amount of protocol runs independent of the stored amount of CRPs.

A. Notations and Prerequisites

The notations for the following PMAKE scheme are listed in Table I following the notation by [5] for the key exchange part of the protocol.

Following previous works in designing MAKE protocols for LDACS [27], we aim to build a secure connection between GSC and AS, with the GS just being the intermediary, forwarding all messages over the air gap to the AS and via the ground based backbone back to the GSC. Every mobile node (aircraft) is equipped with a PUF during the construction process of the specific LDACS radio device. Communication partners AS and GSC will have to have previously agreed upon the chosen DHKE variation and respective public parameters.

TABLE I
Notations used in the PMAKE scheme

Notation	Definition
msg1 $\oplus$ msg2	XOR operation on msg1 with msg2
msg1 | msg2	Concatenation operation on msg1 with msg2
PUF$_A$	Physical Unclonable Function of entity A
HMAC$_K(msg)$	Hash-based Message Authentication Code with key K and input data msg
HKDF(K)	HMAC Key Derivation Function (HKDF) with input K
C_{A_i}	i-th Challenge for PUF from entity A
R_{A_i}	i-th Response from PUF from entity A
ID$_A$	Identifier of entity A
r_A	Random integers of entity A "Ephemeral private key"
t_A	Ephemeral public key of entity A
g	Public Diffie-Hellman parameters
$S_{AS,GSC}$	Static Diffie-Hellman key shared between AS and GSC
$K_{AS,GSC}$	Session key for AS-GSC communications
$\{msg\}_K$	Encrypted data msg with key K

Similar to previous works [26], [27], the ground based entities GSC and GS will have established a secure connection prior to a PMAKE scheme run. Note, it is essential for PMAKE's security that the setup phase where the initial generation of a CRP happens (cf. Section IV-B) will have to remain secure. Compromise of the first CRP renders the protocol insecure. Further, the public ephemeral keys of the DHKE requires to fulfill two purposes, namely (1) being key material, (2) serving as nonces. Thus for every run of the protocol r_A will have to be chosen anew.

B. The Setup Phase

PMAKE's **Setup Phase** starts in a secure environment, with an agreement between GSC and AS as illustrated in Fig. 3. The setup phase will have to be performed only once per aircraft. They need to have agreed upon a choice of a DHKE method and its public parameter g, HMAC, HKDF and on a suitable symmetric encryption algorithm. First, the GSC sends a challenge C_{AS_0} to the AS. Then the AS calculates a response making use of the SRAM PUF and the challenge C_{AS_0} producing R_{AS_0}. The response is send back to the GSC. As last step in this phase, the GSC securely stores $< C_{AS_0}, R_{AS_0} >$ and the AS stores $< C_{AS_0} >$.

C. The Main Phase

After a successful very first exchange of CRPs in a secure environment PMAKE continues with its **Main Phase**. Fig. 4 illustrates required steps and message exchanges that are:

1) After GSC and GS have established a secure connection, the GS starts broadcasting its identity ID$_{GS}$ regularly.
2) The AS, upon receiving such a beacon, generates a random number r_{AS} and. depending on the respectively chosen DHKE procedure. calculates t_{AS} and $\alpha = HMAC_{R_{AS_0}}(\text{ID}_{AS}, \text{ID}_{GS}, t_{AS})$. It then responds with $|t_{AS} \oplus C_{AS_0}|\alpha|\text{ID}_{AS}|$.

