Peltonen, Aleksi; Sasse, Ralf; Basin, David

A Comprehensive Formal Analysis of 5G Handover

Published in:
WiSec 2021 - Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks

DOI:
10.1145/3448300.3467823

Published: 21/06/2021

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Peltonen, A., Sasse, R., & Basin, D. (2021). A Comprehensive Formal Analysis of 5G Handover. In *WiSec 2021 - Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 1-12). Article 3467823 ACM. https://doi.org/10.1145/3448300.3467823

A Comprehensive Formal Analysis of 5G Handover

Aleksi Peltonen
Department of Computer Science
Aalto University
Espoo, Finland
aleksi.peltonen@aalto.fi

Ralf Sasse
Department of Computer Science
ETH Zurich
Zurich, Switzerland
ralf.sasse@inf.ethz.ch

David Basin
Department of Computer Science
ETH Zurich
Zurich, Switzerland
basin@inf.ethz.ch

ABSTRACT

5G has been under standardization for over a decade and will drive the world's mobile technologies in the decades to come. One of the cornerstones of the 5G standard is its security, also for devices that move frequently between networks, such as autonomous vehicles, and must therefore be handed over from one network operator to another. We present a novel, comprehensive, formal analysis of the security of the device handover protocols specified in the 5G standard. Our analysis covers both handovers within the 5G core network, as well as fallback methods for backwards compatibility with 4G/LTE. We identify four main handover protocols and formally model them in the security protocol verification tool Tamarin. Using these models, we determine for each protocol the minimal set of security assumptions required for its intended security goals to be met. Understanding these requirements is essential when designing devices and other protocols that depend on the reliability and security of network handovers.

CCS CONCEPTS

• **Networks** → **Protocol testing and verification**; **Mobile networks**.

KEYWORDS

5G, handover protocols, protocol verification, formal analysis

ACM Reference Format:
Aleksi Peltonen, Ralf Sasse, and David Basin. 2021. A Comprehensive Formal Analysis of 5G Handover. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28–July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3448300.3467823

1 INTRODUCTION

In the year 2020, the number of mobile subscriptions grew to almost 8 billion worldwide. More than half of these still rely on the Long-Term Evolution (LTE) mobile access technology, standardized by the 3rd Generation Partnership Project (3GPP) over a decade ago [18]. To keep up with the growing user base, the 3GPP has been standardizing the next generation of mobile technologies, commonly known as 5G. This technology is intended to provide fast, reliable, and secure device mobility across different networks and technologies.

WiSec '21, June 28–July 2, 2021, Abu Dhabi, United Arab Emirates

Many of the anticipated use cases for 5G, like autonomous vehicles and IoT devices [17, 24], require reliable connections with low latencies, even when the devices are moving at high speeds. In practice, this means that not only must the serving network provide fast and reliable connectivity, but also that switching between different networks must be seamless and not break any ongoing data connections. This includes both moving between different base stations within the 5G Core Network (5GC), as well as connecting to networks implementing older standards, such as LTE.

Transferring an ongoing connection from one network (or base station) to another is commonly called a *handover* in mobile communication. Handovers in cellular networks can further be divided into intra- and inter-system handovers. An intra-system handover is performed when the source and the target network share a common Radio Access Technology (RAT), i.e., when they implement the same network standard, such as 5G. In contrast, an inter-system handover is required when the networks implement different standards, such as when switching from a 5G to an LTE network or vice versa. In this paper, we use formal methods to model and analyze the security of both intra- and inter-system handovers in 5G. Since the interaction between 5G and networks implementing standards older than LTE is currently not supported [6], we limit our analysis of fallback methods to LTE.

Contributions. Our main contributions are as follows. First, the 5G standard has considerable complexity and is divided over a large number of documents. For both intra- and inter-system handovers we extract and concisely summarize from the relevant standardization documents the handover protocols, their security objectives, and stated assumptions on the operating environment. Second, we formally model both intra- and inter-system handovers specified in the 5G standard. This necessitates developing appropriate abstractions to reflect those security-relevant parts of the protocol. Finally, we carry out a comprehensive security analysis of our models. A particularly novel aspect of our work is a detailed analysis of which combinations of environmental assumptions are required for security. We expand on these points below.

Formalization and formal modeling of 5G handover protocols. From Release 16 [7] of the 3GPP specification set for 5G, we identify nine documents, running over 2,600 pages, that describe the overall architecture, terminology, security requirements, radio technologies, and procedures related to handovers. From these specifications, we identify four handover protocols that cover the most common cases for both intra- and inter-system transitions. We infer security goals from the goals stated for other protocols in the 5G infrastructure, when these are not explicitly given. Furthermore, we explicate the assumptions that the rest of the 5G ecosystem must fulfill for handovers to work as expected.

For inter-5G handovers, the 5G specification includes abstracted versions of the protocols [6], in which messages and parameters that are irrelevant to the functionality or security of handovers are excluded. As part of our modeling, we perform similar abstractions for the intra-5G handovers. Abstracted values include, most notably, configuration parameters and other values provisioned for later use by other protocols within the 5G standard. As we work in the symbolic model of cryptography, we also omit physical layer details, such as the radio frequencies used, etc. We summarize the message flows of the different protocols as easily readable message sequence diagrams and formally model them. We use a state-of-the-art protocol verification tool, the Tamarin prover [23, 27], to model the protocols.

Security evaluation. Using our models and Tamarin, we prove for each protocol that the security goals suggested by the standard hold. As we analyze the security of all protocols within the 5G infrastructure, this includes identifying security requirements for all entities participating in handovers, as well as the requirements for secure communication within the 5G Core Network. Based on our analyses, we present the dependencies and relationships between different keys and identifiers, and identify a minimal set of data for each model that must remain secret for the security goals to hold. These results clearly delimit which data and keys stay secret even in the case of a partial compromise of the associated infrastructure, and what is leaked in such a situation.

Our work provides a precise, concise, and abstract documentation of the main 5G handover protocols, their properties, and assumptions, as well as their formal specification and analysis. These results both provide the 5G community with formal arguments for the security of 5G handover and precise results on *when* they are secure, i.e., under what assumptions. Our work can therefore be seen as being part of a larger program to provide formal proofs of security for all relevant, safety-critical aspects of 5G [9, 12], which is a major undertaking, but commensurate with the importance of this standard.

Related work. The security of handover protocols in cellular networks has been analyzed and formally modeled for previous generations of 3GPP standards. Most recently, both intra- and inter-system handovers in LTE networks were analyzed using the ProVerif verification tool [11, 20]. Similarly to our work on 5G, they verify secrecy and authentication properties of the standard. However, despite the security of handovers in LTE networks, various studies [15, 21, 25] have shown the practical limitations of these handovers and expressed a need for faster, more reliable handover protocols in future standards. Since the 5G specification is still under development and has not yet been widely deployed for commercial use, there have not yet been many studies done for handovers in 5G. To the best of our knowledge, our work is the first that rigorously analyzes the security of 5G handovers using formal methods.

In contrast to the security of 5G handovers, other parts of the specification have been formally modeled and analyzed. For example, [9] and [12] analyze the 5G Authentication and Key Agreement (5G AKA) protocol using Tamarin. Both studies identify weaknesses in earlier versions of the standard and suggest improvements that have partially been adopted in later releases. For this reason, we believe it is also important to formally model and verify other critical parts of the standard, including handovers, which are the focus of this paper. Furthermore, we use the results from the models presented in other studies, [9] in particular, as a starting point for our analyses, extending the coverage of their results and the set of formally verified protocols of the 5G standard.

Attack finding techniques have been applied to other parts of 5G, but not to handovers. Such techniques, in general, do not provide correctness guarantees. In contrast, our approach is sound and complete, and thus can guarantee the absence of attacks with respect to the model.

Outline. The rest of the paper is structured as follows. In Section 2, we describe 5G handovers and explain the different protocol variations. In Section 3, we explain the security assumptions and requirements for these protocols. In Section 4, we present our formal models of the handovers and our results. Finally, in Section 5, we draw conclusions.

2 5G HANDOVER PROTOCOLS

In cellular networks, handovers are used to transfer an ongoing call or data connection between networks. In this section, we describe how intra-system handovers work in 5G, i.e., how a device is handed over from a source to a target network when they both implement the 5G standard. We describe the two protocols that are defined for intra-5G handovers and their major differences. We also describe the abstractions we found helpful for modeling and analyzing these protocols. Finally, we briefly cover inter-5G handovers.

The analyses and models are based on the specification set from the Stage 3 freeze of Release 16 [7] ("5G phase 2"), completed in July 2020. The main references are TS 23.501 [8], TS 23.502 [5], TS 33.501 [6], TS 38.300 [4], TS 23.401 [2], TS 33.220 [3], and TS 33.401 [1], henceforth referred to as [TS 23.501], [TS 23.502], [TS 33.501], [TS 38.300], [TS 23.401], [TS 33.220], and [TS 33.401].

