Post-Quantum Ready Key Agreement for Aviation

Marcel Tiepelt\textsuperscript{1}, Christian Martin\textsuperscript{1} and Nils Maeurer\textsuperscript{2}

\textsuperscript{1} Karlsruhe Institute of Technology, KASTEL, Karlsruhe, Germany
\textsuperscript{2} Airbus, Airbus Defence and Space, Taufkirchen, Germany

\textbf{Abstract.} Transitioning from classically to quantum secure key agreement protocols may require to exchange fundamental components, for example, exchanging Diffie-Hellman-like key exchange with a key encapsulation mechanism (KEM). Accordingly, the corresponding security proof can no longer rely on the Diffie-Hellman assumption, thus invalidating some security guarantees. As a consequence, the security properties have to be re-proven under a corresponding security notion.

We initiate the study of the LDACS key agreement protocol (Edition 01.01.00 from 25.04.2023), which is soon-to-be-standardized by the International Civil Aviation Organization. The protocol’s cipher suite features Diffie-Hellman as well as a KEM-based key agreement protocol to provide post-quantum security. While the former results in an instantiation of an ISO key agreement inheriting all security properties, the security achieved by the latter is ambiguous.

We formalize the computational security using the systematic notions of de Saint Guilhem, Fischlin and Warinshi (CSF ’20), and prove the exact security that the KEM-based variant achieves in this model; primarily entity authentication, key secrecy and key authentication. To further strengthen our “pen-and-paper” findings, we model the protocol and its security guarantees using Tamarin, providing an automated proof of the security against a Dolev-Yao attacker.

\textbf{Keywords:} authenticated key exchange \cdot post-quantum key exchange \cdot formal verification \cdot LDACS

\section{Introduction}

\textbf{Post-Quantum Cryptography} The progress in quantum technology makes a potential threat of large scale universal quantum computers to cryptography undeniable. To enable secure communication in the future, quantum secure alternatives to Diffie-Hellman-like key exchanges, that do not rely on the hardness of the discrete logarithm problem, have been proposed. The most prominent of such alternatives are the post-quantum schemes that are currently undergoing standardization as part of the National Institute for Standards and Technology (NIST) post-quantum competition [fST22]. These schemes are based on key encapsulation mechanisms (KEMs), meaning that they cannot readily be combined with existing protocols that build on a Diffie-Hellman-like key exchange structure, thus invalidating security guarantees. On the other side, any protocol that achieves security based on a generic notion for key encapsulation mechanisms could be instantiated with any of the NIST post-quantum schemes, providing a quantum-secure protocol.

\textbf{Authenticated Key Exchange} Authenticated key exchange enables two or more parties to secretly agree on a key, additionally assuring the parties that they are interacting with...
their intended peer. Common frameworks to prove the security of key agreement protocols are BR- [BFWW11] or SK-security [CK02], with adversaries that have the capabilities to send or modify any messages during protocol execution. Additionally, adversaries may either learn the initial state of a party (weak corruption), or even learn intermediate states during execution of the protocol (strong corruption). We review common protocols and their security that relate to this manuscript. A broader overview can be found in [BMS20].

The Station to Station (STS) protocol [WVOW92] combines a Diffie-Hellman (DH) key exchange with a public-key infrastructure signature scheme. At first, the initiator sends a public DH value to a responder, who generates their own DH values, computes the secret key, and responds with their own DH value and a signature on both values. The responder encrypts their return message with the shared key. In the last pass, the initiator sends their own signature on the DH public values encrypted under the shared key. A variant of the STS protocol removes the encryption of the signatures and either adds a message authentication code (MAC) on the public DH values, or includes the identity of the intended partner into the signature. This construction allows to achieve security against weak corruption.

The ISO/ IEC 11770-3 protocols, specifically ISO KAM-7 [co21, §11.7] pick up at this latter construction, but add an identifier for the intended partner to the signature and an additional message authentication code to the message flow, lifting the protocol to provide security against strong corruption.

Finally, the Internet Key Exchange (IKEv2) [KHN+14a], which is implemented in IPsec and virtually all IP-based secure communications (e.g. VPNs), follows the SIGn-and-MAc (SIGMA) approach [Kra03]. The SIGMA approach combines the public-key-infrastructure-based signature, the message authentication code and the encryption of the two using the shared key, and was proven secure against strong corruption.

The above protocols have been, originally, proven secure under the Decisional Diffie-Hellman assumption [CK02, Cre11], thus are based on only classically secure components. A first formal analysis of IKEv2 assuming a post-quantum secure variant of DH was conducted by [GGCG+21], in which case the original proof would carry over, except under the post-quantum DH assumption. An alternative approach was taken by [FKMS20], who show that IKEv2 is “post-quantum secure” if pre-shared keys are used to negotiate new key material. Further, [BBF+19] provide a detailed analysis of hybrid combiners using DH values and KEMs, along with a fine-grained analysis of adversarial power. They provide a multi-stage BR security proof for an independent authenticated key exchange based on key encapsulation mechanism from a SIGMA approach. Further, [Pei14] sketched the proof of a variant of SIGMA, which exchanged the Diffie-Hellman key exchange for a key encapsulation mechanism.

**Aviation Protocols** Current Air Traffic Management suffers from a lack of digitalization, for example analogue voice communications, and insufficient cybersecurity measures in aeronautical datalinks and applications. In Europe, these challenges are investigated within the Single European Sky Air traffic management Research joint undertaking [JU]23b. As a result, a new long-range terrestrial Air-Ground communication protocol was proposed, which must include measures to “[Provide] a secure channel [...] to ensure authentication and integrity of [...] message exchange” [Aer21, Int21]. Currently, the L-band Digital Aeronautical Communications System (LDACS) [JU23a] is under standardization by the International Civil Aviation Organization [Int21], which provides a framework for air-ground communication between civilian aircraft and ground stations. A placement of LDACS in such communication networks is depicted in Figure 1.

At the heart of the LDACS security architecture lies a mutually authenticated key exchange, instantiating either an ISO key agreement protocol [co21] with DH, or an similar protocol where the DH component is exchanged for a key encapsulation mechanism. This
is motivated by the understanding, that the public key exchange schemes undergoing standardization as part of the NIST post-quantum competition [IST22] are all KEMs. After successful key agreement, the resulting key material will be used to secure LDACS control-plane and user-plane data. Examples of user-plane data include applications such as the Controller-Pilot Data Link Communications, Automatic Dependent Surveillance-Contract or Ground-Based Augmentation System. The first is used for communications of clearances, route-changes, speed or radio frequency assignments and other mission critical data. The second application allows the automatic surveillance of the airspace and informs air traffic controllers about the position, levels and headings of aircraft. The third enables fully automatic landings, without the need of a human intervention [JU23a]. Since the landing is naturally a dangerous phase of any flight the lack of a human in the loop as a control instance requires a substantial amount of trust in these data. To the best of our knowledge previous investigations of the LDACS MAKE protocol (for example [MGG+21, MGS21, MGC22]) rely on heuristic arguments and do not provide security proofs or a formal analysis of the security guarantees in the computational and symbolic model.

1.1 Contribution

In this work we bridge the gap between classically and quantum secure authenticated key agreement by when using any (post-quantum) IND-CPA secure key encapsulation mechanism. Our main contribution is the analysis of the LDACS key agreement protocol in Edition 01.01.00 with Template Edition 02.00.05 from 25.04.2023 [JU23a, §C.8.2], which supports to deploys a key encapsulation mechanism instead of a Diffie-Hellman key exchange. We provide a simplified and idealized variant of the real-world protocol in Section 3.1, which we then prove to be secure in a computational, game-based model [BFWW11, dSGFW19], by proving Theorem 1 in Section 4. Additionally, we provide an automated Tamarin proof in the symbolic model, the results of which are outlined in Section 5 assuming a Dolev-Yao attacker.

Theorem 1. Let kem be an IND-CPA secure key encapsulation mechanism except with advantage \( \varepsilon_{kem} \) and correctness \( 1 - \lambda_{kem} \), let sig be an EUF-CMA secure signature scheme except with advantage \( \varepsilon_{sig} \), and prf be an \( \epsilon_{prf} \) secure pseudo-random function. Let \( n \) be a bound on the number of parties and \( l \) a bound on the total number of sessions and \( \kappa \) a security parameter. Then the LDACS MAKE protocol (cf. Figure 3) provides (almost) full explicit entity authentication and (almost) full explicit key authentication, which implicitly includes BR-secrecy. Any quantum polynomial time bounded adversary has advantage of falsifying the notions of at most

\[
4n\varepsilon_{sig} + \frac{4l^2}{2^{2\kappa}} + 5l\lambda_{kem} + 2l^2 \left( \frac{4(\varepsilon_{kem} + \varepsilon_{prf})}{1^2} - 2(\varepsilon_{kem} + \varepsilon_{prf}) - n\varepsilon_{sig} \right) + 2(\varepsilon_{kem} + \varepsilon_{prf}) + \frac{2}{2^\kappa}.
\]

We provide a complete proof of Theorem 1, with modularized security notions and
explicit reductions, giving the precise security loss. The protocol achieves security against polynomially bounded quantum adversaries if the respective instantiations are quantum secure, i.e., if the KEM and the signatures are instantiated with post-quantum secure schemes, and the \textit{prf} is secure with appropriate key length. Independently, we provide a model of the LDACS protocol in Tamarin, achieving security when assuming the cryptographic components to be \textit{perfect}. The results of the latter confirm our findings for the computational proof of the LDACS protocol. We include the source code of the symbolic proof and a \textit{Dockerfile} along with this manuscript to reproduce our results.

1.2 Technical Outline

We consider the setting of two parties each with a unique id, an initiator “ground station” \textit{GS} and a responder “air station” \textit{AS}, engaging in a key agreement scheme. Every party has access to a public-key infrastructure, i.e., a long-term private signing key for an EUF-CMA secure signature scheme \textit{sig} as well as a respective verification key to check signatures of an intended communication partner. Further, the parties have agreed on a cipher suite determining an IND-CPA secure key encapsulation mechanism \textit{kem}, an EUF-CMA secure message authentication code \textit{mac}, and a pseudo-random function \textit{prf}.

The party \textit{GS} initiates the protocol by generating a \textit{fresh} KEM key pair and sending the public key \textit{pk} to \textit{AS}. \textit{AS} runs an encapsulation algorithm on \textit{pk} resulting in a key \textit{k} and a ciphertext. A MAC key and a session key are derived from \textit{k} using the pseudo-random function \textit{prf}. Then the \textit{AS} generates a MAC tag and a signature of the ciphertext, the unique id of \textit{GS} and \textit{pk} using the MAC key and their long-term signature key. Finally, the \textit{AS} sends the ciphertext, the signature and the tag to \textit{GS}. \textit{GS} verifies the signature, decapsulates the ciphertext, derives the MAC key and a session key and verifies the MAC tag. If the MAC and signature verifications succeed, \textit{GS} constructs their own signature and MAC tag of the ciphertext, the id of \textit{AS} and the KEM public key, send both to \textit{AS} and accepts the session key. \textit{AS} accepts their session key if the tag and the signature verify correctly. The above protocol resembles a simplification of the LDACS MAKE protocol as detailed in Section 3.1.