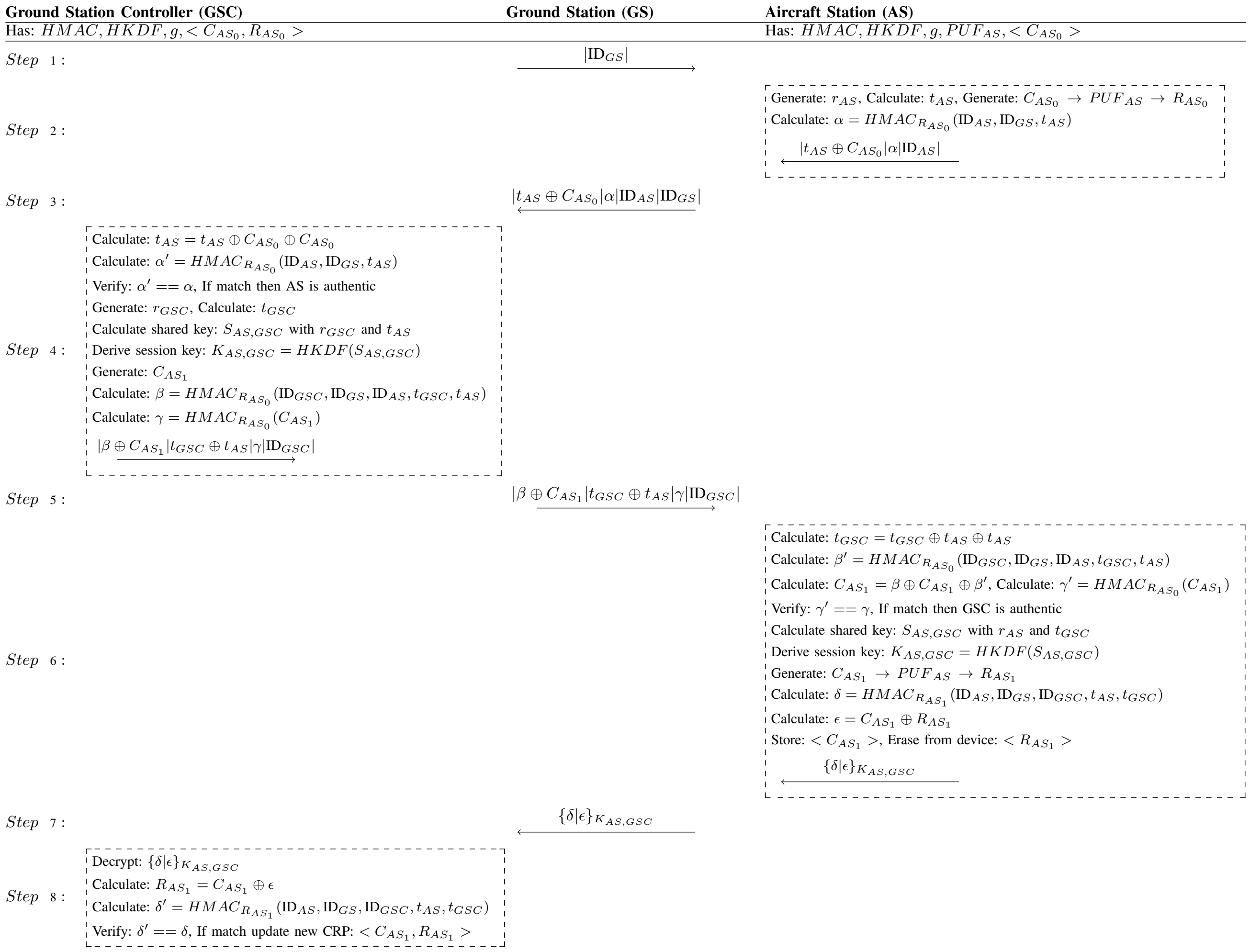

Ground Station Controller (GSC)
Ground Station (GS)
Aircraft Station (AS)
Has: $HMAC, HKDF, g, < C_{AS_0}, R_{AS_0} >$
Has: $HMAC, HKDF, g, PUF_{AS}, < C_{AS_0} >$
Step 1 :
$|\mathrm{ID}_{GS}|$
Step 2 :
Generate: r_{AS}, Calculate: t_{AS}, Generate: $C_{AS_0} \rightarrow PUF_{AS} \rightarrow R_{AS_0}$
Calculate: $\alpha = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$
$|t_{AS} \oplus C_{AS_0}|\alpha|\mathrm{ID}_{AS}|$
Step 3 :
$|t_{AS} \oplus C_{AS_0}|\alpha|\mathrm{ID}_{AS}|\mathrm{ID}_{GS}|$
Step 4 :
Calculate: $t_{AS} = t_{AS} \oplus C_{AS_0} \oplus C_{AS_0}$
Calculate: $\alpha' = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$
Verify: $\alpha' == \alpha$, If match then AS is authentic
Generate: r_{GSC}, Calculate: t_{GSC}
Calculate shared key: $S_{AS,GSC}$ with r_{GSC} and t_{AS}
Derive session key: $K_{AS,GSC} = HKDF(S_{AS,GSC})$
Generate: C_{AS_1}
Calculate: $\beta = HMAC_{R_{AS_0}}(\mathrm{ID}_{GSC}, \mathrm{ID}_{GS}, \mathrm{ID}_{AS}, t_{GSC}, t_{AS})$
Calculate: $\gamma = HMAC_{R_{AS_0}}(C_{AS_1})$
$|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|\mathrm{ID}_{GSC}|$
Step 5 :
$|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|\mathrm{ID}_{GSC}|$
Step 6 :
Calculate: $t_{GSC} = t_{GSC} \oplus t_{AS} \oplus t_{AS}$
Calculate: $\beta' = HMAC_{R_{AS_0}}(\mathrm{ID}_{GSC}, \mathrm{ID}_{GS}, \mathrm{ID}_{AS}, t_{GSC}, t_{AS})$
Calculate: $C_{AS_1} = \beta \oplus C_{AS_1} \oplus \beta'$, Calculate: $\gamma' = HMAC_{R_{AS_0}}(C_{AS_1})$
Verify: $\gamma' == \gamma$, If match then GSC is authentic
Calculate shared key: $S_{AS,GSC}$ with r_{AS} and t_{GSC}
Derive session key: $K_{AS,GSC} = HKDF(S_{AS,GSC})$
Generate: $C_{AS_1} \rightarrow PUF_{AS} \rightarrow R_{AS_1}$
Calculate: $\delta = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$
Calculate: $\epsilon = C_{AS_1} \oplus R_{AS_1}$
Store: $< C_{AS_1} >$, Erase from device: $< R_{AS_1} >$
$\{\delta|\epsilon\}_{K_{AS,GSC}}$
Step 7 :
$\{\delta|\epsilon\}_{K_{AS,GSC}}$
Step 8 :
Decrypt: $\{\delta|\epsilon\}_{K_{AS,GSC}}$
Calculate: $R_{AS_1} = C_{AS_1} \oplus \epsilon$
Calculate: $\delta' = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$
Verify: $\delta' == \delta$, If match update new CRP: $< C_{AS_1}, R_{AS_1} >$