2.1 Protocol Overview

In 5G networks, an intra-system handover is used to transfer a User Equipment (UE), such as a mobile phone, from one Radio Access Network (RAN) to another. A handover may be required for reasons including load balancing, changed radio conditions, or user movement [TS 23.502, Sec. 4.9.1.1]. In other words, when a UE's current network is no longer capable of serving it, or when a more suitable network is discovered, the serving network will trigger the process of handing over the device. This can occur, for example, when the user is moving, or when many devices are simultaneously connected to the same network.

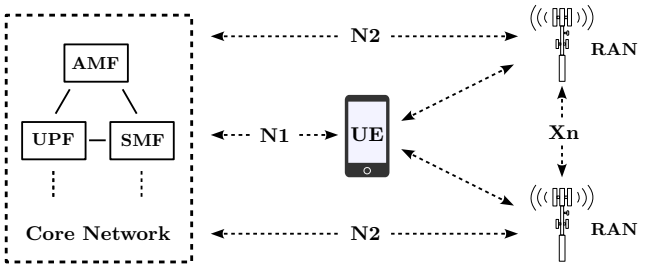

Figure 1: Overview of the 5G architecture and network interfaces, simplified.

The 5G architecture, described in [TS 23.501, Sec. 4.2], is a service-based architecture that consists of many Network Functions (NFs), such as the Access and Mobility Management Function (AMF), the Session Management Function (SMF), and the User Plane Function (UPF). The AMF is responsible for access authentication and authorization. Since outside entities, such as UEs and RANs, are not part of the core network architecture, they do not interact directly with most of the individual functions. Instead, they connect to the 5G Core Network (5GC) over secure network interfaces, such as the N1 and N2 interfaces provided by the AMF (see Figure 1).

Interaction between different Radio Access Networks can be direct or indirect, depending on the available network interfaces. When an intra-5G handover is required, the source network can choose to initiate one of two versions of the protocol: the Xn- or the N2-based variation. In an Xn-based handover, messages between the two networks are sent directly over the Xn interface, which reduces the number of messages sent to the core network. In contrast, in the N2 variation there is no direct connectivity between the two RANs. Messages are instead delivered indirectly through the 5GC using the N2 interface between the RANs and the AMF, as shown in Figure 1. Although the two variations have some notable differences, which will be explained later, the 5G specification presents them as equal alternatives, without recommending either one.

For our analyses and formal models, we create minimal versions of the protocols by abstracting away those parts that do not affect the security properties. Our main abstraction with regards to the overall architecture is to group together all the core network functions used in the protocol into one entity, the "Core Network (CN)." This is a reasonable abstraction since, according to [TS 33.501, Sec. 5.9.3], the internal communication of the core network provides confidentiality, integrity, authenticity, and replay protection. Without this abstraction, modeling and analyzing the internal messages of the 5GC would create an unnecessary overhead since we assume that it cannot be compromised. Hence, the attacker cannot learn or alter any messages sent within the core network. Similarly, we also combine the Universal Subscriber Identity Module (USIM) and the Mobile Equipment (ME) into one entity, the "User Equipment (UE)." We refer to these entities throughout this paper and in our formal models.

2.2 Initial Setup

Prior to a handover, the following (symmetric) long-term keys have been negotiated: *i)* K_{SEAF}, an anchor key derived by the UE and the CN; *ii)* K_{AMF}, a long-term key derived from K_{SEAF} by the UE and the CN; *iii)* K_{gNB}, a session key derived by the UE and the source RAN (SRAN); and *iv) NH*, an intermediate key (and its associated counter, NCC) derived by the UE and the SRAN.

In addition, all participating entities may have information obtained from their previous exchanges, including keys derived during the initial setup or keys re-derived from preceding handovers. This means that the CN, the SRAN, and the UE all share the necessary parameters and keys required for secure communication and for future re-keying. The target RAN (TRAN), however, need not have any previous knowledge of the UE or share keys with the other participants, as long as it is securely connected to the core network.

Intra-5G handovers always include re-keying of the session key K_{gNB}, either from the key itself (horizontal key derivation) or from the intermediate NH parameter (vertical key derivation). The main difference between these options is that forward security (see Section 3.2) is only provided by vertical key derivation. In both variations, the newly derived intermediate session key, K_{gNB^*} becomes the new session key after the handover is completed. The protocol may also re-derive K_{AMF} if the allocated AMF changes during the handover or when the current AMF updates its key.

2.3 Xn-based Intra-5G Handovers

The Xn network interface securely connects two Radio Access Networks. It provides integrity, confidentiality, and replay protection for the communication between them [TS 33.501, Sec. 9.4]. The interface can be used for message delivery during inter-RAN handovers, in which the core network and its AMF remain unchanged. The 5G specification defines six variations of the Xn-based handover, differing in which network functions are re-allocated or removed. However, since the differences between the variations all take place within the core network, we do not model or analyze them separately, as explained in Section 2.1.

Each Xn-based handover consists of three parts:

(1) *Handover Preparation.* The source network (SRAN) requests to transfer a UE to a target network (TRAN), and provides it with a newly derived session key to be used with the UE. If the TRAN is capable and willing to accept the UE, it responds with an acknowledgment message [TS 38.300, Sec. 9.2.3.2.1].
(2) *Handover Execution.* The UE exchanges parameters with both RANs and derives the session key sent to the TRAN in Step 1 [TS 38.300, Sec. 9.2.3.2.1].
(3) *Handover Completion.* The TRAN and the CN agree on session identifiers and temporary keys. Finally, the CN informs the SRAN that all resources related to the UE can be released [TS 23.502, Sec. 4.9.1.2].

In addition to these parts, there is also a conditionally executed Mobility Registration Update (MRU) [TS 23.502, Sec. 4.2.2.2.2] that may occur after the handover is finished. During the MRU, the UE and the TRAN exchange and update additional parameters, notably the 5G Globally Unique Temporary Identifier (5G-GUTI). However, since the AMF remains unchanged, only a subset of the full MRU needs to be completed. It is included in our Tamarin model.

Figure 2 shows the protocol's message flow. As discussed previously, besides the messages included in the figure, other parameters are updated and exchanged during the procedure. However, we abstract these away, since they do not affect the handover's functionality or security. Details of the full protocol can be found in [TS 23.502] and [TS 38.300].

2.4 N2-based Intra-5G Handovers

The N2 network interface connects RANs with the core network's AMF. Similarly to the Xn interface, it also provides integrity, confidentiality, and replay protection [TS 33.501, Sec. 9.2]. When using the N2 interface for a handover, the two RANs do not communicate directly as they do in the Xn-based variation. Instead, all messages are routed through the 5GC or the UE (see Figure 1). An N2-based handover can be used when there is no direct connectivity between