![Explicit Proofs](cf. Section 4.1)  
![Corollaries](cf. Section 4.2)

\begin{figure}[h]  
\centering  
\begin{tikzpicture}  
\node (BRSecrecy) at (0,4) {BRSecrecy};  
\node (Match) at (2,4) {Match};  
\node (aKeyConf) at (4,4) {aKeyConf};  
\node (iKeyConf) at (6,4) {iKeyConf};  
\node (iEntAuth) at (8,4) {iEntAuth};  
\node (fEntConf) at (10,4) {fEntConf};  
\node (KMSoundness) at (2,3) {KMSoundness};  
\node (fExKeyAuth) at (4,3) {fExKeyAuth};  
\node (aExKeyAuth) at (6,3) {aExKeyAuth};  
\node (fExEntAuth) at (8,3) {fExEntAuth};  
\node (aExEntAuth) at (10,3) {aExEntAuth};  
\node (Theorem 1) at (10,-1) {(cf. Theorem 1)};  
\draw [->] (BRSecrecy) -- (Match);  
\draw [->] (Match) -- (aKeyConf);  
\draw [->] (aKeyConf) -- (iKeyConf);  
\draw [->] (iKeyConf) -- (iEntAuth);  
\draw [->] (iEntAuth) -- (fEntConf);  
\draw [->] (KMSoundness) -- (fExKeyAuth);  
\draw [->] (fExKeyAuth) -- (aExKeyAuth);  
\draw [->] (fExEntAuth) -- (aExEntAuth);  
\end{tikzpicture}  
\caption{Overview of computational proof structure, showing how the explicit proofs of the security notions (as defined in Section 2.2) and the consequential security notions are related. The latter notions are implied by the logical conjunction of corresponding preceding notions.}
\end{figure}

The security of the simplified key agreement protocol is captured in the Match-security model [BPR00]. We adopt the predicate-based framework of [dSGFW19] to model security goals and notions. Particularly, we prove all individual notions required to assemble Theorem 1 in Section 4, achieving the following properties:
Entity Authentication. The notion of (Almost) Full Explicit Entity Authentication captures the promise that each party is assured that they interact with their intended peer, and that their peer is aware of the identity of the party. Entity authentication holds due to the EUF-CMA security of the signature scheme $\text{sig}$.

Key Authentication. (Almost) Full Explicit Key Authentication gives the parties assurance that their intended peer and only their intended peer knows the secret key, which holds due to the EUF-CMA security of $\text{sig}$, the IND-CPA security of $\text{kem}$ and the pseudo-randomness of $\text{prf}$. This notion implies BR-secrecy with forward secrecy against weak corruption.

We provide a complete set of explicit proofs to various security notions of [dSGFW19] as outlined in Figure 2. The proof of BR-secrecy, which is implicitly used to assemble Theorem 1, partially follows the SK-security proof of the SIGMA protocol [Kra03, CK02], with the suggestions of [Pei14] for exchanging the DH values for a key encapsulation mechanism in the SIGMA protocol. The adaptions are marked accordingly.

Further, we provide an implementation of mutual authentication, key confirmation and secrecy corresponding to the protocol, which are proven symbolic model, the implementation of which is outlined in Section 2.3, and the results of which are detailed in Section 5. The automated proof supports the findings of the computational proof. The corresponding source code can be run using Tamarin, or setup with the Dockerfile attached to the manuscript.

Remark 1. The message authentication code used in the LDACS protocol has no impact on the security loss in Theorem 1. This is not surprising, since the KEM-based LDACS protocol features a signature similar to ISO-type protocols, which are known [Kra03, §4] to achieve security with DH-based instantiations by including the identities into the signatures. This is also in line with the main goal of LDACS to provide security against attackers that only corrupt the long-term keys.

2 Preliminaries

Let $\kappa$ denote the security parameter and $x \leftarrow X$ uniformly random sampling $x$ from distribution $X$. We denote $x, y$ the (individual) $y$ associated with $x$, and $\mathbb{P}[z]$ as the probability that event $z$ occurs. Whenever we talk about an adversary $A$, we assume that it is polynomially bounded.

2.1 Cryptographic Constructions

This section formally defines the various cryptographic components and their associated security notions used within the paper.

Definition 1 (Key Encapsulation Mechanism (KEM)). A key encapsulation mechanism $\text{kem}$ is a tuple $(\text{Gen}, \text{Encaps}, \text{Decaps})$ of probabilistic polynomial-time (PPT) algorithms: $\text{Gen}$ generates a secret key $sk \in SK$ and a public key $pk \in PK$, $(pk, sk) \leftarrow \text{Gen}(1^\kappa)$, $\text{Encaps}$ generates a key $k \in K$ and a ciphertext $c \in C$ as $(k, c) \leftarrow \text{Encaps}(pk)$, and $\text{Decaps}$ decapsulates the ciphertext to a shared secret, $(k', \bot) \leftarrow \text{Decaps}(sk, c)$, returning either a key or an error symbol $\bot$. The KEM is $\lambda_{\text{kem}}$ correct, if $k'$ is equal to $k$ with a probability of at least $1 - \lambda_{\text{kem}}$.

A common security notion for key encapsulation mechanism is indistinguishability (of the key) under a chosen plaintext attack (IND-CPA). In the game-based security a challenger samples a bit $b^*$ and a key pair $(pk^*, sk^*)$, creates an encapsulation ciphertext $c^*$, and passes to the adversary $pk^*$, $c^*$ and $k^*$, which is either the key from the encapsulation,
We consider game-based security for authenticated key exchange [BFWW11] as formalized parties is the corresponding security notion achieved for a specific entity. The set of authenticating indicating an air station, depending on

\[ I \subset \text{set} \]

\[ \text{Setup: Identities and Protocol Executions} \]

The security model is defined over a

\[ \text{Sec. 2} \] to describe the model and its parameters.

A short version of [dSGFW19] was published as [DFW20]. However, we refer by [dSGFW19], which features precise notation using predicates with explicit security

One-Way Functions (owf)

An efficiently computable function \( \text{owf}: \mathcal{X} \rightarrow \mathcal{Y} \) is called one-way, if for every polynomially bounded adversary and for every \( \kappa \in \mathbb{N} \), the adversary cannot find a pre-image to a given, random image except with advantage \( \varepsilon_{\text{owf}} \leq \text{negl}(\kappa) \):

\[ \text{Adv}_{\text{owf}}(\mathcal{A}, \kappa) := \frac{\text{Prob}\{\text{owf}(x^*) = \text{owf}(x') \mid x' \leftarrow \mathcal{A}(1^\kappa, \text{owf}(x^*)), x^* \leftarrow \mathcal{X}\}}{\text{negl}(\kappa)} \leq \varepsilon_{\text{owf}} \]

2.2 Computational Security Model

We consider game-based security for authenticated key exchange [BFWW11] as formalized by [dSGFW19], which features precise notation using predicates with explicit security properties. A short version of [dSGFW19] was published as [DFW20]. However, we refer to the full version as we believe this to be more accessible. We closely follow [dSGFW19, Sec. 2] to describe the model and its parameters.

Setup: Identities and Protocol Executions The security model is defined over a set \( I \subset \mathbb{N} \) of parties. Each party has a unique party identifier \( i, j \in I \). The total number of parties, \( n = |I| \), is fixed a priori. Later, we will use either \( GS \) as an identifier to indicate that a party is a ground station or \( AS \) indicating an air station, depending on the corresponding security notion achieved for a specific entity. The set of authenticating parties is \( S \). Since we only consider the case of mutual authentication for all parties, we
have $S = I$. We work in the pre-specified peer model, which means, that each party is aware of their own identifier, and also knows their intended partner’s unique identifier, which is also called the pid.

These parties engage in a protocol $Π = (KG, Π_C)$, defined by an initial key generation $KG$ as well an algorithm $Π_C$ corresponding to the locally executed procedure of each party. Each individual execution of a protocol by an entity $i ∈ I$ is called a local session, associated with a local session identifier $ℓ = (i, j, k)$ where $k$ denotes that this is the $k$-th session between party $i$ and party $j$. The total number $ℓ$ of local sessions is bound a priori, such that $k ≤ l$.

**Game States and Bookkeeping** The security of a protocol $Π$ is defined via an experiment called a game, where the adversary engages in protocol executions and adaptively interacts with or corrupts parties. [dSGFW19] introduce five lists to track the individual states of protocol executions and the game.

1. The list SST of protocol-related session states stores for each local session $ℓ = (i, j, k)$ a signature key pair $(vk^i_{sig}, sk^i_{sig})$ of party $i$ as well as their intended partner’s verification key $vk^j_{sig}$. Further, it stores the session identifier, key and two variables, sid, K, kcid, ecid ∈ $\{0, 1\}^* \cup \perp$, all of which are initialized to $\perp$, and are set as soon as the local session accepts. The latter two are set during a session and then remain invariant for the remainder of the session. The kcid’s purpose is to unambiguously determine the value of the session key before the session accepts while the ecid determines the value of the session identifier. The model features a key confirmation flag $kconf$ ∈ {none, almost, full}, denoting which form of confirmation should be achieved. For $GS$ the flag is set to “almost”, and for the $AS$ to “full”.

2. The list LST of game-related local session states corresponds to how the adversary interacts with the sessions throughout the game. For each session, it stores whether the owner and peer of a session are honest or corrupted, $δ_{owner}, δ_{peer} ∈ \{honest, corrupt\}$, and similarly the state of a session $δ_{sess} ∈ \{fresh, revealed\}$. Parties and sessions are honest and fresh by default, and may change their state depending on the adversary’s interaction.

3. The list corresponding to the game execution state EST contains information, $\{(i, vk^i_{sig}, sk^i_{sig}, δ_i)\}$, denoting which parties have been corrupted (independently of sessions).

4. LSID is the list of valid local sessions identifiers.

5. The list MST holds information related to specific security notions.

**Experiment and Adversarial Interaction** Security is defined via an experiment where an adversary interacts with a game. In the setting of quantum-secure communication the adversary $A$ is a quantum polynomial-time algorithm which interacts through classical queries with the game. The set of all queries is $Q = \{SEND, REVEAL, CORRUPT\}$. On input $SEND(ℓ, m)$, the game processes $Π_C$ on $m$ on behalf of local session $ℓ$, and returns the result to the adversary. On input $REVEAL(ℓ)$, the game sets $ℓ, δ_{sess}$ to revealed, and returns $ℓ, K$ to the adversary. On input $CORRUPT(i)$, the entity $i$ is marked as corrupt in variable $δ_i$. Then, for any session owned by that entity $ℓ = (i, i, i)$, and any session where it is listed as a peer $ℓ = (ℓ, i, ·)$, the entity is marked as corrupt, i.e., the game sets $δ_{owner} = corrupt$ (respectively for $δ_{peer}$). Finally, the secret signing key $sk^i_{sig}$ is returned to the adversary.

The game returns responses to the adversary according to an algorithm $χ$, which evaluates a query $q ∈ Q$ and the game state. [dSGFW19] further allow the adversary to submit invalid queries, determined by a predicate $Valid$, for which $χ$ is not executed. We
note that such queries are not relevant in our setting. The state of each game $G$ comprises the five lists from the previous paragraph.

The experiment then consists of three phases: In a first phase of the experiment, key pairs for all entities are generated and variables initialized as previously defined. In the second phase, the adversary may interact with the sessions and parties by submitting queries $q$ to the game, which are processed by $\chi$. In the last phase, after the adversary send all their queries and terminated, the game evaluates a predicate on the state $b \leftarrow P(SST, LST, EST, LSID, MST)$ and outputs the bit $b \in \{0, 1\}$. The adversary wins the game, if $b = 0$.

With this setup, a security notion is fully defined by a predicate $P$. A protocol achieves a security property if for all polynomial-time adversaries $A$ the predicate $P$ evaluates to 1 except with negligible probability, i.e.,

$$\text{Adv}^{G}_{A, II, I, S} = \Pr \left[ \text{Exp}^{G}_{A, II, I, S}(k) = 0 \right] \leq \text{negl}(k),$$

(1)

where $\text{Exp}^{G}_{A, II, I, S}$ corresponds to running the game $G$ with protocol $II$, parties $I$ and authenticating parties $S$ against the adversary $A$. We note that for the remaining paper we only write “adversary” instead of “polynomial-time adversary” for simplification, and security holds against quantum polynomial-time adversaries if the respective components are post-quantum secure.

### 2.2.1 Predicates

We recall the definitions of the various security properties and the predicates introduced by [dSGFW19] with the simplifications relevant to this paper. Note that all predicates are quantified over the list of valid local session identifiers, i.e., $\forall \ell \in \text{LSID}$. The predicates SAMEKEY, SAMEKCID, SAMEECID and PARTNERED are defined to enable the readability of the subsequent predicates:

**Definition 3 (SAMEKEY).** SAMEKEY$(\ell, \ell')$ ⇔ $\ell.K \neq \bot = \ell'.K$ for distinct sessions $\ell, \ell'$.

Remark: The definitions for SAMEKCID and SAMEECID are analogous.

**Definition 4 (PARTNERED).** PARTNERED$(\ell, \ell')$ ⇔ $\ell \neq \ell'$ and $\ell.side = \ell'.side \neq \bot$.

The MATCH property promises, intuitively, that two parties engaging with the same session identifier also derive the same key $K$ and $kcid$, and that the latter guarantees the computation of identical keys. Additionally, the property promises that each local session is partnered with at most one other local session.