Fig. 4. PMAKE's Main Phase

3) Once the GS receives the response to the beacon message, it appends its ID to the message and forwards $|t_{AS} \oplus C_{AS_0}|\alpha|\mathrm{ID}_{AS}|\mathrm{ID}_{GS}|$ to the GSC.
4) With the help of the previously stored tuple $< C_{AS_0}, R_{AS_0} >$, the GSC can compute the public key of the AS $t_{AS} = t_{AS} \oplus C_{AS_0} \oplus C_{AS_0}$ and $\alpha' = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$. It then checks whether $\alpha' == \alpha$ match. If that is the case, the AS has authenticated to the GSC. Then the GSC generates a random number r_{GSC} of its own and again in dependence on the previously agreed DHKE procedure, calculates t_{GSC}. Now the shared AS-GSC key $S_{AS,GSC}$ can be calculated via the secret of the GSC r_{GSC} and the public key of the AS t_{AS}. With that, the GSC calculates the session key $K_{AS,GSC}$ via the HKDF and $S_{AS,GSC}$. Finally a new challenge C_{AS_1} is chosen by the GSC and two new MAC tags are calculated. β is used to conceal C_{AS_1}, while γ serves as authenticity proof about the GSC for the AS. It finally sends $|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|\mathrm{ID}_{GSC}|$ to the GS.
5) The GS forwards that message to the AS.
6) First the AS calculates the public key of the GSC via $t_{GSC} = t_{GSC} \oplus t_{AS} \oplus t_{AS}$. To be able to decipher C_{AS_1}, β' is calculated by the AS by reconstructing R_{AS_0} and using previously established values t_{GSC}, t_{AS}, ID_{GSC}, ID_{GS}, ID_{AS}. As $C_{AS_1} = \beta \oplus C_{AS_1} \oplus \beta'$ the AS successfully received the new challenge C_{AS_1}. It then calculates its own value for $\gamma' = HMAC_{R_{AS_0}}(C_{AS_1})$ and compares $\gamma' = \gamma$. If they match, the GSC has authenticated to the AS. Furthermore the verifiable integrity and return of t_{AS} proves to the AS, that the GSC actually participated in the protocol. Now the AS calculates the shared key $S_{AS,GSC}$ with r_{AS} and t_{GSC} and derives the session key $K_{AS,GSC} = HKDF(S_{AS,GSC})$. Via the AS PUF a new response R_{AS_1} is generated to the new challenge C_{AS_1} via $C_{AS_1} \rightarrow PUF_{AS} \rightarrow R_{AS_1}$. It then calculates $\delta = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$ that will be used by the GSC as proof for the authenticity and correctness of the new response R_{AS_1}. $\epsilon = C_{AS_1} \oplus R_{AS_1}$ is used to conceal the response R_{AS_1} during transport. At this point,

the AS securely stores C_{AS_1} and erases R_{AS_1} from memory. As AS and GSC have previously agreed upon suitable encryption algorithms, the AS sends δ and ϵ encrypted with $K_{AS,GSC}$ back to the GSC.