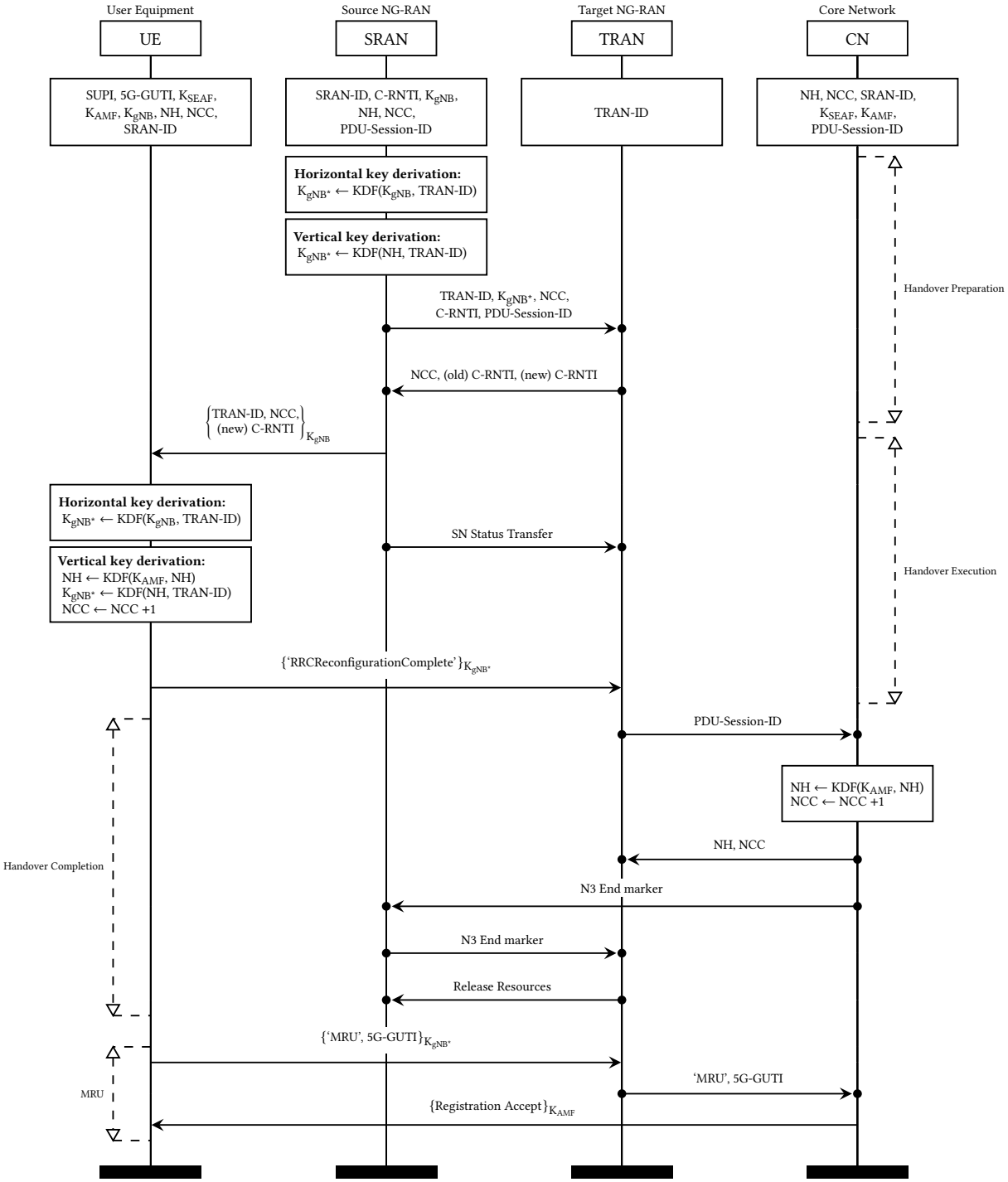

Figure 2: Xn-based intra-5G handover. The symbol • means that a channel is secure (provides integrity, confidentiality, and replay protection). Symmetric encryption with a key K is denoted $\{\}_K$.

the source and the target network, or when a previously attempted Xn-based handover has failed. Furthermore, unlike the other variation, it can also include an AMF change in the core network, which transfers the UE's security capabilities to a new AMF.

An N2-based handover consists of two parts and a mandatory Mobility Registration Update, which unlike in the Xn-based variation, is performed during the handover. Since there is no direct connectivity between the SRAN and the TRAN, more messages are exchanged. The sequence diagram of the protocol messages is shown in Figure 5 in Appendix B, with abstractions similar to those made in the Xn model. The two parts of the handover are:

(1) *The Preparation Phase.* Similarly to the handover preparation in the Xn-based handover, the SRAN and the TRAN negotiate the handover of a UE. However, as mentioned before, all messages are routed through the CN, rather than sent directly between the networks. The CN internally decides whether the currently allocated AMF must be changed and prepares to update session values as needed [TS 23.502, Sec. 4.9.1.3.2].
(2) *The Execution Phase.* The UE and the RANs exchange session values and re-key K_{AMF} if needed. Finally, the CN informs the SRAN that all resources related to the UE can be released [TS 23.502, Sec. 4.9.1.3.3].

2.5 Inter-5G Handovers

The first complete set of 5G standards was published as Release 15 in 2018. In 2020, the first major update, Release 16, was completed. So far, relatively few commercial implementations have been introduced to the market, but the situation is slowly changing. The number of 5G subscriptions grew to roughly 220 million in the year 2020 [19] and is estimated and reach 2.8 billion within the next five years. However, LTE is still predicted to be the dominant mobile technology for the foreseeable future, peaking at 5.1 billion subscribers in 2022 [18]. Hence, the 5G specification must allow for ongoing connections to be transferred to a network implementing an older technology, especially in the early stages of adoption.

In order to provide backwards compatibility with the existing 4G/LTE infrastructure, the 5G specification defines handovers for transferring a UE between the Evolved Packet Core (EPC) of the 4G network and the 5GC. Depending on a UE's capabilities, interoperability between the two networks can be achieved through either single or dual registration. A device in dual registration mode maintains two different security contexts simultaneously, one for each system. This makes transferring it between the two networks simpler, but requires more data to be stored on the UE side. Correspondingly, in single registration mode, the device only keeps track of one security context, but must perform a full handover and registration procedure when switching between the different networks [TS 33.501, Sec. 8.1].

Similarly to the previously discussed intra-5G handovers, there are different variations of the procedure depending on the availability of network interfaces. Much like in the N2-based handover, there is no direct communication channel between the source and the target network. Instead, indirect connectivity can be provided over the optional N26 network interface between the AMF of the 5GC and the Mobility Management Entity (MME) of the EPC. We just model the variations in which this interface is available, since the lack of a communication channel between the core networks makes the procedure of transferring a UE between them more like a re-registration than a handover. Hence, interworking between the 5GC and the EPC when the N26 interface is not supported is left for future work. We also do not analyze interconnectivity when the UE is in dual registration mode.

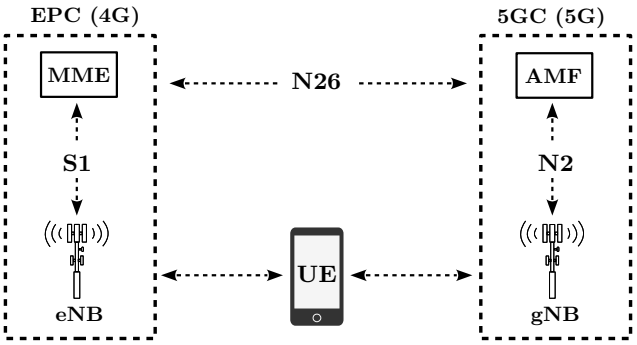

Figure 3: Overview of inter-5G connectivity between the Evolved Packet Core (EPC) of the 4G network and the 5G Core Network (5GC), simplified.

The 5G specification defines two versions of the inter-5G handover, one for each direction (4G to 5G and 5G to 4G). Both versions are specified in detail in [TS 23.502, Sec. 4.11.1.2.1-4.11.1.2.3] and [TS 23.401, Sec. 5.5.1.2.2]. Furthermore, [TS 33.501, Sec. 8.3-8.4] presents minimal versions of the protocols, where all messages and parameters that are unrelated to security are abstracted away. We base our models mostly on these abstracted versions, with a few notable exceptions. In particular, we include some identifiers from the detailed specifications for modeling purposes. However, we do not modify the protocols in any way that changes their behavior: all messages and parameters in our models are described in at least one of the aforementioned specifications. Hence, we pick the right abstraction level for tool support.

3 SECURITY ASSUMPTIONS AND REQUIREMENTS

In this section, we discuss the security assumptions on the initial state of a handover involving 5G networks. We also explain our threat model, summarize the key-derivation processes, and discuss the abstractions related to key-derivation that we used for our protocol models. Finally, we explain the security requirements for all four handover variations. Even though examples and details are only given for intra-5G variations, all information, unless otherwise stated, applies for both the intra- and the inter-5G handovers.

3.1 Setup Assumptions

We identify two main security assumptions for all four handover protocols: (1) all keys and identifiers are initially secret, and (2) the attacker cannot compromise any of the secure channels. Otherwise, the attacker trivially breaks the security.

The channels used in 5G protocols can be divided into private and public channels. As discussed in Section 2.1, all channels within the

5G Core Network are assumed to be secure and uncompromisable. Similarly to the Xn and N2 network interfaces, they provide integrity, confidentiality, and replay protection [TS 33.501, Sec. 5.9.3]. Hence the attacker is unaware of what is sent over these channels and cannot interfere with any traffic. In contrast, the public channels are subject to both passive and active attacks. However, since the initial state is assumed to be secure, communication over public channels can be protected using the shared key material. The 5G specification defines two types of keys for protecting communication over public channels: one for symmetric encryption and one for integrity protection.

Table 1: Overview of channels, network interfaces, and encryption keys, where i = integrity, c = confidentiality, and r = replay protection.

Channel			Network interface	Protection			Encryption key(s)
				i	c	r	
RAN	↔	RAN	Xn	✓	✓	✓	–
RAN	↔	AMF	N2	✓	✓	✓	–
UE	↔	AMF	N1	✓	✓	✓	K_{NASint}, K_{NASenc}
UE	↔	RAN	–	✓	✓	✓	K_{UPint}, K_{UPenc} K_{RRCint}, K_{RRCenc}

All channels, as well as their encryption keys and network interfaces, used for communication in intra-5G handovers are summarized in Table 1, and modeled appropriately. Channels for internal communication within the 5G Core Network are omitted from the table. However, as mentioned previously, they provide integrity, confidentiality, and replay protection [TS 33.501, Sec. 5.9.3].

Messages sent between the UE and the AMF are protected with two keys: K_{NASint} and K_{NASenc}. These are both derived from the K_{AMF} and used for integrity protection and encryption respectively [TS 33.501, Sec. 6.2]. We omit the derivation of these keys and instead encrypt messages directly with K_{AMF} to provide both integrity and confidentiality in our symbolic model. This is a reasonable abstraction since revealing K_{AMF} would allow the attacker to derive both of the aforementioned keys. Similarly to K_{AMF}, the intermediate key K_{gNB^*} is used to derive four keys for protecting traffic between the UE and the RAN: K_{UPenc}, K_{UPint}, K_{RRCenc} and K_{RRCint} [TS 33.501, Sec. 6.2]. These keys are used for encryption and integrity protection of User Plane (UP) traffic and Radio Resource Control (RRC) signaling. As with the other set of keys, rather than deriving the four keys separately, we encrypt all messages directly with K_{gNB^*}.