**Definition 5 (Match predicate).**

MATCH ⇐ $\forall \ell, \ell', \ell'' : (\text{PARTNERED}(\ell, \ell') \land \ell.K \neq \bot = \ell'.K) \implies \text{SAMEKEY}(\ell, \ell')$

$\land (\text{PARTNERED}(\ell, \ell') \land \ell.kcid \neq \bot = \ell'.kcid) \implies \text{SAMEKCID}(\ell, \ell')$

$\land (\text{PARTNERED}(\ell, \ell') \land \text{PARTNERED}(\ell, \ell'')) \implies \ell = \ell''$

$\land (\text{SAMEKCID}(\ell, \ell') \land \ell.K \neq \bot = \ell'.K) \implies \text{SAMEKEY}(\ell, \ell')$

**Entity and Key Authentication** Implicit entity authentication holds, if any party is guaranteed that for each of its sessions, only its intended partner has a matching sid.

**Definition 6 (Implicit Entity Authentication).**

$\text{iEntAuth} \iff \forall \ell : (\forall \ell' : \text{PARTNERED}(\ell, \ell') : \ell'.id = \ell.pid)$
Entity confirmation improves this by providing assurance that there exists another session with the same sid ("full"), or the same ecid ("almost full"), where for the latter matching ecids eventually result in the same sid if the respective session terminates successfully.

**Definition 7** (Full Entity Confirmation).

\( f_{\text{EntConf}} \iff \forall \ell \text{ that accept } \land \ell.\delta_{\text{peer}} = \text{honest} : \exists \ell' : \text{PARTNERED}(\ell, \ell') \)

**Definition 8** (Almost-Full Entity Confirmation).

\( a_{\text{EntConf}} \iff \forall \ell \text{ that accept } \land \ell.\delta_{\text{peer}} = \text{honest} : \exists \ell' : (\text{SAMEECID}(\ell, \ell') \land (\ell'.\text{sid} \neq \bot \implies \text{PARTNERED}(\ell, \ell'))) \)

"Almost" full key confirmation promises, that parties engaging with an honest peer have assurance, that their peer derives the same key. We note that "full" key confirmation is implied by another, stronger predicates later on, and thus not explicitly defined.

**Definition 9** (Almost-Full Key Confirmation).

\( a_{\text{KeyConf}} \iff \forall \ell \text{ that accept } \land \ell.\delta_{\text{peer}} = \text{honest} : \exists \ell' : \text{SAMEKCID}(\ell, \ell') \land ((\ell'.\text{K} \neq \bot) \implies \text{SAMEKEY}(\ell, \ell')) \)

The following four primary security notions of [dSGFW19] are the main terms in our Theorem 1. (Almost) Full explicit entity authentication promises that for honest, authenticating parties only the intended partner has a matching sid and there exists at least one such session with matching sid (respectively ecid for "almost").

**Definition 10** (Full Explicit Entity Authentication).

\( f_{\text{exEntAuth}} \iff \forall \ell \text{ that accept } : (\forall \ell' : \text{PARTNERED}(\ell, \ell') : \ell'.\text{id} = \ell.\text{pid}) \land (\ell.\delta_{\text{peer}} = \text{honest} \implies \exists \ell' : \text{PARTNERED}(\ell, \ell')) \)

**Definition 11** (Almost-Full Explicit Entity Authentication).

\( a_{\text{exEntAuth}} \iff \forall \ell \text{ that accept } : (\forall \ell' : \text{PARTNERED}(\ell, \ell') : \ell'.\text{id} = \ell.\text{pid}) \land (\ell.\delta_{\text{peer}} = \text{honest} \implies \exists \ell' : \text{SAMEECID}(\ell, \ell')) \land (\ell'.\text{sid} \neq \bot \implies \text{PARTNERED}(\ell, \ell')) \)

Similarly, (almost) full explicit key authentication promises that only the intended partner has sessions with matching key and that at least one such session with matching key exists (respectively kcid).

**Definition 12** (Full Explicit Key Authentication).

\( f_{\text{exKeyAuth}} \iff \forall \ell \text{ that accept } : (\forall \ell' : \text{SAMEKEY}(\ell, \ell') : \ell'.\text{id} = \ell.\text{pid}) \land (\ell.\delta_{\text{peer}} = \text{honest} \implies \exists \ell' : \text{SAMEKEY}(\ell, \ell')) \)

**Definition 13** (Almost-Full Explicit Key Authentication).

\( a_{\text{exKeyAuth}} \iff \forall \ell \text{ that accept } : (\forall \ell' : \text{SAMEKEY}(\ell, \ell') : \ell'.\text{id} = \ell.\text{pid}) \land (\ell.\delta_{\text{peer}} = \text{honest} \implies \exists \ell' : \text{SAMEKCID}(\ell, \ell') \land (\ell'.\text{K} \neq \bot \implies \text{SAMEKEY}(\ell, \ell'))) \)
Secrecy To define BRSec, \([dSGFW19, \S 5]\) provide a modified game \(G_{BRSec}\), where the adversary’s goal is to distinguish a real and a random session key. The modified game state includes EST, SST, LST. The state MST includes two additional bits and a challenge session. The bit \(b_{test}\) holds whether the adversary is provided with a real key from a session, or whether they are provided with a random key. The bit \(b_{guess}\) will hold the adversary’s guess. The challenge session \(\ell_{test}\) will correspond to the adversary’s choice of which session to test. To set these states, the game provides two additional queries to the adversary. On input \(Test(\ell)\), the game sets the test session \(\ell_{test} \leftarrow \ell\) and returns \(K = \ell.K\) if \(b_{test} = 1\), or a random key \(K\) from the key space if \(b_{test} = 0\). On input \(Guess(b)\), the bit \(b_{guess} \leftarrow b\) is updated. Additionally, the game restricts the adversary to submit only a single \(Test\) query. The the \(BRSec\) predicate evaluates to the bit \(b_{guess}\) as in Definition 14:

**Definition 14 (BR-secrecy).** The \(BRSec\) predicate is defined as follows:

\[
\text{if } \text{MST}.\ell_{test} \neq \bot \land \ell.\delta_{own} = \ell.\delta_{peer} = \text{honest} \land \ell.\delta_{sess} = \text{fresh} \land \forall \ell' \in \text{LST} : \text{Partnered}(\ell, \ell') \Rightarrow \ell'.\delta_{sess} = \text{fresh} \\
\text{then } \text{BRSec} \leftarrow \text{MST}.b_{guess} \\
\text{else } \text{BRSec} \leftarrow 0
\]

Let \(G_{BRSec}^{b_{test}=b}\) denote the BR-secrecy game during which \(b_{test}\) has the value \(b\). Due to the distinguishing nature of the BR-secrecy game, the adversarial advantage is defined as

\[
\text{Adv}_{A, I, I, I}(1^\kappa) := \frac{\Pr \left[ \text{Exp}_{A, I, I, I}(1^\kappa) = 1 \right] - \Pr \left[ \text{Exp}_{A, I, I, I}(1^\kappa) = 1 \right]}{2}.
\]

**Remark 2.** In \([dSGFW19, \text{Def } 5.2]\), the \(BRSec\) predicate has value \(\bot\) in some cases. Since the adversarial advantage does not distinguish whether \(BRSec\) has the value 0 or \(\bot\), we omit this detail.

### 2.3 Symbolic Security Model

The symbolic proof model establishes the correctness and security of a cryptographic protocol without making assumptions about the computational limitations of an adversary. The adversary is modeled as a Dolev-Yao attacker [NS78, DY83], who can send, receive or alter messages in interactive protocols, and who has access to cryptographic primitives as perfect black-boxes. The messages sent over the network are inputs to these black-boxes and the adversary is restricted to use only these. A protocol is formalized using correspondence assertions of the form “If event x is executed, then event y is executed”. An automated symbolic prover, such as Tamarin [MSCB13], can check whether a protocol fulfills security goals by (exhaustively) exploring the possible options for parties (called agents) assuming the various roles in the protocol.

In Tamarin [MSCB13], security is formalized over a system state as an initially empty multi-set of predicates called facts. Rules define how the state can transition to a new set, adding or removing facts from the system state. Each rule is associated with a premise and a conclusion. A rule can only be applied, if all facts of the premise are present in the system state. If the rule is applied, then the system state is updated according to the facts in the conclusion. Additionally, rules may feature action facts, which record the application of the rule by appending all action facts to a trace.

With these rules the algorithmic behaviors of a protocol can be modeled by defining rules mimicking the interaction of the agents. Similarly, adversarial powers can be modeled via action facts, for example, a rule may feature an action fact representing that a long-term secret is available to the adversary and that the corresponding party is corrupted.

Security properties on the other hand are modeled via traces of action facts. These are denoted lemmas. This means, a property is modeled by giving a formula which is
evaluated on the traces. Then a security property can be modeled either with an existential (“exists”) or an universal (“all”) quantification, indicating that the formula has to evaluate to \( \text{True} \) either for any one trace, or for all traces. Usually, security properties are required to hold for all traces.

**Protocol and Adversarial Rules** The Tamarin manual [Tea23] already provides built-in code for signing and hashing. Celi et al. [CHSW22a, §3.2.1] provide a Tamarin instantiation of a KEM, which satisfies Definition 1. The protocol described in Section 2.3 is modeled via rules and facts, allowing each party corresponding to a unique identifier to register a long-term key, and then to engage with any other party in a protocol session.

To model the adversary additional rules are added that allow to reveal the long-term key, a KEM key or a session key: The rule “Reveal_ltk” has as premises a long-term key associated with an agent \( X \), an action fact that marks the agent as corrupted via the fact “CorruptedLtik(X)”, and which adds the long-term key in question as a conclusion fact to the state. Analogously, “Reveal_kem” and “Leak_session” allow to reveal the secret key output by \( \text{Encaps} \), \( \text{Decaps} \), or the session key. As such, the adversary in the symbolic model is slightly stronger than in the computational model, as they are allowed to have the KEM key leaked (in the computational model, only long-term key via a \( \text{Corrupt} \) query and session keys via \( \text{Reveal} \) queries (or \( \text{Test} \) queries, in the \( \text{BRSec} \) predicate)).

**Security Properties** In the following we describe the lemmas associated with the security properties relevant to this work, where agent A and B correspond to the ground-and air stations:

- **mutual_authentication\_A/B** The property is modeled via Lowes [Low97] bi-directional full-agreement property as outlined in the Tamarin manual [Tea23], combined with a unique element exchanged between agent A and B. Full agreement is the combination of injective agreement, i.e., stating that if agent A accepts with agent B, then they can be sure B also accepted with A, except if either of long-term keys was revealed (resulting in corruption of the agent as an action fact). The uniqueness property is modeled via the \( \text{session\_uniqueness\_A/B} \) lemma (modeled as in [GGCG\_21]), i.e., the guarantee that different sessions have different keys. When both lemmas hold, mutual authentication is achieved via full-agreement. Hence, the \( \text{mutual\_authentication\_A/B} \) lemma can be regarded as a combination of Definitions 6 to 8.

- **secrecy** Secrecy corresponds to BR-secrecy, promising that when a session key \( x \) is assigned a “secret” property at time \( i \), then either the adversary does not know \( x \), or \( x \) has been revealed, or a corresponding agent was marked as corrupted via an action fact. Similarly, **secrecy\_pfs** guarantees, that the adversary does not know \( x \), except if the agent was corrupted at a time \( j \) prior to \( i \), i.e., \( j < i \).

- **key\_consistency\_A/B** Key consistency [GGCG\_21, §A.6.4] corresponds to key confirmation, such that for all sessions with agents A and B with keys keyA and keyB respectively, the following holds: When agent A accepts keyA at time \( i \) in session \( t_A \), and agent B accepts with keyB at time \( j \) in the same session, then keyA and keyB must be same, except if one of the agents was corrupted. This corresponds to key confirmation in the computational model.

