The Challenge of Private Identification

Stig Frode Mjølsnes, Ruxandra Florentina Olimid

The Challenge of Private Identification

Stig F. Mjølsnes and Ruxandra F. Olimid

Department of Information Security and Communication Technology, NTNU,
Norwegian University of Science and Technology, Trondheim, Norway
sfm@ntnu.no, ruxandra.olimid@ntnu.no

Abstract The cryptographic protocol problem of how to make a secure exchange of identifying information among communicating entities, in particular within security constraints of confidentiality and personal privacy, is here denoted as *the private identification problem.* We consider this to be still an open problem. Although we can find its motivation and partial solutions in some of the existing systems, this paper describes the problem in a more generalised form. What is the solution space of efficient and scalable private identification protocols within the settings of the various communication systems and models, for instance in future mobile communication systems with very low latency requirements? Possible directions and solutions are discussed, in terms of pseudonyms, temporary identifiers, computational trade-offs such as key search, and public key solutions. All existing proposals to the private identification challenge suffer from one or more limitations and weaknesses, such as computational costs and time latencies, or the security is reduced. Finally, the paper collects a considerable reference list of papers related to the problem of private identification.

Keywords: Private Identification, Cryptographic Protocols, Privacy, Mobile Communications, Network Security, 5G Security

1 Introduction

1.1 Motivation

Privacy in a digital world is a difficult notion to define in the general sense. Put it simple, privacy means that users can control which of their personal information can be accessed by other parties, when and under what circumstances. Privacy is one of the fundamental requirements in mobile communication systems, but it becomes challenging to maintain because of the very fast technological advances:

> *New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. [...] The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.* [1]

Finn et al. list seven types of privacy, imposed by the development of technology. They include privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association [2]. A simple example of privacy exposure is location tracking in mobile communication systems: the adversary checks the presence of subscribers in a location and tracks the location of mobile devices as they move. This is possible in all mobile generation networks starting with 2G (including 4G) by tracking the permanent identity of the subscriber IMSI (International Mobile Subscriber Identity), or by linking the permanent identity to temporary identities associated to each subscriber. In practice, identities disclosure can be done both passively (by eavesdropping on the uplink or downlink channel between the user equipment and the tower) and actively (by using IMSI Catchers, rogue base stations that acquire subscribers' identities within a location) [3–7]. The attacks are possible, for instance, because the adversary can force the following scenario, documented in the 3GPP standards as a breach in the confidentiality of the user identity:

> *[. . .] requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents a breach in the provision of user identity confidentiality.* [8]

We explained above the motivation in terms of mobile communication networks, but of course the same challenge arises in all systems where devices must be identified, while keeping their identity hidden to a possible adversary. Examples include RFID (Radio Frequency Identification) devices that might be used to track people's movement by localising the tags associated to objects, or vehicles in intelligent transport systems, which might leak movement to unauthorised parties.

A frequent cause for privacy disclosure is that (permanent) identifiers are communicated in clear. Although this should be done only in specific circumstances that should occur with low probability, the adversary can force this functionality, and therefore break the privacy of subscribers. Throughout the paper, by *identification* we simply mean that a subscriber makes its identity known to a service provider (e.g.: network operator, card reader, etc.). If the identity is sent in cleartext, it is immediately revealed to third parties by eavesdropping. Later on, the identity is proved during the *authentication* procedure and is grant access to resources and services by *access control* mechanisms. We do not deal here with the process of confirming the correctness of the identity, but we are only interested on how can a device communicate its identity without exposing it to unauthorised parties. Decoupling identification from authentication maintains the authentication mechanisms unchanged and introduces the private identification challenge as a general standalone problem.

1.2 Our contribution

We propose to investigate the following open problem:

How can we construct efficient and scalable private identification mechanisms in (mobile) communication systems? More concrete, how can a device identify itself to the (mobile) network while never disclosing its (permanent) identity to an adversary?

We state the problem here in terms of mobile communication and networking and emphasise its importance for 5G and beyond, but the problem is of interest of its own. The problem is not new and has been stated before, both in the field of mobile communication systems and others. However, all the approaches are particular to the system of interest. We now formally define the problem in abstract terms and challenge to find a general private identification solution that addresses all scenarios (or as many as possible, aiming to be a universal solution up to some assumptions). A feasible solution to the general challenge of private identification that can accommodate a large number of subscribers would be of great value for both theoreticians and practicians. We target for a solution with no central trusted authority, but only a bi-directional communication between the subscriber and the provider. Moreover, we aim no change in the architecture of the existing systems, and we challenge the existence of a solution that works in the general settings, as explained before.