For the public channels, we use a standard Dolev-Yao attacker [16] as our threat model. The attacker can read, write, modify, and create messages, but not forge signatures or decrypt encrypted messages without the appropriate keys. The attacker also has access to the same set of functions as the honest parties. This means that a leaked key gives the attacker the same capabilities as its owner. However, due to the assumption that the initial state is secure, the key must be learned during the protocol execution.

3.2 Key Derivation

During the initial key agreement process, which precedes a handover, a session key K_{gNB} and a virtual NH parameter are derived by the UE and the SRAN:

> **[TS 33.501, Sec. 6.9.2.1.1]**: "At initial setup, the K_{gNB} is derived directly from K_{AMF}, and is then considered to be associated with a virtual NH parameter with NCC value equal to zero. At initial setup, the derived NH value is associated with the NCC value one."

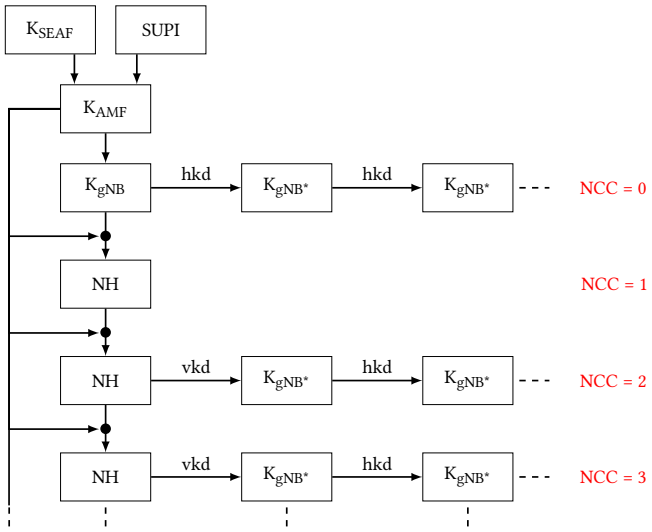

Figure 4: High-level overview of horizontal and vertical key derivation in intra-5G handovers. Combination of [TS 33.501, Fig. 6.9.2.1.1-1] and [TS 38.300, Fig. 13.1-1].

As part of the handover, a new session key is always derived and associated with the target network. There are two alternative methods for re-keying session keys: horizontal or vertical key derivation (see Figure 4). In horizontal key derivation (hkd), the current session key is used as the input key when deriving the next one. The downside of this method is that it does not provide forward security, since learning an old key enables the attacker to derive all subsequent keys. This can be avoided by using vertical key derivation (vkd), which unlike hkd does not use the previous key when deriving the next one. Instead, the new key is derived using an intermediate Next Hop (NH) parameter provided by the AMF. This means that forward security holds with respect to reveals of earlier session keys, as long as the long-term key K_{AMF} remains secret.

Note that the term *forward security* should not be confused with the standard definition of *forward secrecy*. For perfect forward secrecy, if a long-term key is leaked, the attacker cannot derive past session keys and hence decrypt traffic previously sent with them. However he can impersonate parties in the future. In contrast, with forward security, knowing an old session key does not reveal any future keys. The 5G specification defines it as follows:

> **[TS 33.501, Sec. 3.1]**: "In the context of K_{gNB} key derivation, forward security refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to predict any future K_{gNB} that will be used between the same UE and another gNB. More specifically, n hop forward security refers to the property that a gNB is unable to compute keys that will be used between a UE and another gNB to which the UE is connected after n or more handovers (n = 1 or more)."

In Xn-based handovers, the first session key K_{gNB^*} following the initial setup is always be derived using horizontal key derivation:

> **[TS 33.501, Sec. 6.9.2.1.1]**: "Since the AMF does not send the NH value to gNB/ng-eNB at the initial connection setup, the NH value associated with the NCC value one cannot be used in the next Xn handover or the next intra-gNB/intra-ng-eNB-CU handover, for the next Xn handover or the next intra-gNB-CU/intra-ng-eNB handover the horizontal key derivation will apply."

For subsequent handovers, vertical key derivation should be used whenever the SRAN has an unused {NH, NCC} pair available [TS 33.501, Sec. 6.9.2.3.2]. Our models check both options. Table 2 summarizes the key derivation functions used in all of our models.

In Xn-based handovers, the only mandatory key update is to derive the new session key K_{gNB^*} either using horizontal or vertical key derivation. In most cases, no re-keying of long-term keys is necessary, since inter-AMF mobility is not supported in this protocol. However, as specified in [TS 33.501, Sec. 6.9.2.3.2], it is possible for the active AMF to re-derive its long-term key K_{AMF} in case of a 5G NAS security context update. If a handover is subsequently required, but occurs prior to a UE Context Modification procedure, the K_{AMF} must be updated on the UE side before deriving the new session key. Since this requires further actions to be taken in addition to the handover protocol, we do not include it in our model. In contrast, in the N2-based variation, AMF mobility is supported and hence also included in our model.

In N2-based handovers, the session key K_{gNB^*} is always derived using an intermediate NH parameter. In addition to the mandatory re-keying of the session key, the core network can also decide to update its current AMF key. Regardless of whether or not this is the case, a fresh NH is always used for deriving the session key:

> **[TS 33.501, Sec. 6.9.2.3.3]**: "If the source AMF does not change the active K_{AMF} (meaning no horizontal K_{AMF} derivation) [...] the source AMF shall increment its locally kept NCC value by one and compute a fresh NH from its stored data. [...] If horizontal K_{AMF} derivation is performed, [...] the source AMF shall derive a new K_{gNB} associated with NCC = 0 using the newly derived K_{AMF}. [...] Upon receipt of the NGAP HANDOVER REQUEST message from the target AMF, the target ng-eNB/gNB shall compute the K_{gNB^*} to be used with the UE [...] with the {NH, NCC} pair received."

3.3 Security Requirements

The 5G standard does not explicitly state any security requirements for handover protocols. However, it can be assumed that all previous requirements (namely those for initial key agreement) should still hold, i.e., an attacker should be unable to learn any confidential information as a result of a handover. This includes all keys and identifiers derived or created prior to the handover, as well as those updated during it. We identify two main requirements for the protocols: (1) injective agreement of re-derived keys, and (2) secrecy of all keys and identifiers created or used during a handover.

Injective agreement. Informally, injective agreement means that the two parties agree that they are communicating with each other in the same session, which eliminates the possibility of a replay attack. Formally, for key agreement properties, we use Lowe's [22] definition of injective agreement:

Definition 3.1. An agent a in role A is in injective agreement on a key k with an agent b in role B, if whenever a completes a run of the protocol, b has previously been running it with a, and they both agree on the key k. In addition, each run of a must correspond to a unique run of b.

In intra-5G handovers, the two main keys that can be re-derived are the session key K_{gNB} and the AMF key K_{AMF}. Both keys are also derived when transferring a UE from a 4G to a 5G network. Similarly,

Table 2: All key derivations in the 5GC protocols use the Key Derivation Function (KDF) specified in [TS 33.220, Annex B.2.0]. We use a simplification of the KDF function, in which the input string consists of only one (distinct) value, typically P0.

Key	Derivation function	Reference	Xn	N2	5G to 4G	4G to 5G
K_{AMF}	KDF(K_{SEAF}, SUPI)	[TS 33.501, Annex 7]	✓	✓	–	–
	KDF(K_{AMF}, NAS COUNT)	[TS 33.501, Annex 13]	–	✓	–	–
	KDF(K_{ASME}, NH)	[TS 33.501, Annex 15.2]	–	–	–	✓
K_{ASME}	KDF(K_{AMF}, NAS COUNT)	[TS 33.501, Annex 14.2]	–	–	✓	–
K_{gNB}	KDF(K_{AMF}, NAS COUNT)	[TS 33.501, Annex 9]	✓	✓	✓	✓
K_{gNB^*}	KDF(NH, TARGET-ID)	[TS 33.501, Annex 11]	✓	✓	–	✓
	KDF(K_{gNB}, TARGET-ID)	[TS 33.501, Annex 11]	✓	✓	–	
K_{eNB}	KDF(K_{ASME}, NAS COUNT)	[TS 33.401, Annex 3]	–	–	✓	✓
K_{eNB^*}	KDF(NH, eNB-ID)	[TS 33.401, Annex 5]	–	–	✓	–
NH	KDF(K_{ASME}, K_{eNB})	[TS 33.401, Annex 4]	–	–	✓	–
	KDF(K_{ASME}, NH)	[TS 33.401, Annex 4]	–	–	✓	–
	KDF(K_{AMF}, K_{gNB})	[TS 33.501, Annex 10]	✓	✓	–	✓
	KDF(K_{AMF}, NH)	[TS 33.501, Annex 10]	✓	✓	–	–

when moving from a 5G to a 4G network, the UE derives a session key K_{eNB} and a MME key K_{ASME}. As explained in Section 3.1, these so-called *root keys* are used to derive additional keys, which protect the communication over public channels. We abstract these derived keys away and only consider the root keys, thus allowing an attacker access to all related communication.