7) The GS forwards that message to the GSC.
8) The GSC decrypts the message with the agreed upon encryption algorithm and key $K_{AS,GSC}$. It then computes $R_{AS_1} = C_{AS_1} \oplus \epsilon$. It then calculates $\delta' = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$ and checks whether $\delta' == \delta$. If that is the case, the GSC can be sure of the authenticity of the response R_{AS_1} and the participation of AS in the protocol. It updates the current tuple for that AS to $< C_{AS_1}, R_{AS_1} >$.

Assuming everything went fine, secure user data communication between AS and GSC can now commence with the session key $K_{AS,GSC}$. After a successful encrypted user data message exchange between AS and GSC, also key confirmation is achieved.

V. Evaluation of PMAKE

In this section we will evaluate our proposed PMAKE scheme. First we evalute its security and then its suitability for LDACS using the latency emulation model from [13], [27]. Thus, we evaluate used message sizes and introduced data/latency overhead due to the new security implementation.

A. Security Evaluation of PMAKE

Throughout the protocol, an eavesdropper can tap on all messages exchanged on the air-gap between GS and AS. GSC and GS have established a secure connection prior any aircraft being able to join an LDACS cell. Throughout the protocol, an attacker can eavesdrop on *step 1*: ID_{GS}, *step 2:*: $t_{AS} \oplus C_{AS_0}$, $\alpha = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$, ID_{AS}, *step 4:* $HMAC_{R_{AS_0}}(\mathrm{ID}_{GSC}, \mathrm{ID}_{GS}, \mathrm{ID}_{AS}, t_{GSC}, t_{AS}) \oplus C_{AS_1}$ (c.f., the first $HMAC$ operation was denoted with β in Fig. 4), $t_{GSC} \oplus t_{AS}$, $\gamma = HMAC_{R_{AS_0}}(C_{AS_1})$, ID_{GSC} and *step 6:* $\{\delta = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC}) | \epsilon = C_{AS_1} \oplus R_{AS_1}\}_{K_{AS,GSC}}$. The attacker can try to use this information to obtain the public keys and nonces t_{AS}, t_{GSC} and the challenge and response pairs C_{AS_i}, R_{AS_i}. All these values protected via respective $\oplus$ operations or $HMAC$ and can thus not be eavesdropped.

If an attacker successfully blocks communication during PMAKE, the secure database within the GSC simply does not update to new CRP values and the MAKE attempt between AS and GSC fails. However, it can simply be resumed at a later point in time.

Every PMAKE attempt is based on new nonces t_{AS}, t_{GSC}. Therefore PMAKE is secure against replay attacks.

If an attacker tries to impersonate an AS after step 1, he does not have access to either C_{AS_i} or R_{AS_i}, thus the GSC would note the spoofer when validating α. If an attacker tries to impersonate an AS after step 4, he could not obtain the correct session key $K_{AS,GSC}$ and thus the GSC would notice after step 7. If an attacker impersonates a GS, communication to the backbone via the GSC cannot take place and after step 5, the AS would recognize the imposter due to wrong values for β, γ and $t_{GSC} \oplus t_{AS}$. If an attacker tries to impersonate GSC during communication and assuming that communication via a GS would somehow be possible, the AS would still notice after step 5, due to wrong β, γ and $t_{GSC} \oplus t_{AS}$ values. Thus PMAKE can be regarded as hardened against spoofing attacks, as all communication partner can detect spoofing attempts during the protocol.

PMAKE makes use of PUF installed within the LDACS radio device. Due to the nature of PUFs, cloning is impossible.

B. Evaluation on Data and Latency Overhead

a) Latency Model: As discussed in Section II-D, we use the latency emulation model for LDACS, presented in [13] with all newer updates from [27]. Taking retransmissions into account, FL latency can be calculated as

$$L_{FL}(t) = m_{FL}(t) + (1 + \delta_{RX}(1 + n)) \times d_{MF} \quad (1)$$

and RL latency as

$$L_{RL}(t) = m_{RL}(t) + (2 + \delta_{RX}(N + 3)) \times d_{MF}. \quad (2)$$

Here we explain the notation used in the equations, based on the LDACS frame details presented in Section II-A.

In Equation 1, we use $m_{FL}(t)$ to classify the time until the start of the next CC frame, $\delta_{RX} \in \{0, 1\}$ to indicate a retransmission, d_{MF} to denote the length of a MF and n is derived from the length of the reverse link medium access cycle from forward link perspective.

In Equation 2, we use $m_{RL}(t)$ to denote the time until the start of next DC slot, $\delta_{RX} \in \{0, 1\}$ to indicate a retransmission, d_{MF} to denote the length of a MF and N is derived from the length of the reverse link medium access cycle from reverse link perspective.