The models of session uniqueness and key confirmation are based on the implementation from Donenfeld et al. [DM17].
3 LDACS

In this section, we provide a simplified protocol resembling the LDACS MAKE. The LDACS MAKE protocol in Edition 01.01.00 with Template Edition 02.00.05 from 25.04.2023 [JU23a, §C.8.2] features two individual definitions that either use a Diffie-Hellman key exchange, or a KEM based key exchange. The first instantiates the standardized Key Agreement Mechanism 7 (KAM-7) [co21, §11.7], and inherits all security properties. As such, we do not provide any further analysis of this instantiation. The latter substitutes the Diffie-Hellman key exchange for a construction using a key encapsulation mechanism, and thus does not instantiate ISO KAM-7, as this requires to be instantiated with a commutative function $F$:

The session key is computed as $k = F(r_i, F(r_j, g)) = F(r_j F(r_i, g))$ [co21, §10.2], where $r_i$ is a random value provided by one party, and $r_j$ by the other party. The variant with the key encapsulation, however, computes the session key from $k, c ← Encaps(pk_{kem}, r_j)$ and $k ← Decaps(c)$, and thus does strictly not instantiate ISO KAM-7. As a consequence, the KEM-based protocol does not inherit the security properties of the ISO KAM-7. An examination of the security objectives [oI23, JU23a], which are in understanding of the official security requirements for aeronautical communications set by the International Civil Aviation Organization (ICAO) [Aer21, Int21], is provided in this context. In Section 3.2 we compare our results to other authenticated key agreements.

3.1 Key Agreement Protocol

The LDACS MAKE protocol is split into two phases: In the cell entry stage, the two parties ground station GS and air station AS exchange miscellaneous information over an insecure channel with no attempt to achieve any security. At the end of the cell entry, both parties are aware of an intended partner associated by an identifier $id_{GS}$ and $id_{AS}$, as well as a cipher suite used in the instantiation of the subsequent stage. Additionally, the AS may send a flag signaling that they do not have the GS’s signature public key $vk_{sigGS}$, which may then be sent (in plain) by GS. We note that no security must hold for this initial phase, and this is not modeled in the protocol. Instead, we assume the intended entity identifiers $id_{GS}$, $id_{AS}$ and respective signature keys from the public key infrastructure to be an input to the respective party. In the second stage, the two parties engage in a mutual authenticated key agreement protocol to exchange a secret that is used to derive multiple keys. This second stage is the 3-round MAKE protocol between two parties, the KEM-variant of which is the focus our analysis.

The protocol described in Figure 3 is a simplifications of the second stage from Section 3.1: Both parties take as input a unique identifier pid for an intended partner, their own unique identifier id, the public key $vk_{pid}$ of the intended partner, as well as the secret signing key $sk_{sigid}$, the latter two of which are provided by the public key infrastructure. After completing the protocol, if the parties accept, then they have a session key K and assurance that only their intended partner has knowledge of this key. The desired security properties are discussed below, the achieved security notions along with the respective proof in Section 4. We prove the computational security of these notions in the game-based model [BFWW11, DFW20] for authenticated key exchange, and verify the security properties in the symbolic model using the Tamarin prover.

Simplifications  The LDACS MAKE protocol in the specification [JU23a, §C.8.2] details the instantiation of the key derivation as well as identifier strings constructed from constant values that result in multiple individual session keys, which are not relevant to security. In order to de-clutter the specification and provide a clear view of the protocol in question, we simplified the specification. In this paragraph we make these simplifications explicit and provide assumptions and justifications required for security of the protocol:
\[\text{sid}_{GS} := (\text{id}_{GS}, \text{id}_{AS}, \text{pk}_{kem}, c)\]
\[\text{sid}_{AS} := (\text{id}_{GS}, \text{id}_{AS}, \text{pk}_{kem}, c)\]
\[\text{pid}_{GS} := \text{id}_{AS}\]
\[\text{pid}_{AS} := \text{id}_{GS}\]

**Figure 3:** Simplified key agreement protocol between the ground station \(GS\) and the air station \(AS\). We denote this protocol LDACS MAKE. If any of the verification \(\text{Vfy}\) or \(\text{MacVfy}\) fail, the respective party aborts. The dotted lines with the blue identifiers are relevant for the computational proof in Section 4.

1. The ground and air station are uniquely identified by \(\text{id}_{GS} = (\text{UA}_{GS}, \text{SAC}_{GS})\) and \(\text{id}_{AS} = (\text{UA}_{AS}, \text{SAC}_{AS})\) respectively.
2. If \(\text{id}_{GS}, \text{id}_{AS}\) are unique identifiers, then so is \(\mathcal{H}(\text{id}_{GS}, \text{id}_{AS})\).
3. Security achieved for the session key \(K_X\) also holds for multiple keys, i.e., “DCH session key”, “Voice session key”, “DCCH session key” and “Key encryption key”.
4. The composition of \(HKDF\) and \(HMAC_{\text{Hash}}\) is a pseudo random function.
5. Authentication Centers (AuC) are treated as if they were \(GS\)s.

Simplification (1) is purely cosmetic. Simplification (2) is justified because \(SHA256, \mathcal{H}\), is believed to be a collision resistant hash function [IST15]. Simplification (3) is justified because all keys are derived in the same manner, by computing \(prf(k, (\mathcal{H}(\text{id}_{GS}, \text{id}_{AS}), 1))\) with constant strings as additional inputs. Simplification (4) is justified, because \(HMAC\) instantiated with \(SHA256\) is a pseudo-random function as shown by [Bel06]. This assumes that \(HKDF\) is instantiated accordingly. For Simplification (5), the specification mentions the possibility for \(GS\) to verify the \(AS\) certificates by communicating with an Authentication...
Center (AuC) over a secure channel [JU23a, §C.8.2] (see the “dashed” box). Since the communication with the AuC is considered secure we ignore this special case, and simply assume that the ground station can verify the correctness of the AS certificate locally. To the best of our knowledge our simplifications do not invalidate any security guarantees for the protocol as in the specification, since we only merge redundant components.

Security Goals Aeronautical standards are split in two parts: First, the ICAO Standards And Recommended Practices (SARPs) define requirements of the technology; second, the specification described the technical realization of these requirements. As such, LDACS security goals are described in the SARPs [oI23], with the LDACS specification [JU23a] detailing the protocols and other security measures.

LDACS SARPs [oI23] set requirements for providing integrity protection [oI23, §13.8.2] and confidentiality [oI23, §13.8.4] of messages in transit, as well as mutual authentication [oI23, §13.8.5] between ground and air stations. These basic requirements were extended upon in the LDACS specification, i.e., that the key agreement fulfills mutual authentication and key establishment [JU23a, §C.8.2], as well as key confirmation [JU23a, §C.2, table 96] without specifying details. Further, the requirements ask for a “capability to prevent the propagation of intrusions within the LDACS access networks” [oI23, §13.8.8], which may be interpreted as forward secrecy, such that leakage of long-term keys does not invalidate security properties of other, honest parties.

3.2 Comparison with other KEM-based Key Agreements

SIGMA-style Authentication The simplified protocol in Figure 3 is similar to the protocol suggested by [Pei14, §6.2], with adjustments to the messages used to generate the signature and the tag. [Pei14, Thm 6.1] states, that their protocol is secure in the CK02 model but no complete proof is provided. Indeed, our proof of BR-secrecy partially follows the sketch they outlined, and we mark this in Section 4 where appropriate.

[BBF +19] present a compiler for hybrid authenticated key exchange, combining multiple KEMs and a SIGMA-style authentication scheme [BBF +19, Fig. 13]. Particularly, their scheme exchanges a KEM public key and ciphertext, which is subsequently authenticated along with a randomly sampled string (a nonce) along with the party identifiers. The authors show that their AKE construction provides BR-Match security and BR key secrecy in the BR93 model if the KEM is IND-CPA secure and if the signature scheme and the MAC are EUF-CMA secure, thus providing security against quantum adversaries, if the underlying components are quantum secure. In contrast, the protocol used in LDACS as well as our abstraction in Figure 3 uses ISO-style authentication and no nonces.

Comparison to Key Exchange in IKEv2 The minimal key exchange component [KHN +14b, Section 1.2] of the Internet Key Exchange Version 2 [KHN +14a] consists of an initialization step IKE_SA_INIT and an authentication step IKE_AUTH, corresponding to the first three messages exchanged between the parties. Similarly to our setting, IKEv2 builds on an existing public key infrastructure and assumes that both parties can validate respective signatures. In the first step, the two parties perform a DH key agreement along with exchanging a randomly chosen nonce for each party. Using the shared secret and the two nonces they derive several keys [KHN +14a, Section 2.14] such as a session key and an additional key used for further authentication. In the second step, IKE_AUTH, each party sends an authenticated encryption with associated data (AEAD) of its own id and of a signature. The signature contains the message the party sent in the IKE_SA_INIT exchange, the nonce of the other party and the output of a PRF with the id of the party as input [KHN +14a, Section 2.15]. The AEAD and the PRF use some of the keys derived after IKE_SA_INIT.
The main differences between the key agreement of IKEv2 and the simplified protocol Figure 3 are that IKEv2 uses DH specifically and makes use of additional nonces. Further, they use an AEAD for the IKE_AUTH messages, and the signatures contain neither the id nor the DH exponential of the respective other party. They use a PRF instead of a MAC, the PRF output is contained in the signature and the PRF does not take the id of the other party as input.

Finally, IKEv2 [KHN+14a, §2.12] allows the reuse of DH exponents. Since the KEM’s pk and \( c \) in the LDACS protocol also function as nonces (i.e., for each session they are chosen freshly uniformly at random and are unique except with negligible probability), it is essential that they are not reused, which is in line the LDACS specification.

4 Computational Proof

In this section we present the computational proof of security for the key agreement protocol described in Section 3. Specifically, we prove correctness of Implicit Entity Authentication (cf. Theorem 3) and BR secrecy (cf. Theorem 7) for both parties, Full entity confirmation (cf. Theorem 4) for the air station \( AS \), and Almost Full Entity Confirmation (cf. Theorem 5) and Almost Full Key confirmation (cf. Theorem 6) for the ground station \( GS \). From this, additional properties can be inferred, as detailed in Section 4.2.

4.1 Explicit Proofs and Reductions

We start by proving Lemma 1 which will be used throughout the subsequent proof. For all of the proof we set \( kcid = sid = ecid = (id_{GS}, id_{AS}, pk_{kem}, c) \). For the remaining section we note that the key output space of the \( kem \) and the key input space of the \( prf \) are identical. The same holds for the key space of the \( mac \) and the co-domain of the \( prf \), i.e., \( K_{kem} = K_{prf}, Y_{prf} = K_{mac} \).

Lemma 1. Let \( A \) be an adversary interacting with the LDACS MAKE protocol. Let \( sig \) be an \( \epsilon_{sig} \) secure signature scheme and \( n \) the number of parties participating in the protocol. Then the probability that an adversary can forge a signature of a party \( P \) that was not corrupted (cf. Definition 21) is bounded by

\[
\mathbb{P}[\text{Sig-Forge}] \leq n \cdot \epsilon_{sig}.
\]

Proof. For an adversary forging a signature we can construct a trivial reduction that first guesses the impersonated party, and then uses the forgery to win the EUF-CMA game, thus the lemma only depends on the security of the signature scheme. A full proof is given in Appendix A1, which loosely corresponds to part of [CK02, Lemma 7].

Theorem 2 (Match Security, cf. Definition 5). Let \( kem \) be \( \lambda_{kem} \) correct and \( l \) the number of local sessions. Any adversary’s advantage to falsify the Match predicate in LDACS MAKE is bounded by

\[
\forall \text{ adversaries } A : \text{Adv}_{A, H, \mathcal{T}}^{G_{sync}}(1^n) \leq \frac{l^2}{2^{2n}} + l\lambda_{kem}.
\]

Proof. Recall that the kcid and session identifier are identical, kcid = sid, thus if \( \ell, \ell' \) are partnered and the kcid is set, then they also Match. Since \( \ell, kcid := (id_{GS}, id_{AS}, pk_{kem}, c) \), they have the same view of the ciphertext \( c \) and the public key \( pk_{kem} \), and thus the keys Match, except with probability \( \lambda_{kem} \), the latter of which can occur on every session in question. Second, if the sessions \( \ell', \ell'' \) both share the same view of the sid with session \( \ell \), then \( \ell' = \ell'' \) except if there is a collision in both the public key and ciphertext, which happens with probability at most \( 1/2^{2n} \) for each pair of instances.
Theorem 3 (Implicit Entity Authentication, cf. Definition 6). Any adversary’s advantage of falsifying the $i\text{ENTAUTH}$ predicate is zero:

$$\forall \text{adversaries } A : \text{Adv}_{A,H,I,I}^{G_{\text{ EvenAuth}}}(1^\kappa) = 0$$

Proof. This is trivially fulfilled due to Matching $\text{id} := (\text{id}_{GS}, \text{id}_{AS}, \text{pk}_{kem}, c)$.