In both intra-5G variations, a new session key K_{gNB} must be derived by (or provided to) the UE and the TRAN. The AMF key K_{AMF}, however, is only updated during an AMF change in the N2-based handover, or in either variation if the AMF has activated a new Non-Access Stratum (NAS) security context but not yet performed a UE Context Modification procedure. When moving to a network implementing a different standard, new keys must always be derived.

Secrecy (confidentiality) refers to the protection of confidential information against disclosure to unauthorized parties. In all four variations, we analyze whether the following secrecy requirements hold: the attacker does not learn the Subscription Permanent Identifier (SUPI), or any of the keys used or derived during the handover. These include K_{SEAF}, K_{AMF}, K_{ASME}, K_{gNB}, K_{gNB^*}, K_{eNB}, and K_{eNB^*}. The intermediate key NH is omitted from the analysis, since it is only used for re-keying other keys. If the attacker learns it, he will also be able to derive at least one of the other keys as well.

4 FORMAL MODELING AND SECURITY EVALUATION

We use the Tamarin prover, a state-of-the-art protocol verification tool, to formally model and analyze the different 5G handovers. In this section, we give a brief overview of Tamarin, explain how we formalize protocol goals, and summarize our analysis results. All models and the information needed to construct the proof derivations can be found at [26].

4.1 The Tamarin Prover

Tamarin [23, 27] is a state-of-the-art verification tool for the symbolic modeling and analysis of security protocols. Given a formal model of a protocol and its expected properties as input, the tool tries to either prove or disprove the properties. Since the correctness of security protocols is an undecidable problem, termination cannot be guaranteed. Hence, in addition to an efficient and fully automated proof construction mode, Tamarin also provides a mode for interactive reasoning. This ability to provide user guidance when Tamarin's built-in proof strategy does not terminate was one of our main reasons for choosing it as our verification tool. It has also previously been successfully used to analyze various complex, real-world protocols, such as 5G AKA [9, 12] and TLS 1.3 [13, 14].

In symbolic models, all values are described as *terms*, rather than as bitstrings. Each term is either a name, a constant, or a (cryptographic) function application. Functions are represented by *operators*, and their behavior is given by equations. For example, the behavior of symmetric encryption and decryption of a message m is given by the equation `sdec(senc(m,k),k) = m`, where k is a variable representing the encryption key, and the operators `senc` and `sdec` represent functions for encryption and decryption respectively. Tamarin implements many common cryptographic primitives, such as hashing and signatures, by defining equations for their algebraic properties. It is also possible, with some limitations, to create custom functions and equations.

Protocols are modeled using an expressive language based on multiset rewriting rules. These rules give rise to a labeled transition system consisting of a symbolic representation of the protocol's state, messages, and the attacker's knowledge. The state consists of a multiset of facts, where a fact is a predicate applied to terms, representing state information. For example, the state of an agent a in the role A, in which it only knows its own identifier id, is described by the fact `St_1_A(~id)`, where ~ denotes freshness of the value. Both the attacker and honest agents interact by updating the current state of the system. This includes creating fresh constants, applying cryptographic functions to existing terms, and sending and receiving messages over the network.

Protocol rules. In Tamarin, protocol rules are specified using the following syntax: `rule R: [l]–[a]->[r]`, where R is the rule's name, l is its premise, a are its action facts, and r is its conclusion. Premises, actions, and conclusions each consist of multisets of facts. Unlike premises and conclusions, action facts are only observable in the trace. They exists for modeling purposes only and are used to specify security properties, called *lemmas*, expressed as first-order logic formulas.

Attacker knowledge. Tamarin implements a default Dolev-Yao model [16] of the attacker, giving him the capability to delete, inject, modify, and intercept messages in the network. The attacker's knowledge of a message M is denoted `K(M)`. Leakage of any confidential information is modeled by sending it unencrypted over the network and marking the trace with an action fact. We use the notation `Rev(A,M)` to model that an agent A has been compromised and the content of the message M has been revealed to the attacker. For example, the following rule models an agent A revealing its long-term key *skA*:

```
rule reveal_skA:
  [ Ltk(A,skA) ] --[ Rev(A,sKA) ]-> [ Out(skA) ]
```

We use the action fact `Honest(A)@i` to model that an agent A has to be uncompromised at a time point i, for a lemma to be meaningful. A is honest in a trace T, if it has not revealed any information to the attacker, i.e., `Rev(A,M)` $\notin T$.

Secure channels. Sending and receiving messages over the public channel is modeled with the facts `Out(M)` and `In(M)`. However, since many of the communication channels used in handover protocols offer different levels of protection (see Table 1), we implement a standard secure channel abstraction introduced by Basin et al. [10]. This allows us to model messages being sent securely between participants, without having to explicitly create keys for traffic encryption and integrity protection. The rules for securely sending and receiving messages are:

```
rule send_secure:
  [ SndS(~cid,A,B,m) ] --[]-> [ Sec(~cid,A,B,m) ]

rule receive_secure:
  [ Sec(~cid,A,B,m) ] --[]-> [ RcvS(~cid,A,B,m) ]
```

In contrast to the standard public channel, the attacker has no rules to listen in on a secure channel and thereby augment his knowledge `K(.)`. A compromised channel is modeled by revealing the channel identifier *cid* to the attacker, or by allowing messages to be injected

into it. In both cases, additional rules must be introduced to give the attacker the ability to interact with the channels.

Proof strategies. As mentioned previously, Tamarin supports two methods to prove or disprove protocol properties: (1) a fully automatic mode, and (2) an interactive mode. The automatic mode uses heuristics for finding states that terminate each trace. This is often the preferable alternative, since it does not require user input and is thus easily repeatable when verifying the results or changing the model. However, in case of non-termination, or for complicated proofs, the user may choose to explore the state space manually. This can be time-consuming, but is often only necessary in the modeling phase to ensure that a trace in fact exists and to discover a fast way of finding it. Once an efficient proof strategy has been deduced, a small script (called an *oracle*) can be written to guide the automatic prover.

Since our goal is to analyze the protocol properties for an unlimited number of consecutive handovers, we construct an optimized oracle for each model. This helps us avoid non-termination and keeps the time and memory requirements needed for constructing derivations reasonably low.

4.2 Formalizing Protocol Properties

As explained in Section 3.3, we analyze two types of protocol goals: (1) key agreement, and (2) secrecy. We also define and prove various auxiliary lemmas that improve the performance of the prover and perform sanity checks. For example, for every possible variation of the protocols, we prove an executability lemma to ensure that there is *at least one* trace of the protocol that, without the attacker's help, executes to completion. These lemmas improve confidence in the give model, but since they are unrelated to security and not part of the protocol itself, we will not discuss them further.

Key agreement. We denote commitment to a key between agents with the action fact `Commit`, and the intent to complete the protocol with a given partner with the action fact `Running`. Injective agreement of a key holds as defined above, if each instance of `Commit` uniquely corresponds to an instance of `Running` with the required parameters. Furthermore, to prove injective agreement from both participants' point of view, each key requires a second lemma, in which the roles of `a` and `b` are swapped. In Tamarin, injective agreement is formalized as:

```
lemma injectiveagreement_a_b_k:
  " All a b k #i. Commit(a,b,<A,B,k>>)@i
     ==> (Ex #j. Running(b,a,<A,B,k>)@j
          & not (Ex a2 b2 #i2. Commit(a2,b2,<A,B,k>)@i
                 & not (#i2 = #i))) "
```

Secrecy. A value `k` is considered to be secret, if there does not exist a time `j` when the attacker knows `k`, i.e., ¬(∃j. K(k)@j). In Tamarin, a common way of modeling this is by using the action fact `Secret(k)@i`, denoting that a key `k` at a time point `i` is secure, unless it has been revealed to the attacker by an honest agent. If the agent is compromised, the resulting attack is trivial and of no interest. In Tamarin, this is formalized as:

```
lemma secret_k:
  " All k #i. Secret(k)@i
     ==> (not (Ex #j. K(k)@j))
          | (Ex X #r. Rev(X,k)@r & Honest(X)@i) "
```

4.3 Results

Using our models and Tamarin, we show that, after a successful handover, injective agreement holds for all newly derived keys, provided that none of the participating agents or secure channels have been compromised or have leaked any secret information. Furthermore, we prove that misbinding of endpoints is impossible, by letting the attacker unrestrictedly compromise other agents and run unlimited parallel sessions.

Table 4 summarizes the verification results for the key agreement properties. Each property is examined separately from both participants' point-of-view, as explained in Section 4.2. In the Xn-based intra-5G handover, as well as in both inter-5G handovers, the only keys requiring re-keying are the session keys K_{eNB^*} (4G) or K_{gNB^*} (5G). In contrast, the N2-based intra-5G handover may, in case of AMF mobility, also include re-keying of the long-term key K_{AMF}. If the core network decides to allocate a new AMF to the UE, a new long-term key K_{AMF} is also derived. In this case, the UE and the AMF will also agree on the new key.