We model $\delta_{RX} \in \{0, 1\}$ as stochastic process, based on the packet error rate. Given a Bit Error Rate (BER), we can calculate the packet error rate based on the length of a packet l: $P(\{\text{no error in packet}\}) = (1 - BER)^l$. Thus the opposite event, that a packet indeed contains an error is: $P(\{\text{error in packet}\}) = 1 - ((1 - BER)^l)$. These two probability decide the value of δ_{RX}, whether a retransmission is necessary and, thus, an error appeared in the packet, or not. For more details on this model we refer to [13] and [27]. In Table II we list the used parameters for LDACS's MAC protocol, necessary for PMAKE's evaluation.

b) Message Sizes: Every LDACS message has a 48bit header at the beginning of a user data message. Sizes of t_{AS}, t_{GSC} vary, depending on the choice of DHKE procedure and keys lengths are chosen similar to [27] leading to: $t_{GSC} : \{DHKE = 3072 | ECDH = 256 | SIDH = 2624\}$ and $t_{AS} : \{DHKE = 3072 | ECDH = 256 | SIDH = 2640\}$.

As recommended in [7], we decided for a 128bit length for the the Message Authentication Code (MAC) tags. A MAC is derived from any operation in PMAKE that involves the HMAC function(e.g., α, β, γ, δ and ϵ are all MAC tags).

All communication entity identities $\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}$ are 28 bit long.

TABLE II
PARAMETER VALUES FOR LATENCY TIMING FOR THE LDACS MEDIUM ACCESS LAYER (MAC) PROTOCOL

Forward Link Model $L_{FL}(t)=m_{FL}(t)+$ $(1+\delta_{RX}(1+n))\times d_{MF}$		**Reverse Link Model** $L_{RL}(t)=m_{RL}(t)+$ $(2+\delta_{RX}(N+3))\times d_{MF}$	
Para-meters	**Values**	**Para-meters**	**Values**
d_{MF}	60ms	d_{MF}	60ms
$m_{FL}(t)$	Time until start of next FL MF: Every 1 to 60ms modelled by $U(1,60)$	$m_{RL}(t)$	Average time until start of next MAC cycle: $\#\text{AS}/32\times d_{MF}$ $+wait$ $wait$ modelled by $U(1,60)$
n	Average amount of MF after transmission until next DC slot is scheduled for AS in MAC-cycle: $n=\#\text{AS}/32$	N	Average amount of MF after transmission until next DC slot scheduled for AS in MAC-cycle: $N=(\#AS/32-3)$ $\mod\ \#AS/32$
BER	$0,10^{-6},10^{-5}$		
P	$P(\{\text{no error in packet}\})=(1-BER)^{l}$ $P(\{\text{error in packet}\})=1-((1-BER)^{l})$		

c) Data Overhead: Now we assign the aforementioned message sizes to every PMAKE message. Please note, that the message in *step 1* is part of LDACS control plane, thus we start our evaluation in *step 2*.

Message in step 2: it consists of a $header=48$, $t_{AS}=\{DHKE=3072, ECDH=256, SIDH=2640\}$ xored with the challenge C_{AS_0} (resulting in the same bit lengths as t_{AS}), a MAC tag $\alpha=128$ and the aircraft ID $\text{ID}_{AS}=28$, totalling in $\{3276,460,2844\}$bits.

Message in step 4: it consists of a $header=48$, a MAC tag xored with the new challenge $\beta\oplus C_{AS_1}=128$, both t_{GSC} and t_{AS} xored together resulting in $\{DHKE=3072, ECDH=256, SIDH=2624\}$, another MAC tag $\gamma=128$ and the GSC ID $\text{ID}_{GSC}=28$, totalling in $\{3404,588,2956\}$bits.

Message in step 6: it consists of a $header=48$ and two MAC tags $\delta=128$ and $\epsilon=128$ totalling in 304bits.
We show all PMAKE message sizes in Table III.

TABLE III
MESSAGE SIZES FOR PMAKE IN *bit*

Message	**PMAKE-DHKE**	**PMAKE-ECDH**	**PMAKE-SIDH**
Step 2	3276	460	2844
Step 4	3404	588	2956
Step 6	304	304	304
Total	6984	1352	6104

d) Latency Overhead: Now we calculate LDACS latencies for the PMAKE procedure, based on aforementioned LDACS latency model and depending on the BER on the link and the amount of AS in an LDACS cell. We will use the three BER levels mentioned in Table II, namely 0 BER for getting a baseline authentication latency, BER of 10^{-6}, which is the working point of LDACS, and a BER of 10^{-5} for a worst case BER.