Theorem 4 (Full Entity Confirmation, cf. Definition 7). Let $\text{sig}$ be an $\varepsilon_{\text{sig}}$ secure signature scheme. Any adversary’s advantage of falsifying the $F\text{ENTCONF}$ predicate for the air station $AS$ is bounded by

$$\forall \text{adversaries } A : \text{Adv}_{A,H,I,I}^{G_{\text{ EvenConf}}}(1^\kappa) \leq n\varepsilon_{\text{sig}}$$

Proof. Let $\ell_{AS}$ be a session with peer $\ell_{GS}$. Then $\ell_{AS}$ accepts after they received a signature $\sigma \leftarrow \text{SIGN}(sk_{GS}^{\text{sid}}, (\text{id}_{AS}, c, \text{pk}_{kem}))$ such that $\text{Vfy}(vk_{GS}^{\text{sid}}, (\text{id}_{AS}, c, \text{pk}_{kem}), \sigma)$ evaluates to 1. For an honest peer $\ell_{GS}, \text{id} = \ell_{GS}, \text{id}$ it holds that $\ell_{GS}, \text{sid} := (\ell_{GS}, \text{id}, \ell_{AS}, \text{id}, \text{pk}_{kem}, c)$, which is the same view of sid that $\ell_{AS}$ has, and thus they are partnered. For the successful verification we can construct a reduction to the EUF-CMA security of the signature analog to that of Lemma 1, such that the advantage is bounded by $n\varepsilon_{\text{sig}}$.

Theorem 5 (Almost-Full Entity Confirmation, cf. Definition 8). Let $\text{sig}$ be an $\varepsilon_{\text{sig}}$ secure signature scheme. The $\text{af\text{ENTCONF}}$ predicate is fulfilled for the ground station $GS$ if sig is a secure signature scheme:

$$\forall \text{adversaries } A : \text{Adv}_{A,H,I,I}^{G_{\text{ afEvenConf}}}(1^\kappa) \leq n\varepsilon_{\text{sig}}$$

Proof. The proof is the same as for Theorem 4 with the argument over the ecid instead of the sid.

Theorem 6 (Almost-Full Key Confirmation, cf. Definition 9). Let $\text{sig}$ be an $\varepsilon_{\text{sig}}$ secure signature scheme, and kem $\lambda_{\text{kem}}$ correct. The $\text{af\text{KEYCONF}}$ predicate is fulfilled for the ground station $GS$, if sig is a secure signature scheme:

$$\forall \text{adversaries } A : \text{Adv}_{A,H,I,I}^{G_{\text{ afEvenConf}}}(1^\kappa) \leq n\varepsilon_{\text{sig}} + \lambda_{\text{kem}}$$

Proof. The proof is the same as for Theorem 4, but with kcids instead of sid. Additionally, $\text{af\text{KEYCONF}}$ requires $\ell, \ell'$ to have the same key, which is the case if the kcids Match, except if the kem fails to decapsulate correctly.

Theorem 7 (BR-Secrecy, cf. Definition 14). The $BR\text{Sec}$ predicate is fulfilled for both parties, if kem, prf and sig are secure, i.e., $\varepsilon_{\text{kem}}, \varepsilon_{\text{prf}}, \varepsilon_{\text{sig}} \leq \text{negl}(\kappa)$:

$$\forall \text{adversaries } A : \text{Adv}_{A,H,I,I}^{G_{\text{ BASEC}}}(1^\kappa) \leq \frac{4(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{\frac{1}{2} - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})} + 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})$$

Proof. The proof of BR-secrecy for the LDACS MAKE protocol shows that the probability of an adversary to distinguish the experiment $G_{\text{BRSEC}}$ outputting a real or random key is negligible. In this section we sketch the proof, a full proof can be found in Appendix A1.1.

We follow the proof of SK-security for the basic SIGMA protocol [CK02], which defines five hybrids via five variants of a simulator $S$. Each of the $S$ variants guesses the test session and its partner in order to modify the generation of the session and mac keys for these two local sessions. If $S$ guesses incorrectly or the adversary manipulates the communication between the two local sessions, then the simulator aborts. The first of the hybrids (“REAL”) corresponds to the $G_{\text{BRSEC}}$ game with real Test output, unless the associated simulator $S_{\text{REAL}}$ aborts. In the second, denoted “RPRF”, the shared secret is exchanged for randomness which is used to compute the session and mac key. In the
third game, “ALLR”, both the session and the mac key are exchanged for randomness. The fourth game, “HYBR”, reverses the change for the mac key, to be generated from a random secret again. Finally, in the last game “RAND”, the mac key is reversed to be generated from the exchanged secret, and only the session key is set to a random value. Figure 4 shows how the five hybrids correspond to the individual lemmata to show indistinguishability of real and random outputs of the Test query in $G_{BRSec}$.

![Figure 4: Overview of the lemmas in our proof of BR-Secrecy for the LDACS MAKE protocol. The five middle columns resemble the hybrid games according to the proof of SK-security in [CK02].](image)

We define four different events which may occur during $G_{BRSec}$ or one of the hybrids: An Abort event happens when the $\hat{S}$ simulator aborts, i.e., it guessed the test session or its partner incorrectly or the adversary manipulated the communication between the two local sessions. An Affirm event happens when the adversary sets $b_{guess}$ to 1. Since the adversary acts as a distinguisher, we can express the indistinguishability of the hybrids via a negligible difference in the probabilities of the Affirm event. A Guess event happens when the $\hat{S}$ simulator guesses correctly. A Sig-Forge event happens when the adversary successfully forges a signature from one of the protocol parties.

As a first step, our proof constructs Lemmas 2 to 5, which show that the probabilities of the four events only differ by a negligible amount between the different variants of the $\hat{S}$ simulator (cf. Appendix A1.1.3). Since we get $\hat{S}_{RPRF}$ from $\hat{S}_{REAL}$ and $\hat{S}_{HYBR}$ from $\hat{S}_{RAND}$ by replacing the shared secret of the two guessed local sessions with a random value, and since in our case, the shared secret is a kem key, we can use the IND-CPA property of the kem to show the negligible difference between these simulators. We get $\hat{S}_{ALLR}$ from $\hat{S}_{RPRF}$ or from $\hat{S}_{HYBR}$ by replacing the outputs of the prf with random values for the two guessed local sessions. Therefore, the negligible difference between these simulators follows from the prf property.

Subsequently, we make a connection between the hybrid games and the $G_{BRSec}$ game. For this purpose, we first define Lemmas 6 to 8. Lemma 6 states that an Abort and a Guess event cannot coincide under an $\hat{S}_{REAL}$ simulator. Recall that a Guess event implies that the simulator guesses the test session and its partner correctly. This especially means that a local session exists which will eventually become the partner of the test session, unless it aborts. In our case, that local session has the same ecid as the test session. The ecid of a local session is composed of the identities of the two parties involved in the current protocol session as well as the public key and the ciphertext for the kem, which also are all the values and identities that the adversary could have manipulated via the exchanged messages. Thus, in case of a Guess event, the simulator guesses the test session and its partner correctly and the adversary does not manipulate the communication between the two, i.e. the simulator will not abort.

Lemma 7 shows that each local session which accepts and has an uncorrupted intended partner has the same ecid as some other local session. To ensure identical ecids, either of
the two exchanged signatures is sufficient since it covers the public key and the ciphertext for the kem as well as the identity of the party which receives the signature. The identity of the signer is implicitly associated to the verification key. The lemma is useful for Lemma 8, which establishes a noticeable lower bound for a Guess event. The probability of correctly guessing two specific local sessions is trivially noticeable in the size of the set of all local sessions. However, the test session may not even have a partner, so we also need to use Lemma 7 to limit the probability for this case.

Now we are able to show in Lemmas 9 and 10 that the “REAL” hybrid given a Guess event is equivalent to $G_{BRSec}$ with real Test output and that the “RAND” hybrid given a Guess event is equivalent to $G_{BRSec}$ with random Test output, except for a negligible probability. The reasoning is that, by Lemma 6, a Guess event prevents the simulator from aborting. If the simulator does not abort, then all local sessions behave consistently and thus the adversary cannot distinguish between the simulation of the hybrids and $G_{BRSec}$. Finally, we combine all game hops in Lemmas 2 to 5, 9 and 10 to prove the BR-secrecy of the LDACS MAKE protocol. Although we now only consider the hybrids under the precondition that a Guess event happens, the game hops of Lemmas 2 to 5 are still valid since Lemma 8 proved the probability of a Guess event to be noticeable.

4.2 Consequential Security Properties

Following the work of De Saint Guilhem et al. [dSGFW19], the Theorems 2 to 7 also imply the following security notions:

**Corollary 1** (Full Explicit Entity Authentication, cf. Definition 10). The $fexEntAuth$ predicate is fulfilled for the air station AS if sig is a secure signature scheme:

$$\forall \text{adversaries } A : \operatorname{Adv}^{G_{fexEntAuth}(1^\kappa)}_{A,\Pi,\mathcal{I},\mathcal{L}}(1^\kappa) \leq n \cdot \varepsilon_{\text{sig}}$$

This follows from $iEntAuth \land fEntConf \Leftrightarrow fexEntAuth$ [dSGFW19, Prop. 9.3.] and from Theorems 3 and 4.

**Corollary 2** (Almost-Full Explicit Entity Authentication, cf. Definition 11). The $afexEntAuth$ predicate is fulfilled for the ground station GS if sig is a secure signature scheme:

$$\forall \text{adversaries } A : \operatorname{Adv}^{G_{afexEntAuth}(1^\kappa)}_{A,\Pi,\mathcal{I},\mathcal{L}}(1^\kappa) \leq n \cdot \varepsilon_{\text{sig}}$$

This follows from $iEntAuth \land afEntConf \Leftrightarrow afexEntAuth$, which can be proven in an analogous way to [dSGFW19, Thm. 3.1.], and from Theorems 3 and 5.

**Corollary 3** (Key-Match Soundness). The $KMSoundness$ predicate is fulfilled for both parties if kem, prf and sig are secure:

$$\forall \text{adversaries } A : \operatorname{Adv}^{G_{KMSoundness}(1^\kappa)}_{A,\Pi,\mathcal{I},\mathcal{L}}(1^\kappa) \leq l^2 \cdot \left( \frac{4(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{l^2} - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) - n \varepsilon_{\text{sig}} \right) + \left( \frac{l^2}{2^\kappa} + 1 \right)$$

This follows from Theorems 2 and 7 and from [dSGFW19, Theorem 5.1.], which states that, with session key space $\mathcal{K}_\Pi$, the following holds:

$$\forall \text{adversaries } A \exists \text{adversaries } B_1, B_2 :$$

$$\operatorname{Adv}^{G_{KMSoundness}(1^\kappa)}_{A,\Pi,\mathcal{I},\mathcal{L}}(1^\kappa) \leq l^2 \cdot \operatorname{Adv}^{G_{BRSec}(1^\kappa)}_{B_2,\Pi,\mathcal{I},\mathcal{L}}(1^\kappa) + \operatorname{Adv}^{G_{KMSound}(1^\kappa)}_{B_1,\Pi,\mathcal{I},\mathcal{L}}(1^\kappa) + \frac{1}{|\mathcal{K}_\Pi|}.$$
Corollary 4 (Implicit Key Authentication). The iKeyAUTH predicate is fulfilled for both parties if kem, prf and sig are secure:

\[ \forall \text{adversaries} A : \text{Adv}^{G_{\text{iKeyAuth}, \Pi, I}}_{A, \Pi, I}(1^\kappa) \leq l^2 \left( \frac{4(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{1 - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})} - n\varepsilon_{\text{sig}} \right) + 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) + 2 \cdot \left( \frac{l^2}{2^\kappa} + l\lambda_{\text{kem}} \right) + \frac{1}{2^\kappa} \]

This follows from iKeyAUTH \( \rightleftharpoons \) iEntAuth \( \land \) Match \( \land \) KMSoundness [dSGFW19, Prop. 9.2.] and from Theorems 2 and 3 and Corollary 3.