In addition to key agreement properties, we also prove that all keys used or derived during a handover remain secret. Intuitively, this means that the level of confidentiality remains the same: an attacker should not learn any new confidential information as the result of a handover. Furthermore, for each key, we infer the minimum requirements for secrecy to hold. We do this by gradually strengthening the requirements for secrecy lemmas, until Tamarin

Table 3: Minimum requirements for secrecy. X means that the property holds if X is not known to the attacker. The predecessor (i.e., a previous key from the same horizontal derivation branch) of a key K is denoted $P_{(K)}$. An uncompromised network interface n is marked in_n. The symbol – means that a key can only be known by the attacker if the key itself (or one of its predecessors) has been revealed.

Key	Minimum Requirements for Secrecy (Xn)
K_{SEAF}	–
K_{AMF}	$(K_{SEAF} \vee \text{SUPI})$
K_{gNB}	$(K_{SEAF} \vee \text{SUPI}) \wedge K_{AMF}$
K_{gNB^*}	$(K_{SEAF} \vee \text{SUPI}) \wedge K_{AMF} \wedge \text{in}_{Xn} \wedge P_{(K_{gNB^*})}$
Key	**Minimum Requirements for Secrecy (N2)**
K_{SEAF}	–
K_{AMF}	$(K_{SEAF} \vee \text{SUPI}) \wedge P_{(K_{AMF})}$
K_{gNB}	$(K_{SEAF} \vee \text{SUPI}) \wedge P_{(K_{AMF})} \wedge K_{AMF}$
K_{gNB^*}	$(K_{SEAF} \vee \text{SUPI}) \wedge P_{(K_{AMF})} \wedge K_{AMF} \wedge \text{in}_{N2} \wedge P_{(K_{gNB^*})}$
Key	**Minimum Requirements for Secrecy (5G to 4G)**
K_{AMF}	–
K_{ASME}	$K_{AMF} \wedge \text{in}_{N26}$
K_{gNB}	K_{AMF}
K_{eNB^*}	$K_{AMF} \wedge \text{in}_{N26} \wedge K_{ASME}$
Key	**Minimum Requirements for Secrecy (4G to 5G)**
K_{ASME}	in_{N26}
K_{AMF}	$K_{ASME} \wedge \text{in}_{N26}$
K_{eNB}	$K_{ASME} \wedge \text{in}_{N26}$
K_{gNB^*}	$K_{ASME} \wedge \text{in}_{N26} \wedge K_{AMF}$

Table 4: Key agreement. The symbol ✓ indicates injective agreement on a key between the agents. The symbol – means that the key is not applicable for the combination.

	Intra-5G Handover						Inter-5G Handover			
Protocol ▹	Xn		N2				5G to 4G		4G to 5G	
POV ▹	UE	TRAN	UE		CN	TRAN	UE	eNB	UE	gNB
Counterpart ▹	TRAN	UE	CN	TRAN	UE		eNB	UE	gNB	UE
K_{gNB^*}	✓	✓	–	✓	–	✓	–	–	✓	✓
K_{eNB^*}	–	–	–	–	–	–	✓	✓	–	–
K_{AMF}	–	–	✓	–	✓	–	–	–	–	–

can no longer find an attack trace and provides a proof instead. Table 3 shows the minimum requirements (in conjunctive normal form) for secrecy to hold for each key. All keys are assumed to originate from the same initial key agreement. A key that is not sent over any channel is assumed to remain secret, since it cannot be leaked as the result of a handover. We explain these results below and comment on their significance for the 5G protocol suite and associated infrastructure.

Intra-5G handovers. After the initial key agreement between a UE and a RAN, the anchor key K_{SEAF} and the UE's secret identifier SUPI are used to derive a long-term key K_{AMF}, which in turn is (indirectly) used to derive all other keys. None of these keys or identifiers are sent over any channel during a handover, which limits the risk of an attacker learning any of the long-term keys. In the Xn-based handover, this means that K_{AMF} cannot be compromised after it has been derived, since it is fixed and only keys derived one-way are used. Tamarin reports that, as shown in the second row in the first table in Table 3, the attacker can only derive K_{AMF} by first learning both K_{SEAF} and SUPI. Furthermore, as indicated in the subsequent rows, since K_{AMF} is used as the anchor key, none of the other keys will remain secret if these two are leaked.

As explained in Section 4.2, the N2-based handover supports AMF mobility. If the CN decides to update the AMF allocation of the UE during a handover, a new K_{AMF} is also derived. Since the new K_{AMF} uses the previous one as keying-material, no new information that could compromise the secrecy of the key is exchanged. However, if an old K_{AMF} (indicated as $P_{(K_{AMF})}$ in the second table in Table 3) is leaked, future keys are no longer secure, since forward security is not provided. This (shown in the subsequent rows in the table) means that the attacker can use any deprecated K_{AMF} for deriving all future keys.

The initial session key K_{gNB} is derived directly from K_{AMF} and, similarly to its parent key, it is never sent over any channel during a handover; this explains the conjunctions for K_{gNB} in the Xn and N2 tables. In both intra-5G protocols, an intermediate session key K_{gNB^*} is derived from either its predecessor (hkd) or from the intermediate NH parameter (vkd). After the handover is successfully completed, K_{gNB^*} becomes the new session key. Similarly to K_{AMF} in the N2-based protocol, horizontal key derivation does not protect future keys from an attacker who knows an old session key, i.e., forward security is not provided.

Furthermore, in both models, either the session key itself or the intermediate parameter that it is derived from, is sent over a secure interface. Consequently, an attacker can learn K_{gNB^*} in one of two ways: (1) by compromising an agent that knows the key (or one of its predecessors), or (2) by compromising the secure interface(s) that the key (or one of its predecessors) was sent over. An uncompromised interface is marked in Table 3 as $in_{Xn/N2/N26}$.

Inter-5G handovers. In inter-5G handovers, the anchor key used to derive session keys depends on the current network of the UE: K_{AMF} in 5G and K_{ASME} in 4G. In Table 3, these are shown on the first row of the third and fourth tables respectively. When moving from 5G to 4G, the AMF of the 5G network derives K_{ASME} from K_{AMF} and sends it over the (secure) N26 interface to the 4G network's Mobility Management Entity. Similarly, when moving from 4G to 5G, the MME sends K_{ASME} to the AMF so that a new K_{AMF} can be derived. Unlike in the intra-5G protocols, this means that the long-term keys can be leaked if the attacker can compromise a secure network interface or trick the sending network function to leak the key to the wrong receiver. However, as our Tamarin verification proves, this can only happen if the security assumptions and requirements presented in Section 3 are neglected.

Similarly to vertical key derivation in intra-5G handovers, a new session key is derived in the inter-5G handovers using intermediate parameters, which are derived from the anchor key. Consequently, as can be seen on the fourth row in the lower tables of Table 3, the session key can only be known to the attacker if the keys themselves, or the corresponding anchor key, have been leaked.

5 CONCLUSION

We have analyzed the security of handovers involving 5G networks. The current version of the standard (Release 16) includes nine documents describing four main variations of the protocol, covering both intra- and inter-system handovers. Using formal methods, we analyzed all of these procedures and established the minimal assumptions under which they are secure. Namely, none of the handovers reveal any confidential information to an attacker, as long as the initial state is secure and none of the honest participants can be compromised.

As future work, we recommend extending the coverage of formally verified sections of the 5G standard. In addition to creating new models of previously unverified protocols, updating existing models can be helpful for detecting vulnerabilities introduced in later releases. Furthermore, we plan to extend our work by considering the impact of downgrade attacks. Even though we have shown that inter-system handovers do not leak information, an attacker might benefit from forcing a device to fall back to a network implementing an older standard. In particular, an attacker might be able to use fallback methods of the LTE network to further weaken the security provided by the newer standards.

ACKNOWLEDGMENTS

This work was partly funded by the Academy of Finland (Grant No.: 296693). The authors also thank Huawei Singapore Research Center for their support for parts of this research.