Authentication Latency Baseline: With $BER=0$, the different sizes of the DHKE variations have no impact on the latency times as no retransmission due to lost packets is necessary. In Fig. 5 we see that minimum PMAKE authentication latency values range from 300ms with few AS in a cell, to 2200ms when the LDACS cell is full. For maximum values, we see ranges from 480ms for few aircraft to 2400ms for a full LDACS cell.

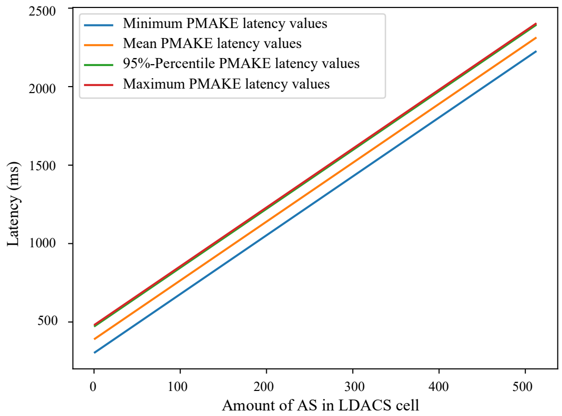


Fig. 5. Baseline authentication latency of PMAKE depending of the amount of AS in an LDACS cell at BER= 0.

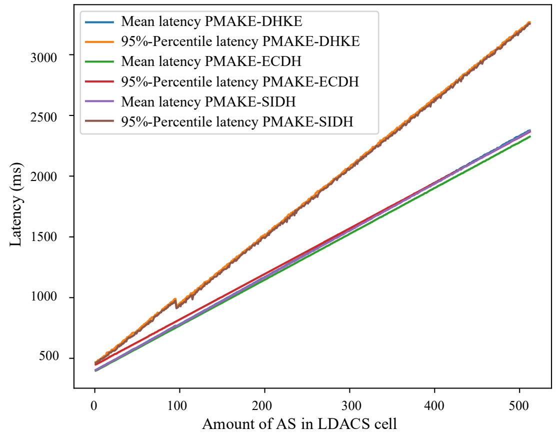


Fig. 6. Authentication latency of the PMAKE scheme depending of the amount of AS in an LDACS cell and DHKE at BER=10^{-5}. Note that the small peaks in the result for less than 3×32 AS are caused by the DC slot falling into an unfavorable position for retransmissions as calculated by N in Table II.

Authentication Latency with realistic BER: For the evaluation under realistic BER, we emulated 10,000 authentication attempts per AS in the LDACS cell to get a realistic view on the authentication latency times, following the same argumentation as in [27]. At a BER of 10^{-6}, retransmissions and thus the choice of DHKE flavor does not play a large role for the authentication latency. Thus independent of the choice of DHKE procedure, mean PMAKE authentication latency ranges from 420ms for 1 AS in a cell to 2300ms for 512 AS in a cell. The 95%-percentiles range from 480ms to 2360ms.

At a BER of 10^{-5}, retransmissions and thus the choice of DHKE flavor do play a large role. Fig. 6 reveals, that the bigger key sizes of DHKE and SIDH trigger more reliably retransmissions in the 95%-percentile cases and thus PMAKE-ECDH turns out to be about 1000ms faster in the worst case with a full LDACS cell. Apart from that, we see that on average all procedures take again between 480ms to 2400ms.

C. Evaluation Findings

Overall PMAKE allows for mutual authentication and key exchange capabilities between ground and aircraft without the use of a PKI or digital certificates. The only prerequisite is that a CRP is exchanged previously to the main phase of the protocol and kept secret, until the next CRP is used in which case the previous pair can even be disclosed as no relevant information can be derived. Furthermore, via the use of a PUF, the physical entity of the aircraft and respectively the LDACS radio can be tied to the respective aircraft identity.

Now we want to put the results of the latency and data overhead evaluation into perspective. In [26], [27], a STS based MAKE scheme for LDACS was introduced and evaluated.

Comparing data overhead values from PMAKE to the scheme of [27], we see that PMAKE requires 6% (DHKE), 23% (ECDH), 6% (SIDH) less data for the entire MAKE procedure.

In terms of latency duration, PMAKE takes roughly the same amount of time, when few aircraft are in an LDACS cell. However, as the number of AS in a cell goes up, PMAKE can take up 800ms longer. The reason for that is, PMAKE uses one FL messages and two RL messages, while the proposed STS scheme in [27] takes two FL messages and one RL message and FL latency is usually smaller than RL latency. Here the benefit of PMAKE is, an unauthorized AS can be ruled out quicker, as the first message in the PMAKE scheme comes from the AS.

VI. Conclusions

In this paper the applicability of PUF, CR and DHKE based AKE protocols was investigated. The goal was to derive a new security paradigm for securing digital aeronautical communications systems while taking LDACS's architecture and communication flows as example application.