Corollary 5 (Full Explicit Key Authentication, cf. Definition 12). The fexKeyAUTH predicate is fulfilled for the air station AS if kem, prf and sig are secure:

\[ \forall \text{adversaries} A : \text{Adv}^{G_{\text{fexKeyAuth}, \Pi, I}}_{A, \Pi, I}(1^\kappa) \leq l^2 \left( \frac{4(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{1 - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})} - n\varepsilon_{\text{sig}} \right) + 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) + 2 \cdot \left( \frac{l^2}{2^\kappa} + l\lambda_{\text{kem}} \right) + \frac{1}{2^\kappa} + n\varepsilon_{\text{sig}} \]

This follows from fexKeyAUTH \( \rightleftharpoons \) fexEntAuth \( \land \) Match \( \land \) KMSoundness [dSGFW19, Prop. 9.2.] and from Theorem 2 and Corollaries 1 and 3.

Corollary 6 (Almost-Full Explicit Key Authentication, cf. Definition 13). The afexKeyAUTH predicate is fulfilled for the ground station GS if kem, prf and sig are secure:

\[ \forall \text{adversaries} A : \text{Adv}^{G_{\text{afexKeyAuth}, \Pi, I}}_{A, \Pi, I}(1^\kappa) \leq l^2 \left( \frac{4(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{1 - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})} - n\varepsilon_{\text{sig}} \right) + 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) + 2 \cdot \left( \frac{l^2}{2^\kappa} + l\lambda_{\text{kem}} \right) + 3l\lambda_{\text{kem}} + \frac{1}{2^\kappa} + n\varepsilon_{\text{sig}} \]

This follows from iKeyAUTH \( \land \) afKeyConf \( \rightleftharpoons \) afexKeyAUTH [dSGFW19, Thm. 3.1.] and from Theorem 6 and Corollary 4.

5 Symbolic Proof

In this section we review the automated proof from the Tamarin implementation of the LDACS MAKE protocol as described in Section 3.

5.1 Transition Model

Figure 5 outlines the flow of the Tamarin code relative to the description of the protocol in Figure 3 as a set of states, rules and protocol messages for each of the agents. Recall that agent A corresponds to the ground station GS and agent B to the air station AS.

The states of the agents are “S_A_i” for \( i \in \mathbb{Z} \) for agent A and “S_B_i” for agent B respectively. The rules, corresponding to the transition between the states of the individual agents (here A) within the protocol, are “init_A”, “A_1”, “A_2”, etc., as well as the queries accessible to the adversary, for example “Reveal_ltk”. Additionally, Figure 5 shows the Protocol messages implied by the rules, as well as the cryptographic messages applied in Figure 3. It may be noted that in the symbolic model the parties first exchange the identifier of the intended partner in plain before engaging in the protocol (in comparison to taking the respective identifier as an input in Figure 3).

Our Tamarin code comprises four implementations of the protocol: First, the expected protocol Figure 3 with the key encapsulation mechanism. Second, the protocol but excluding the generation, transmission and verification of MACs, to verify that all lemmas can be achieved without using the MAC. The third and fourth variant correspond to the
Figure 5: Tamarin rules, states, cryptographic messages and operations for the KEM variant of the protocol. This figure was inspired by [CHSW22b, Fig. 2].

Table 1: Tamarin results for LDACS security notions. Modeled in-/excluding a MAC and using DHKE/KEM as key exchange.

<table>
<thead>
<tr>
<th>Lemma</th>
<th>Scope [-traces]</th>
<th>#Steps w HMAC</th>
<th>#Steps w/o HMAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_exists</td>
<td>Exists</td>
<td>24 ✔ DH, 25 ✔ KEM</td>
<td>23 ✔ DH, 23 ✔ KEM</td>
</tr>
<tr>
<td>two_sessions_exist</td>
<td>Exists</td>
<td>46 ✔ DH, 48 ✔ KEM</td>
<td>44 ✔ DH, 44 ✔ KEM</td>
</tr>
<tr>
<td>mutual_authentication_A/B</td>
<td>All</td>
<td>50 ✔ DH, 54 ✔ KEM</td>
<td>50 ✔ DH, 54 ✔ KEM</td>
</tr>
<tr>
<td>session_uniqueness_A/B</td>
<td>All</td>
<td>32 ✔ DH, 32 ✔ KEM</td>
<td>32 ✔ DH, 32 ✔ KEM</td>
</tr>
<tr>
<td>secrecy</td>
<td>All</td>
<td>32 ✔ DH, 28 ✔ KEM</td>
<td>24 ✔ DH, 26 ✔ KEM</td>
</tr>
<tr>
<td>secrecy_pfs</td>
<td>All</td>
<td>32 ✔ DH, 28 ✔ KEM</td>
<td>24 ✔ DH, 26 ✔ KEM</td>
</tr>
<tr>
<td>key_consistency_A/B</td>
<td>All</td>
<td>16 ✔ DH, 16 ✔ KEM</td>
<td>16 ✔ DH, 16 ✔ KEM</td>
</tr>
</tbody>
</table>

For each variant, Tamarin exhaustively explores the possible actions of the agents and the adversary to check if the lemmas mutual_authentication_A/B, session_uniqueness, secrecy, secrecy_pfs and key_consistency_A/B as described in Section 2.3 are fulfilled. Additionally, the model includes a lemma session_exists and two_sessions_exist, with the first lemma showing the possibility for the Tamarin model to terminate and the second even enhancing the attacker’s abilities by allowing them to reuse cryptographic primitives from the previous protocol run.

5.2 Results

Table 1 shows the results of verifying the lemmas with Tamarin: the “Scope[-traces]” correspond to either the existence of a sequence of traces (“Exists”), or the exhaustive search over all (“All”) possible combinations of traces that achieve the conditions required to fulfill the lemma. The “Steps” indicate the number of rules (see Figure 5) that had to be explored to validate the result.

Table 1 shows that both lemmas, session_exists and two_sessions_exist, have a trace.
guaranteeing the completion of a protocol run and that the lemmas hold even if the adversary re-uses values from previous runs. Further, for all combinations of setups (i.e., with Diffie-Hellman or KEM, with or without MAC) the lemmas are satisfied, thus the protocol fulfills the security claims in the symbolic model. Particularly, the lemmas hold even in the setting with the HMAC removed from the protocol, thus the automated proof confirms the findings of Section 4, verifying that the message authentication code is not required to provide security for LDACS MAKE in the setting of weak corruption.

6 Bibliography

References


Supplementary Material
A1 Computational Security of LDACS MAKE

Proof of Lemma 1, i.e., $\Pr[\text{Sig-Forge}] \leq n \cdot \epsilon_{\text{sig}}$

Proof. Let $\mathcal{I}$ be a set of protocol parties, LSID a set of local sessions and $A$ an adversary that successfully forges one of the signatures in a run of the LDACS MAKE protocol with a non-negligible probability. Then we can construct an equally bounded adversary $B_{\text{sig}}$ from $A$ which wins the EUF-CMA security game for $\text{sig}$ with a non-negligible probability:

The EUF-CMA challenger provides a verification key $vk^* \in \mathcal{V}_{\text{sig}}$ for $B_{\text{sig}}$ and grants $B_{\text{sig}}$ access to a signing oracle $O_{\text{Sign}}(\cdot)$. $B_{\text{sig}}$ then samples a party identifier $id_P \leftarrow \mathcal{I}$. It simulates a regular execution of the LDACS MAKE protocol with adversary $A$, except that the verification key of $P$ is $vk^*$ and $P$ produces signatures via $O_{\text{Sign}}(\cdot)$. If at any point $A$ forges a signature $\sigma' \in S_{\text{sig}}$ by $P$ of a value $x' \in M_{\text{sig}}$ such that the conditions of a Sig-Forge event are satisfied, then $B_{\text{sig}}$ returns $(x', \sigma')$ to the EUF-CMA challenger. If $A$ terminates without successfully forging a signature by $P$, then $B_{\text{sig}}$ aborts by returning $\bot$.

The view of $A$ under $B_{\text{sig}}$ is identical to its view in a regular interaction with the LDACS MAKE protocol with $n$ parties. If $A$ successfully forges a signature for some party, then the probability that $B_{\text{sig}}$ guesses the party correctly is $1/n$. In that case, $B_{\text{sig}}$ returns a valid forgery. This means

$$\frac{1}{n} \cdot \Pr[\text{Sig-Forge}] \leq \text{Adv}^{\text{EUF-CMA}}_{\text{sig}}(B_{\text{sig}}, \kappa) \leq \epsilon_{\text{sig}}$$

and consequently,

$$\Pr[\text{Sig-Forge}] \leq n \cdot \epsilon_{\text{sig}}.$$  \hfill (3)

A1.1 Full Proof of BR-Secrecy

A1.1.1 Simulators

In order to prove BR-secrecy, we need a set of simulators which simulate modified versions of the LDACS MAKE protocol. The proof will contain multiple game hops between different simulators. The first simulator is $S$, which simulates the LDACS MAKE protocol with no visible modifications.

Definition 15 (Simulator $S$). The simulator $S$ has the following parameters: a set $\mathcal{I}$ of protocol parties, a set LSID of local sessions of parties from $\mathcal{I}$, the security parameter $\kappa$ and an adversary $A$. We define $n := |\mathcal{I}|$ and $l := |\text{LSID}|$. At the beginning of its run, $S$ samples $\ell_{GS}, \ell_{AS} \leftarrow \text{LSID}$. Then $S$ simulates a run of the BR-secrecy game with the LDACS MAKE protocol against adversary $A$. Whenever $A$ sends a query, $S$ updates the state of the parties and answers the query in accordance with the definition of the query in the model. When the simulation terminates, $S$ terminates with output $b_{\text{guess}}$.

Remark 3. Sampling $\ell_{GS}$ and $\ell_{AS}$ is only necessary to make sure that a Guess event (cf. Definition 19) is defined under $S$.

The other type of simulator is $\hat{S}$, which has five different variants. We will use $\hat{S}$ in the proof of implicit key authentication.

Definition 16 (Simulator $\hat{S}$). Like $S$, $\hat{S}$ runs on parameters $\mathcal{I}$, LSID, $\kappa$ and $A$. At the beginning of its run, $\hat{S}$ samples $\ell_{GS}, \ell_{AS} \leftarrow \text{LSID}$, $(pk_{kem}, sk_{kem}) \leftarrow \text{Gen}_{\text{kem}}(1^n)$ and $(k, c) \leftarrow \text{Encaps}(pk)$. It also generates the keys $K$ and $k_{\text{mac}}$ as soon as the necessary values for generating them are known. How $K$ and $k_{\text{mac}}$ are generated depends on the
variant of \(\hat{S}\). If at any point during its execution an Abort event as in Definition 18 occurs, \(\hat{S}\) terminates with output 0. Like \(S\), \(\hat{S}\) simulates a run of the BR-secrecy game against adversary \(A\). If \(A\) performs a query on local sessions which do not include \(\ell_{GS}\) or \(\ell_{AS}\), \(\hat{S}\) updates the state of the respective parties and answers the query in accordance with the definition of the query in the model. For \(\ell_{GS}\) and \(\ell_{AS}\), \(\hat{S}\) acts the same except that the values \(pk_{c_{em}}\), \(c\), \(K\) and \(k_{mac}\) are replaced by their counterparts sampled by \(\hat{S}\). Additionally, the Test query output for \(\ell_{GS}\) and \(\ell_{AS}\) is always \(K\). If the simulation terminates, then \(\hat{S}\) terminates with output \(b_{\text{guess}}\).