REFERENCES

[1] 3GPP. 2020. 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401, V16.3.0.
[2] 3GPP. 2020. General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access. TS 23.401, V16.7.0.
[3] 3GPP. 2020. Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA). TS 33.220, V16.7.0.
[4] 3GPP. 2020. NR and NG-RAN Overall Description. TS 38.300, V16.2.0.
[5] 3GPP. 2020. Procedures for the 5G System (5GS). TS 23.502, V16.5.0.
[6] 3GPP. 2020. Security architecture and procedures for 5G system. TS 33.501, V16.3.0.
[7] 3GPP. 2020. Summary of Rel-16 Work Items. TR 21.916, V0.4.0.
[8] 3GPP. 2020. System Architecture for the 5G System (5GS). TS 23.501, V16.5.0.
[9] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirović, Ralf Sasse, and Vincent Stettler. 2018. A Formal Analysis of 5G Authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1383–1396. https://doi.org/10.1145/3243734.3243846
[10] David Basin, Saša Radomirović, and Lara Schmid. 2016. Modeling Human Errors in Security Protocols. In *2016 IEEE 29th Computer Security Foundations Symposium*. IEEE, 325–340.
[11] Piergiuseppe Bettassa Copet, Guido Marchetto, Riccardo Sisto, and Luciana Costa. 2017. Formal verification of LTE-UMTS and LTE-LTE handover procedures. *Computer Standards & Interfaces* 50 (2017), 92–106.
[12] Cas Cremers and Martin Dehnel-Wild. 2019. Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion. In *Network and Distributed Systems Security (NDSS) Symposium 2019*.
[13] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, and Thyla van der Merwe. 2017. A Comprehensive Symbolic Analysis of TLS 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, Texas, USA) *(CCS '17)*. Association for Computing Machinery, New York, NY, USA, 1773–1788. https://doi.org/10.1145/3133956.3134063
[14] Cas Cremers, Marko Horvat, Sam Scott, and Thyla van der Merwe. 2016. Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 470–485.
[15] Konstantinos Dimou, Min Wang, Yu Yang, Muhammmad Kazmi, Anna Larmo, Jonas Pettersson, Walter Muller, and Ylva Timner. 2009. Handover within 3GPP LTE: Design Principles and Performance. In *2009 IEEE 70th Vehicular Technology Conference Fall*. IEEE, 1–5.
[16] Danny Dolev and Andrew Yao. 1983. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory* 29, 2 (1983), 198–208.
[17] Ericsson. 2016. *Cellular networks for Massive IoT*. Technical Report. https://www.ericsson.com/4ada75/assets/local/reports-papers/white-papers/wp_iot.pdf.
[18] Ericsson. 2020. *Ericsson Mobility Report, June 2020*. Technical Report. https://www.ericsson.com/49da93/assets/local/mobility-report/documents/2020/june2020-ericsson-mobility-report.pdf.
[19] Ericsson. 2021. *Ericsson Mobility Report, February 2021*. Technical Report. https://www.ericsson.com/49220c/assets/local/mobility-report/documents/2020/emr-q4-2020-update.pdf.
[20] Noomene Ben Henda and Karl Norrman. 2014. Formal Analysis of Security Procedures in LTE – A Feasibility Study. In *Research in Attacks, Intrusions and Defenses*. Springer International Publishing, Cham, 341–361.
[21] Mads Lauridsen, Lucas Chavarría Giménez, Ignacio Rodriguez, Troels B Sørensen, and Preben Mogensen. 2017. From LTE to 5G for Connected Mobility. *IEEE Communications Magazine* 55, 3 (March 2017), 156–162.
[22] Gavin Lowe. 1997. A Hierarchy of Authentication Specifications. In *Proceedings 10th Computer Security Foundations Workshop*. IEEE, 31–43.
[23] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. 2013. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In *Computer Aided Verification*. Springer Berlin Heidelberg, Berlin, Heidelberg, 696–701.
[24] Nokia and Omdia. 2020. *Beyond connectivity: CSP perspectives on higher-value 5G use cases*. Technical Report. https://onestore.nokia.com/asset/207152.
[25] Hyun-Seo Park, Yuro Lee, Tae-Joong Kim, Byung-Chul Kim, and Jae-Yong Lee. 2018. Handover Mechanism in NR for Ultra-Reliable Low-Latency Communications. *IEEE Network* 32, 2 (2018), 41–47.
[26] Aleksi Peltonen, Ralf Sasse, and David Basin. 2021. Tamarin models and instructions for reproducibility. https://github.com/tamarin-prover/tamarin-prover/tree/develop/examples/wisec21-5G-handover. Accessed: 2021-05-25.
[27] Benedikt Schmidt, Simon Meier, Cas Cremers, and David Basin. 2012. Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties. In *2012 IEEE 25th Computer Security Foundations Symposium (CSF '12)*. IEEE Computer Society, USA, 78–94. https://doi.org/10.1109/CSF.2012.25

A ACRONYMS

3GPP	3rd Generation Partnership Project
5G	5th Generation
5G AKA	5G Authentication and Key Agreement
5G-GUTI	5G Globally Unique Temporary Identifier
5GC	5G Core Network
AMF	Access and Mobility Management Function
C-RNTI	Cell Radio Network Temporary Identity
CN	Core Network
eNB	evolved Node B
EPC	Evolved Packet Core
gNB	Next generation Node B
KDF	Key Derivation Function
LTE	Long-Term Evolution
ME	Mobile Equipment
MME	Mobility Management Entity
MRU	Mobility Registration Update
NAS	Non-Access Stratum
NASC	NAS Container
NCC	NH Chaining Counter
NF	Network Function
NG-RAN	Next Generation RAN
NH	Next Hop
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
RAN	Radio Access Network
RAT	Radio Access Technology
RRC	Radio Resource Control
S2TTC	Source to Target Transparent Container
SMF	Session Management Function
SRAN	source RAN
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
T2STC	Target to Source Transparent Container
TR	Technical Report
TRAN	target RAN
TS	Technical Specification
UE	User Equipment
UEC	UE Container
UMTS	Universal Mobile Telecommunications System
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module

B MESSAGE SEQUENCE CHARTS

Figures 5–7 show the detailed message flows of the N2-based intra-5G handover and the N26-based inter-5G handovers. Similarly to the Xn-based handover in Figure 2, all messages and parameters that are unrelated to security are abstracted away.

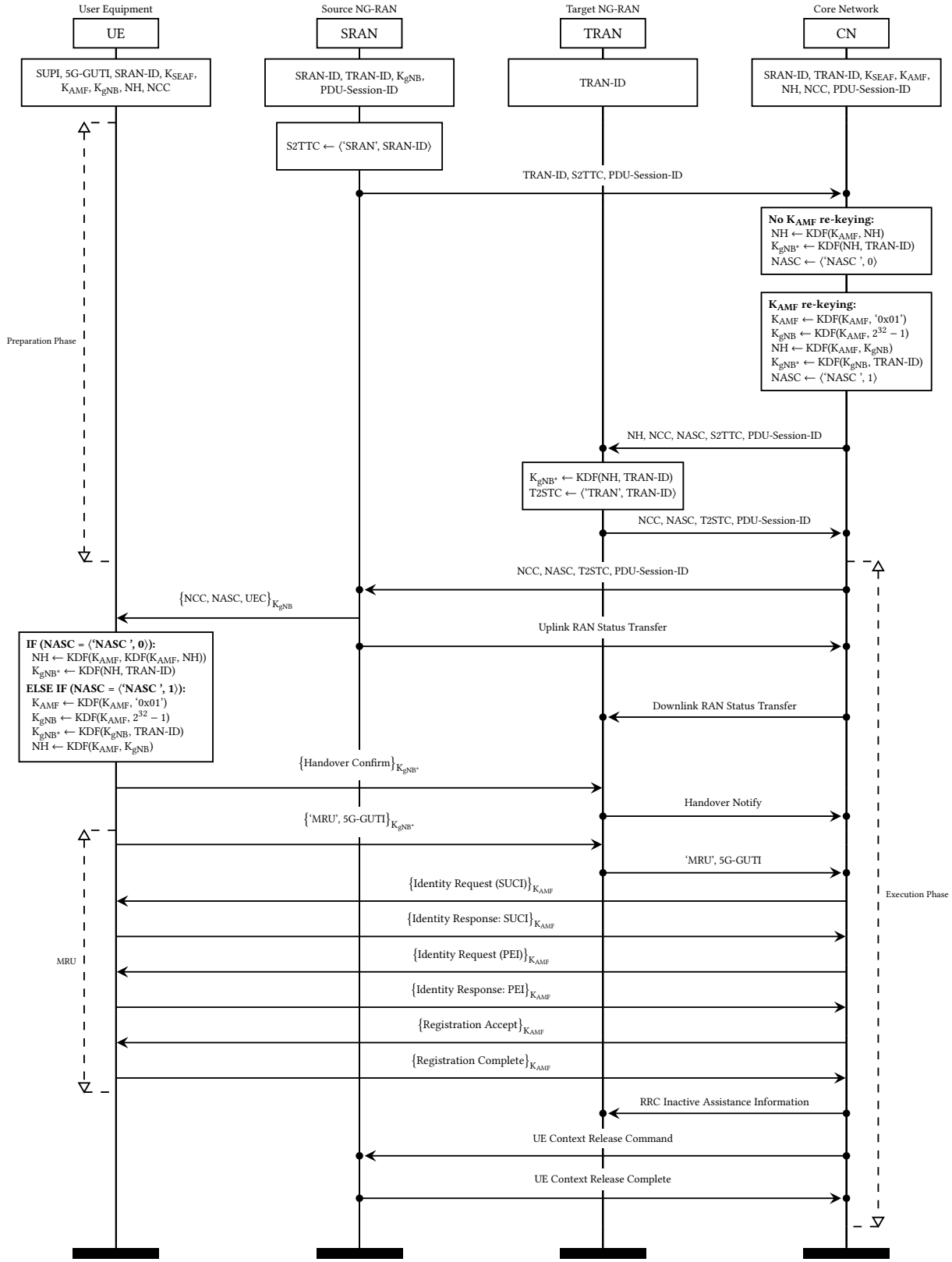

Figure 5: N2-based intra-5G handover. The symbol • means that a channel is secure (provides integrity, confidentiality, and replay protection). Symmetric encryption with a key K is denoted $\{\}_K$.