It turned out that modifications of the HPK mutual authentication scheme can improve the existing cybersecurity architecture of LDACS. The scheme was extended with a key exchange addition, leading to the proposed PMAKE scheme offering a PUF-based mutual authentication key exchange. As the CRPs are central to the security of the protocol, the currently used CRP must not be disclosed to any unauthorized party, as otherwise the security of the protocol is compromised. Based on LDACS's architecture and communication flows, we evaluated the PMAKE scheme in terms of data and latency overhead compared to previously proposed MAKE procedures for LDACS. The results show that PMAKE requires less data but can take more authentication latency times then previous schemes.

For future research, we are going to model the proposed PMAKE scheme in the symbolic model checker Tamarin and proof its security properties. Another open question is how to make the CRPs securely available for a certain GSC at the time when an AS, matching those pairs, enters the LDACS cell served by that GSC. This will also be part of future work.

Appendix

AeroMACS	Aeronautical Mobile Airport Communication System
AOC	Aeronautical Operational Control
AS	Aircraft Station
ATN	Air Traffic Network
ATM	Air Traffic Management
ATS	Air Traffic Services
BC	Broadcast
BER	Bit Error Rate
CA	Certificate Authority
CC	Common Control
CNS	Communication, Navigation and Surveillance
CR	Challenge-Response
CRP	Challenge-Response-Pair
DC	Dedicated Control
DHKE	Diffie-Hellman Key Exchange
ECDH	Elliptic Curve Diffie-Hellman
FCI	Future Communications Infrastructure
FL	Forward Link
GS	Ground Station
GSC	Ground Station Controller
HKDF	HMAC Key Derivation Function
HPK	HMAC-based RFID PUF mutual authentication protocol
ICAO	International Civil Aviation Organization
IKE	Internet Key Exchange
IoT	Internet of Things
LDACS	L-band Digital Aeronautical Communication System
MAC	Medium Access Layer
MAKE	Mutual Authentication and Key Exchange
MF	Multi Frame
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PHY-SDU	Physical Layer Service Data Unit
PKI	Public Key Infrastructure
PMAKE	Physical Unclonable Function based Mutual Authentication Key Exchange
PUF	Physical Unclonable Function
RA	Random Access
RL	Reverse Link
SARPS	Standards and Recommended Practises
SESAR	Single European Sky Air Traffic Management Research
SF	Super Frame
SIDH	Supersingular Isogeny Diffie–Hellman
STS	Station to Station
VDLm2	VHF Digital Link Mode 2

References

[1] 3GPP, "3GPP System Architecture Evolution (SAE); Security architecture," 3rd Generation Partnership Project (3GPP), Tech. Rep., 07 2020, [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33401.htm.

[2] G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger, *A Course in Mathematical Cryptography*. Berlin, Germany: Walter de Gruyter GmbH & Co KG, 2015.

[3] A. Bilzhause, B. Belgacem, M. Mostafa, and T. Gräupl, "Datalink Security in the L-band Digital Aeronautical Communications System (LDACS) for Air Traffic Management," *Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 22–33, Nov. 2017.

[4] S. Blake-Wilson and A. Menezes, "Authenticated Diffe-Hellman Key Agreement Protocols," in *International Workshop on Selected Areas in Cryptography*. Heidelberg, Germany: Springer, Aug. 1998, pp. 339–361.

[5] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for Authentication and Key Establishment*. Heidelberg, Germany: Springer, 2020.

[6] A. Braeken, "PUF Based Authentication Protocol for IoT," *Symmetry*, vol. 10, no. 8, pp. 1–15, Aug. 2018.

[7] BSI, "Cryptographic Mechanisms: Recommendations and Key Lengths," Federal Office for Information Security Germany, Tech. Rep. BSI TR-02102-1, Mar. 2020.

[8] J. Byun, "End-to-End Authenticated Key Exchange Based on Different Physical Unclonable Functions," *IEEE Access*, vol. 7, pp. 102 951–102 965, Jul. 2019.

[9] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. Chakraborty, D. Mahata, and M. Prabhu, "Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424–437, May 2018.

[10] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On Insecurity of ADS-B protocol and Practical Attacks onADS-B Devices," *Black Hat USA*, pp. 1–10, Aug. 2012.