Definition 17 (\(\hat{S}\) Variants). The \(\hat{S}\) simulator has five variants (corresponding to [CK02, §4.3.2]), which calculate the keys \(K\) and \(k_{mac}\) for \(\ell_{GS}\) and \(\ell_{AS}\) in multiple ways. Let \(k\) be the encapsulated key generated by \(\hat{S}\) and let \(h := H(id_{GS}, id_{AS})\). The five variants calculate \(K\) and \(k_{mac}\) in the following ways:

- \(\hat{S}_{\text{real}}\):
  \[K := \text{prf}(k, (h, 0)), \quad k_{mac} := \text{prf}(k, (h, 1))\]

- \(\hat{S}_{\text{rprf}}\):
  \[K' := \text{prf}(k', (h, 0)), \quad k_{mac} := \text{prf}(k', (h, 1)), \quad k' \leftarrow K_{prf}\]

- \(\hat{S}_{\text{allr}}\):
  \[K \leftarrow Y_{prf}, \quad k_{mac} := \text{prf}(k', (h, 1)), \quad k' \leftarrow K_{prf}\]

- \(\hat{S}_{\text{hybr}}\):
  \[K \leftarrow Y_{prf}, \quad k_{mac} := \text{prf}(k', (h, 1)), \quad k' \leftarrow K_{prf}\]

- \(\hat{S}_{\text{rand}}\):
  \[K \leftarrow Y_{prf}, \quad k_{mac} := \text{prf}(k, (h, 1))\]

A1.1.2 Events

During an execution of the LDACS MAKE protocol or one of the simulators, different events may occur. We will define specific events (extending the work of [CK02, §4.3.2]) which will be important in order to prove the security properties. All of these events can be efficiently detected in an execution of each of the simulators defined above. The first type of events defines when an \(\hat{S}\) simulator aborts its execution.

Definition 18 (Abort Event). An Abort event happens in a run of \(\hat{S}\) if and only if one of the following conditions is satisfied:

- \(A\) terminates before having activated \(\ell_{GS}\) and \(\ell_{AS}\).
- \(\ell_{GS}\) is not an initiator.
- \(\ell_{AS}\) is not a responder.
- \(\ell_{AS}\) receives a message before \(\ell_{GS}\) sent its start message.
- \(\ell_{AS}\) receives a value of \(pk\) different to the respective value sent by \(\ell_{GS}\).
- \(\ell_{GS}\) receives the response message before \(\ell_{AS}\) was activated.
- \(\ell_{GS}\) receives a value of \(c\) different to the respective value sent by \(\ell_{AS}\).
- \(A\) performs more than one Test queries.
- \(A\) terminates without performing a Test query.
- \(\ell_{test} \notin \{\ell_{GS}, \ell_{AS}\}\).
- \(\ell_{test}.\delta_{\text{ownr}} = \text{corrupt}\) or \(\ell_{test}.\delta_{\text{peer}} = \text{corrupt}\).
- \(\ell_{test}\) aborts.
- \(\ell_{GS}.\text{pid} \neq \ell_{AS}.\text{id}\).
Lemma 2. Similar to [CK02, Lem. 7] with kem instead of DDH as suggested by [Pei14]
\[
\forall \text{ adversaries } A \forall E \subseteq \mathcal{E} : |P[E_{\text{real}}] - P[E_{\text{rprf}}]| \leq \varepsilon_{\text{kem}}
\]

Proof. If we assume that a set $\mathcal{I}$ of protocol parties, a set LSID of local sessions and an adversary $A$ exist such that the conjunction of all events in $E$ has different probabilities to occur in $\hat{S}_{\text{real}}$ and in $\hat{S}_{\text{rprf}}$, then we can construct an IND-CPA adversary $D_1$ for kem from $A$:

At the start, $D_1$ receives $pk^* \in \mathcal{P}_{\text{kem}}, c^* \in C_{\text{kem}}$ and $k^* \in K_{\text{kem}}$ from the IND-CPA challenger. $D_1$ then simulates $\hat{S}_{\text{real}}$ with arguments $I$, LSID, $\kappa$ and $A$ with the modification that for $\ell_{\text{GS}}$ and $\ell_{\text{AS}}$, the values $pk_{\text{kem}}, c$ and $k$ are replaced by $pk^*, c^*$ and $k^*$, respectively. If all events in $E$ happen in the modified $\hat{S}_{\text{real}}$ simulator, then $D_1$ terminates with output 1. If the modified $\hat{S}_{\text{real}}$ simulator terminates without all events in $E$ happening, then $D_1$ terminates with output 0. $A$ cannot notice inconsistencies if $\ell_{\text{GS}}$ and $\ell_{\text{AS}}$ have differing views of the values of $pk_{\text{kem}}$ and $c$, since in this case, the modified $\hat{S}_{\text{real}}$ simulator aborts. If $k^*$ is a real encapsulated key, then the view of $A$ under $D_1$ is identical to its view under $\hat{S}_{\text{real}}$. If $k^*$ is a random key, then the view of $A$ under $D_1$ is identical to its view under $\hat{S}_{\text{rprf}}$. This means
\[
|P[E_{\text{real}}] - P[E_{\text{rprf}}]| \leq \text{Adv}_{\text{kem}}^{\text{IND-CPA}}(D_1, \kappa) \leq \varepsilon_{\text{kem}} \tag{4}
\]
Lemma 3. Similar to [CK02, Lem. 15]

\[ \forall \text{ adversaries } A \forall E \subseteq \mathcal{E} : |\mathbb{P}[E_{\text{PRF}}] - \mathbb{P}[E_{\text{ALLR}}]| \leq \varepsilon_{\text{prf}} \]

Proof. If we assume that a set \( \mathcal{I} \) of protocol parties, a set LSID of local sessions and an adversary \( A \) exist such that the conjunction of all events in \( E \) has different probabilities to occur in \( S_{\text{PRF}} \) and in \( S_{\text{ALLR}} \), then we can construct a PRF adversary \( D_2 \) for \( \text{prf}(\cdot, \cdot) \) from \( A \).

At the start, the \( \text{prf} \) challenger grants \( D_2 \) access to an oracle \( O_{\text{prf}/rpf}(\cdot) \) which implements \( \text{prf}(k^*, \cdot) \) for a uniformly sampled key \( k^* \in K_{\text{prf}} \) or which implements a random function \( \text{rf} : X_{\text{prf}} \rightarrow Y_{\text{prf}} \). \( D_2 \) then simulates a modified version of \( S_{\text{PRF}} \) which uses \( O_{\text{prf}/rpf}(\cdot) \) instead of \( \text{prf}(k', \cdot) \). This means that \( \ell_{\text{GS}} \) and \( \ell_{\text{AS}} \) use session key \( K := O_{\text{prf}/rpf}(\mathcal{H}(\text{id}_{\text{GS}}, \text{id}_{\text{AS}}), 0) \) and MAC key \( k_{\text{mac}} := O_{\text{prf}/rpf}(\mathcal{H}(\text{id}_{\text{GS}}, \text{id}_{\text{AS}}), 1) \). If all events in \( E \) happen in the modified \( S_{\text{PRF}} \) simulator, then \( D_2 \) terminates with output 1. If the modified \( S_{\text{PRF}} \) simulator terminates without all events in \( E \) happening, then \( D_2 \) terminates with output 0. If \( O_{\text{prf}/rpf}(\cdot) = \text{prf}(k^*, \cdot) \), then the view of \( A \) under \( D_2 \) is identical to its view under \( S_{\text{PRF}} \). If \( O_{\text{prf}/rpf}(\cdot) \) implements \( \text{rf}(\cdot) \), then the view of \( A \) under \( D_2 \) is identical to the view under \( S_{\text{ALLR}} \). This means

\[ |\mathbb{P}[E_{\text{PRF}}] - \mathbb{P}[E_{\text{ALLR}}]| \leq \text{Adv}_{\text{prf}}^{\text{PRF}}(D_2, \kappa) \leq \varepsilon_{\text{prf}} \] (5)

Lemma 4. Similar to [CK02, Lem. 15]

\[ \forall \text{ adversaries } A \forall E \subseteq \mathcal{E} : |\mathbb{P}[E_{\text{ALLR}}] - \mathbb{P}[E_{\text{IVYR}}]| \leq \varepsilon_{\text{prf}} \]

Proof. If we assume that a set \( \mathcal{I} \) of protocol parties, a set LSID of local sessions and an adversary \( A \) exist such that the conjunction of all events in \( E \) has different probabilities to occur in \( S_{\text{ALLR}} \) and in \( S_{\text{IVYR}} \), then we can construct a PRF adversary \( D_3 \) for \( \text{prf} \) from \( A \), similar to how we constructed \( D_2 \) in the proof of Lemma 3. The difference is that \( D_3 \) uses \( S_{\text{IVYR}} \) instead of \( S_{\text{PRF}} \). This means effectively that the only difference between \( D_3 \) and \( D_2 \) is that \( D_3 \) uniformly and independently samples \( K \) instead of generating it via \( O_{\text{prf}/rpf}(\mathcal{H}(\text{id}_{\text{GS}}, \text{id}_{\text{AS}}), 0) \). Accordingly, if \( O_{\text{prf}/rpf}(\cdot) = \text{prf}(k^*, \cdot) \), then the view of \( A \) under \( D_3 \) is identical to the view under \( S_{\text{IVYR}} \) instead of \( S_{\text{PRF}} \). The inequality we can deduce for this lemma is the following:

\[ |\mathbb{P}[E_{\text{ALLR}}] - \mathbb{P}[E_{\text{IVYR}}]| \leq \text{Adv}_{\text{prf}}^{\text{PRF}}(D_3, \kappa) \leq \varepsilon_{\text{prf}} \] (6)

Lemma 5. Similar to [CK02, Lem. 8,15] with kem instead of DDH as suggested by [Pei14]

\[ \forall \text{ adversaries } A \forall E \subseteq \mathcal{E} : |\mathbb{P}[E_{\text{IVYR}}] - \mathbb{P}[E_{\text{RAND}}]| \leq \varepsilon_{\text{kem}} \]

Proof. If we assume that a set \( \mathcal{I} \) of protocol parties, a set LSID of local sessions and an adversary \( A \) exist such that the conjunction of all events in \( E \) has different probabilities to occur in \( S_{\text{IVYR}} \) and in \( S_{\text{RAND}} \), then we can construct an IND-CPA adversary \( D_4 \) for \( \text{kem} \) from \( A \), similar to how we constructed \( D_1 \) in the proof of Lemma 2. The difference is that \( D_4 \) uses \( S_{\text{RAND}} \) instead of \( S_{\text{REAL}} \). This means effectively that the only difference between \( D_4 \) and \( D_1 \) is that \( D_4 \) samples \( K \) independently instead of generating it via \( \text{prf}(k^*, (\mathcal{H}(\text{id}_{\text{GS}}, \text{id}_{\text{AS}}), 0)) \). Accordingly, depending on whether \( k^* \) is real or random, the view of \( A \) under \( D_4 \) is identical to the view under \( S_{\text{RAND}} \) or \( S_{\text{IVYR}} \) instead of \( S_{\text{REAL}} \) or \( S_{\text{PRF}} \), respectively. The inequality we can deduce for this lemma is the following:

\[ |\mathbb{P}[E_{\text{IVYR}}] - \mathbb{P}[E_{\text{RAND}}]| \leq \text{Adv}_{\text{kem}}^{\text{IND-CPA}}(D_4, \kappa) \leq \varepsilon_{\text{kem}} \] (7)


With the next lemma, we show that \( \hat{S}_{\text{REAL}} \) only aborts with a negligible probability if a \textsc{Guess} event happens. We need this because when comparing a regular execution of the LDACS MAKE protocol with \( \hat{S} \), we rely on \( \hat{S} \) not aborting under certain circumstances.

**Lemma 6.** Similar to [CK02, Lem. 7]

\[
\forall \text{ adversaries } A : \mathbb{P}[\text{ABORT}_{\text{REAL}} \land \text{GUESS}_{\text{REAL}}] = 0
\]

*Proof.* Consider a run of \( \hat{S}_{\text{REAL}} \). Assume that a \textsc{Guess} event happens. By the definition of a \textsc{Guess} event (cf. Definition 19), \( A \) has activated \( \ell_{GS} \) and \( \ell_{AS} \). \( \ell_{GS} \) is an initiator, \( \ell_{AS} \) a responder, \( \ell_{GS,ecid} = \ell_{AS,ecid} \). \( A \) performs exactly one \textsc{Test} query and \( \ell_{\text{test}} \in \{\ell_{GS}, \ell_{AS}\} \).