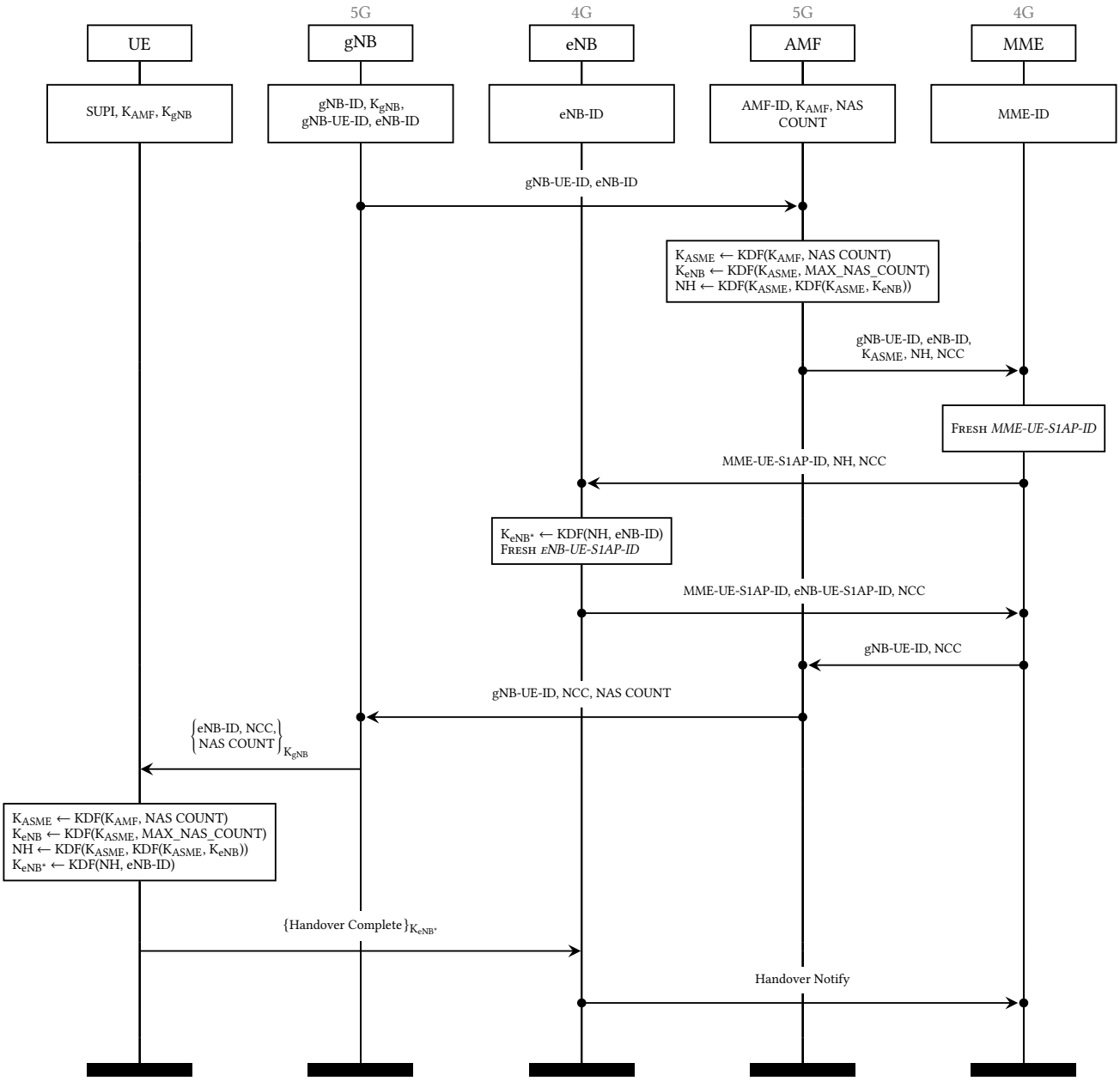

Figure 6: Handover from 5G to 4G over the N26 interface. Only includes messages and parameters that are relevant to security. The symbol • means that a channel is secure (provides integrity, confidentiality, and replay protection). Symmetric encryption with a key K is denoted $\{\ \}_K$. eNB-UE-S1AP-ID and MME-UE-S1AP-ID are unique identifiers of the UE within the eNB and MME [TS 23.401, Sec. 5.7.1]. gNB-UE-ID is the UE identifier within the gNB. MAX NAS COUNT is the constant value $2^{32} - 1$.

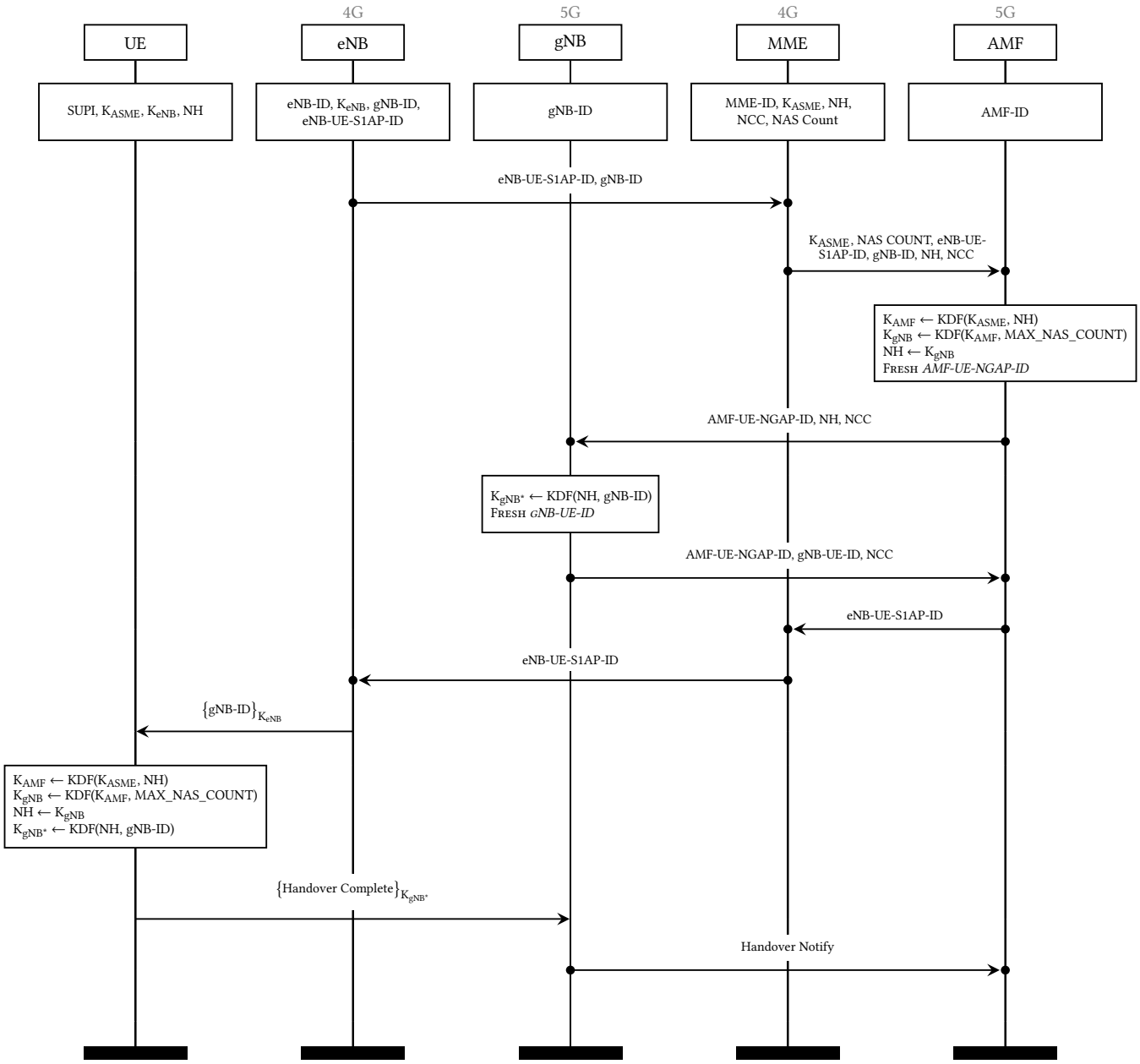

Figure 7: Handover from 4G to 5G over the N26 interface. Only includes messages and parameters that are relevant to security. The symbol • means that a channel is secure (provides integrity, confidentiality, and replay protection). Symmetric encryption with a key K is denoted $\{\}_K$. eNB-UE-S1AP-ID [TS 23.401, Sec. 5.7.1] and AMF-UE-NGAP-ID [TS 23.501, Sec. 5.9.9] are unique identifiers of the UE within the eNB and AMF. gNB-UE-ID is the UE identifier within the gNB. MAX NAS COUNT is the constant value $2^{32} - 1$.