[11] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[12] N. Giraudon, M. Iannes, S. Tamalet, M. Lehmann, S. Ben Mahmoud, N. Larrieu, A. Correas, and S. Fasetta, "Part 1 - AeroMACS Safety and Security Analysis, Part 2 - AeroMACS Security Analysis," Montreal, Canada, Dec. 2014 (accessed Sept. 19, 2020). [Online]. Available: https://www.icao.int/safety/acp/ACPWGF/ACP-WG-S-5/IP09%20-%20SESAR%20AeroMACS%20Safety%20and%20Security%20Analysis.pdf

[13] T. Gräupl and M. Mayr, "Method to Emulate the L-band Digital Aeronautical Communication System for SESAR Evaluation and Verification," in *34th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Oct. 2015, pp. 1–18.

[14] T. Gräupl, C. Rihacek, and B. Haindl, "LDACS A/G Specification," German Aerospace Center (DLR), Oberpfaffenhofen, Germany, SESAR2020 PJ14-02-01 D3.3.030, 2019.

[15] A. Hall, J. Wingfield, G. De Moura, and K. Tiscareno, "Advancing Cyber Resilience in Aviation: An Industry Analysis," World Economic Forum, Davos, Switzerland, Tech. Rep., January 2020.

[16] International Civil Aviation Organization (ICAO), "Finalization of LDACS Draft SARPs - Working Paper WP05 including Appendix," ICAO, Montreal, Canada, Tech. Rep., Oct. 2018.

[17] D. Jao, "Supersingular Isogeny Key Encapsulation," Apr. 2020 (accessed Sept. 19, 2020). [Online]. Available: https://sike.org/files/SIDH-spec.pdf

[18] D. Jao and L. De Feo, "Towards Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies," in *International Workshop on Post-Quantum Cryptography*. Heidelberg, Germany: Springer, Nov./Dec. 2011, pp. 19–34.

[19] S. Jung and S. Jung, "HRP: A HMAC-Based RFID Mutual Authentication Protocol Using PUF," in *International Conference on Information Networking*. New York, NY, USA: IEEE, Jan. 2013, pp. 578–582.

[20] B. Kamali, *AeroMACS: An IEEE 802.16 Standard-based Technology for the Next Generation of Air Transportation Systems*. Hoboken, NJ, USA: John Wiley & Sons, 2018.

[21] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[22] O. Marcia, "AeroMACS PKI," in *Integrated Communications, Navigation, Surveillance Conference*. New York, NY, USA: IEEE, Apr. 2018, pp. 1–15.

[23] N. Mäurer and A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis," in *18th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, Apr. 2018, pp. 1A2/1–1A2–11.

[24] N. Mäurer, T. Gräupl, and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation," in *38th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Sept. 2019, pp. 1–10.

[25] 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)*. New York, NY, USA: IEEE, Apr. 2019, pp. 1A2/1–1A2–13.

[26] Mäurer, N. and Bilzhause, A., "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)," in *37th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Sept. 2018, pp. 1–10.

[27] Mäurer, N., Gräupl, T. and Schmitt, C., "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," in *39th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Oct. 2020, pp. 1–10.

[28] M. Niraula, J. Graefe, R. Dlouhy, M. Layton, and M. Stevenson, "ATN/IPS Security Approach: Two-way Mutual Authentication, Data Integrity and Privacy," in *Integrated Communications, Navigation, Surveillance Conference*. New York, NY, USA: IEEE, Apr. 2018, pp. 1–17.

[29] A. Rostovtsev and A. Stolbunov, "Public-Key Cryptosystem Based on Isogenies," *IACR Cryptology ePrint Archive*, pp. 1–19, May 2006.

[30] M. Schnell, "Update on LDACS - The FCI Terrestrial Data Link," in *19th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, Apr. 2019, pp. 1–10.

[31] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "LDACS: Future Aeronautical Communications for Air-Traffic Management," *Communication Magazine*, vol. 52, no. 5, pp. 104–110, May 2014.

[32] R. Segers, "Cybersecurity for global Aviation - A Trust Framework enabling global secure aviation interoperability," in *ICNS Conference 2018 Plenary Panel I, 18th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, April 2018.

[33] M. Slim, B. Mahmoud, A. Pirovano, and N. Larrieu, "Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey," *Computer Science Review*, vol. 11-12, pp. 1–29, May 2014.

[34] M. Strohmeier, A. Niedbala, M. Schäfer, V. Lenders, and I. Martinovic, "Surveying Aviation Professionals on the Security of the Air Traffic Control System," in *Security and Safety Interplay of Intelligent Software Systems*. Heidelberg, Germany: Springer, Mar. 2018, pp. 135–152.

[35] G. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *44th ACM/IEEE Design Automation Conference*. New York, NY, USA: IEEE, Jun. 2007, pp. 9–14.

[36] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A Practical and Compatible Cryptographic Solution to ADS-B Security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3322–3334, Nov. 2018.