Consider a fixed point in time before which an \textsc{Abort} event has not happened. \( \hat{S}_{\text{REAL}} \) behaves identically to a regular interaction with the LDACS MAKE protocol where the response to the \textsc{Test} query is the real session key. We can assume without loss of generality that after the next adversary query, \( \ell_{\text{test}}, \delta_{\text{owner}} = \ell_{\text{test}}, \delta_{\text{peer}} = \text{honest} \land \ell_{\text{test}}, \delta_{\text{sess}} = \text{fresh} \land (\forall \ell' \in \text{LSID}, \ell'.\text{sid} = \ell_{\text{test}}, \text{sid} : \ell'.\delta_{\text{sess}} = \text{fresh}) \land (\ell_{\text{test}} \text{ accepts}) \) will still hold, since otherwise \( A \) would lose the BR-secrecy game in a regular interaction with the LDACS MAKE protocol. Since \( \ell_{GS,ecid} = \ell_{AS,ecid} \), it must be the case that either \( \ell_{GS,\text{sid}} = \ell_{AS,\text{sid}} \) or only \( \ell_{\text{test}} \) accepts and the other local session does not. In both cases, \( A \) neither reveals \( \ell_{GS} \) nor \( \ell_{AS} \). That both \( \ell_{GS} \) and \( \ell_{AS} \) have the same ECID also means that they have the same view of the values of \( \text{id}_{GS}, \text{id}_{AS}, \text{pk}_{\text{kem}} \), and \( c \).

The above points mean that, if a \textsc{Guess} event has already happened, the next adversary query cannot trigger an \textsc{Abort} event. On the other hand, when an \textsc{Abort} event happens, \( \hat{S}_{\text{REAL}} \) aborts its execution, meaning that a \textsc{Guess} event cannot happen after an \textsc{Abort} event. Thus, both an \textsc{Abort} and a \textsc{Guess} event cannot happen in the same execution of \( \hat{S}_{\text{REAL}} \).

**Lemma 7.** Similar to [CK02, Lem. 11]

\[
\forall \text{ adversaries } A \forall \ell \in \text{LSID} \exists \ell' \in \text{LSID} : \\
(\ell \text{ accepts } \land \ell.\delta_{\text{peer}} = \text{honest} \Rightarrow \mathbb{P}[\neg \text{SAMEECID}(\ell, \ell')] \leq n \cdot \varepsilon_{\text{sig}})
\]

*Proof.* Let \( \ell \in \text{LSID} \) be any local session with \( \ell.\text{accept} = \text{true} \) and \( \ell.\delta_{\text{peer}} = \text{honest} \). Since \( \ell \) accepts, it has received a valid signature of \( \text{pk}_{\text{kem}}, c \) and \( \ell.\text{id} \) by its intended partner. If the intended partner did not create the signature, then \( A \) forged it. By Lemma 1, the probability for this event is at most \( n \cdot \varepsilon_{\text{sig}} \). If the intended partner created the signature, then a local session \( \ell' \in \text{LSID} \) exists which has the same view of the values of \( \text{id}_{GS}, \text{id}_{AS}, \text{pk}_{\text{kem}} \), and \( c \). In this case, \( \ell'.\text{ecid} = \ell.\text{ecid} \). In total, the probability that no local session \( \ell' \in \text{LSID} \) exists with the same ECID is at most \( n \cdot \varepsilon_{\text{sig}} \).

In the following lemma, we establish a noticeable lower bound for the probability of a \textsc{Guess} event. Because of this, we know that negligible probabilities do not become non-negligible when we introduce the condition that a \textsc{Guess} event occurred.

**Lemma 8.** Similar to [CK02, Lem. 9]

\[
\forall \text{ adversaries } A : \mathbb{P}[\text{GUESS}_{\text{REAL}}] \geq \frac{1}{12} - n\varepsilon_{\text{sig}}
\]

*Proof.* We assume without loss of generality that in a regular interaction with the LDACS MAKE protocol, \( A \) chooses exactly one test session \( \ell_{\text{test}} \) and that \( A \) does not corrupt \( \ell_{\text{test}} \) or its intended partner before \( \ell_{\text{test}} \) accepts. This also applies to a simulation of \( A \) under simulator \( \hat{S} \). By Lemma 7, a local session \( \ell' \in \text{LSID} \) exists with \( \ell'.\text{ecid} = \ell_{\text{test}},\text{ecid} \) with a probability of at least \( 1 - n\varepsilon_{\text{sig}} \). If such a local session exists, then the probability
that under simulator $S$, $\ell_{GS}$ is an initiator, $\ell_{AS}$ is a responder and $\ell_{test} \in \{\ell_{GS}, \ell_{AS}\}$, is at least $1/l^2$. In total, the probability of a GUESS event under $S$ is at least

$$\frac{1}{l^2} - n\varepsilon_{sig}.$$ 

Let $\hat{S}_{\text{real}}'$ be a simulator that exactly acts like $\hat{S}_{\text{real}}$ except that it never aborts. Since $A$ has to choose $\ell_{test}$ before it knows the response to the Test query, $A$’s choice of $\ell_{test}$ has the same distribution under $S$ and under $\hat{S}_{\text{real}}'$. Therefore, a GUESS event has the same probability under $S$ and under $\hat{S}_{\text{real}}'$. By Lemma 6 it is not possible that both an ABORT event and a GUESS event happen under $\hat{S}_{\text{real}}$. This also means that the probabilities of a GUESS event under $\hat{S}_{\text{real}}'$ and under $\hat{S}_{\text{real}}$ are identical. We can now deduce:

$$P[\text{GUESS}_{\text{real}}] = P[\text{GUESS under } \hat{S}_{\text{real}}'] = P[\text{GUESS under } S] = \frac{1}{l^2} - n\varepsilon_{sig}.$$ 

With the last two lemmas, we show the connection between $\hat{S}$ and a regular execution of the LDACS MAKE protocol. The first of the two lemmas states that $\hat{S}_{\text{real}}$ with a GUESS event is indistinguishable from a regular interaction with a real session key as a response to the Test query.

**Lemma 9.** Similar to [CK02, Lem. 14]

$$\forall \text{ adversaries } A : |P_{\text{real}}(A) - P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}]| = 0$$

**Proof.** By Lemmas 6 and 8, we know that

$$P[\text{ABORT}_{\text{real}} \land \text{GUESS}_{\text{real}}] = 0 \quad \text{and} \quad P[\text{GUESS}_{\text{real}}] \geq \frac{1}{l^2} - n\varepsilon_{sig}.$$ 

The view of $A$ under $\hat{S}_{\text{real}}$ given a GUESS event is the same as in a regular interaction with the LDACS MAKE protocol with real Test query output unless an ABORT event happens. This means that

$$|P_{\text{real}}(A) - P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}]| \leq P[\text{ABORT}_{\text{real}}|\text{GUESS}_{\text{real}}] = \frac{P[\text{ABORT}_{\text{real}} \land \text{GUESS}_{\text{real}}]}{P[\text{GUESS}_{\text{real}}]} \leq \frac{0}{\frac{1}{l^2} - n\varepsilon_{sig}} = 0.$$
The last lemma states that $S_{\text{rand}}$ with a GUESS event is indistinguishable from a regular interaction with a random value as a response to the TEST query.

**Lemma 10.** Similar to [CK02, Lem. 13] The following holds true:

$$
\forall \text{adversaries } A:\n\left| P_{\text{rand}}(A) - P[\text{AFFIRM}_{\text{rand}}|\text{GUESS}_{\text{rand}}]\right| \leq \frac{2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{1 - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) - n\varepsilon_{\text{sig}}}. \quad (15)
$$

**Proof.** Analogous to Lemma 9, using Lemmas 2 to 5 to argue that

$$
P[\text{ABORT}_{\text{rand}} \land \text{GUESS}_{\text{rand}}] \leq 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) \quad (16)
$$

$$
P[\text{GUESS}_{\text{rand}}] \geq \frac{1}{1 - 2\varepsilon_{\text{kem}} - 2\varepsilon_{\text{prf}} - n\varepsilon_{\text{sig}}} \quad (17)
$$

follows from

$$
P[\text{ABORT}_{\text{real}} \land \text{GUESS}_{\text{real}}] = 0
$$

$$
P[\text{GUESS}_{\text{real}}] \geq \frac{1}{1 - 2\varepsilon_{\text{kem}} - 2\varepsilon_{\text{prf}} - n\varepsilon_{\text{sig}}}
$$

Finalizing the Proof of BR-Secrecy, Theorem 7  Finally, we combine all lemmas to show that in a regular execution of the LDACS MAKE, the key of a session is indistinguishable from an independently sampled random value.

**Proof.** By Lemmas 2 to 5,

$$
\left| P[\text{AFFIRM}_{\text{real}} \land \text{GUESS}_{\text{real}}] - P[\text{AFFIRM}_{\text{rand}} \land \text{GUESS}_{\text{rand}}]\right| \leq 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})
$$

$$
\left| P[\text{GUESS}_{\text{real}}] - P[\text{GUESS}_{\text{rand}}]\right| \leq 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}).
$$

By Lemma 8,

$$
P[\text{GUESS}_{\text{real}}] \geq \frac{1}{1 - 2\varepsilon_{\text{kem}} - 2\varepsilon_{\text{prf}} - n\varepsilon_{\text{sig}}}
$$

By Lemma 9,

$$
|P_{\text{real}}(A) - P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}]| = 0.
$$

By Lemma 10,

$$
|P_{\text{rand}}(A) - P[\text{AFFIRM}_{\text{rand}}|\text{GUESS}_{\text{rand}}]| \leq \frac{2(\varepsilon_{\text{kem}} + 2\varepsilon_{\text{prf}})}{1 - 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) - n\varepsilon_{\text{sig}}}
$$

Let

$$
\nu := |P_{\text{real}}(A) - P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}]| + |P_{\text{rand}}(A) - P[\text{AFFIRM}_{\text{rand}}|\text{GUESS}_{\text{rand}}]|.
$$
We can now deduce:

\[
\begin{align*}
&|P_{\text{real}}(A) - P_{\text{rand}}(A)| \\
&= |P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}] - P[\text{AFFIRM}_{\text{rand}}|\text{GUESS}_{\text{rand}}] \\
&\quad + (P_{\text{real}}(A) - P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}]) \\
&\quad - (P_{\text{rand}}(A) - P[\text{AFFIRM}_{\text{rand}}|\text{GUESS}_{\text{rand}}])| \quad (18) \\
&\leq |P[\text{AFFIRM}_{\text{real}}|\text{GUESS}_{\text{real}}] - P[\text{AFFIRM}_{\text{rand}}|\text{GUESS}_{\text{rand}}]| + \nu \quad (19) \\
&= |P[\text{AFFIRM}_{\text{real}} \land \text{GUESS}_{\text{real}}] - P[\text{AFFIRM}_{\text{rand}} \land \text{GUESS}_{\text{rand}}]| + \nu \quad (20) \\
&= P[\text{GUESS}_{\text{real}}]^{-1} \cdot |P[\text{AFFIRM}_{\text{real}} \land \text{GUESS}_{\text{real}}] \\
&\quad - \frac{P[\text{GUESS}_{\text{real}}]}{P[\text{GUESS}_{\text{rand}}]} \cdot |P[\text{AFFIRM}_{\text{rand}} \land \text{GUESS}_{\text{rand}}]| + \nu \quad (21) \\
&\leq |P[\text{AFFIRM}_{\text{real}} \land \text{GUESS}_{\text{real}}] - P[\text{AFFIRM}_{\text{rand}} \land \text{GUESS}_{\text{rand}}]| \\
&\quad + |P[\text{GUESS}_{\text{real}}] - P[\text{GUESS}_{\text{rand}}]| \cdot |P[\text{AFFIRM}_{\text{rand}} \land \text{GUESS}_{\text{rand}}]| + \nu \quad (23) \\
&\leq P[\text{GUESS}_{\text{real}}]^{-1} \cdot |P[\text{AFFIRM}_{\text{real}} \land \text{GUESS}_{\text{real}}] - P[\text{AFFIRM}_{\text{rand}} \land \text{GUESS}_{\text{rand}}]| \\
&\quad + |P[\text{GUESS}_{\text{real}}] - P[\text{GUESS}_{\text{rand}}]| + \nu \quad (24) \\
&\leq \frac{1}{\tau} \cdot 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) \\
&\quad + |P[\text{GUESS}_{\text{real}}] - P[\text{GUESS}_{\text{rand}}]| \cdot 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) \quad (25) \\
&\leq \frac{4(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}})}{\tau} + 2(\varepsilon_{\text{kem}} + \varepsilon_{\text{prf}}) \quad (26)
\end{align*}
\]