Keeping in mind our motivation, we explain the problem in the particular case of LTE and others (e.g.: RFID) and discuss some partial existing solutions. We do not aim to perform a security analysis of any of the presented protocols, but just discuss different ideas on how to approach the problem, and highlight their drawbacks. Also, we do not aim to provide an exhaustive view of the literature, but redirect the reader to surveys, when needed. Our goal is not to give a fully compliant solution here, but to discuss distinct approaches and highlight open research problems.

2 Related work

2.1 Models and definitions

Abadi and Fournet give an informal definition of the privacy property in the mobile settings [9]. Their definition is stronger than what we aim for here. Besides other properties, they consider authentication too, in the sense that the subscriber needs to prove its identity. They give two constructions that do not assume pre-shared secrets, but make use of the public key cryptography (public key encryption and signatures, certificates generated by a trusted authority). Some other informal definitions of private identification and adversarial models are given in other papers, which we will refer to in Section 4, when we briefly explain what is their approach to solve the problem.

Much more work has been done in formalising a security model for private identification in RFID systems. Hermans et al. introduce a RFID privacy security model that is general and can be applied for multiple readers [10]. It extends the previous models of Vaudenay [11], Canard et al. [12] and others (see [10] for more details). Very recently, Yang et al. define a privacy model for the RFID tag ownership transfer and use it to prove the security of public-key based protocols [13]. However, all these models are particularly built for RFID systems.

2.2 Projects

Several European projects has been allocated to security and privacy issues in communication systems. 5G Ensure is a project that focuses on secure, trustworthy and viable 5G networks. The project will address security, privacy and trust challenges in 5G caused by heterogeneous nature of the new generation networks [14]. Previous examples include PRIME (Privacy and Identity Management for Europe), which aimed to reconcile privacy and accountability of users' electronic interaction [15], and its successor PrimeLife, which continued the work in identity management to future networks and services until 2011 [16]. Within the two projects, IBM Research has designed and implemented a system for identity management, called Identity Mixer, a cryptographic protocol suite that implements privacy-preserving authentication [17].

Many papers, some associated to international projects, try to give solutions to private authentication in mobile communication networks (GSM, UMTS, LTE) and RFID. We skip them here, as many will be referred to in more detail in Section 4, but invite the reader to read the surveys for more details [18–20].

3 Problem statement

3.1 Parties

Subscriber. A subscriber is an entity that has to identify itself to the system, to gain access to the resources and services of a service provider. The user is uniquely identified by a long-term identifier $\mathcal{S}_i$ and can possibly own private credentials (e.g.: passwords or long-term secrets) that are pre-shared with the provider during the registration phase, or it might have certificates emitted by a trusted certificate authority. The subscriber can make use of a rewritable memory and can perform cryptographic computations. Depending on the scenario, the functionalities of the subscriber might be limited in storage and computational power. Let $\mathcal{S} = \{S_1, \ldots, S_n\}$ be the set of all registered subscribers.

Service Provider. A service provider $\mathcal{P}$ is an entity that offers services and resources to subscribers. The service provider may have certificates emitted by a trusted certificate authority or private pre-shared data with the registered subscribers. The provider has more computational power and storage capacity than the subscribers, being capable to process several requests from different subscribers and perform advanced cryptography.

3.2 Assumptions

This work concerns with privacy preserving during the identification of a subscriber to a provider. We assume that there exists a secure generation and distribution mechanism that provides the inputs for the private identification system. We also assume that information is stored secure on both subscriber's and provider's side. This means for example that the pre-shared key in the USIM is not compromised at any time and the adversary cannot gain access to the HSS (Home Subscriber Server), where the identification and authentication parameters of the subscribers are stored in the core network of the mobile operator. Moreover, we do not consider any side channels attacks that could leak private data. This is the case of identification in RFIDs, which were shown to be vulnerable to this kind of attacks [21].

We also ignore communication related identifiers (e.g.: IP addresses, MAC addresses, etc.) that might allow linkage of different messages that are sent over the communication medium. More precise, we assume that communication itself does not reveal any information about the identity of the subscriber. This assumption has been done in previous work too [9]. We realise that this assumption is strong, and it will hardly be reasonable without further measures within many practical communication system contexts.

3.3 Adversarial power

The adversary can intercept any message sent on the communication medium. We also assume that the adversary is active, in the sense that can insert, change or delete any message on the communication channel. Hence, the adversary can try to impersonate the parties by any means with the aim to break the privacy of the subscriber. A concrete example of this capability of the adversary is the IMSI Catcher: a false base station that impersonate the mobile operator and asks the subscribers to reveal their IMSIs in clear.

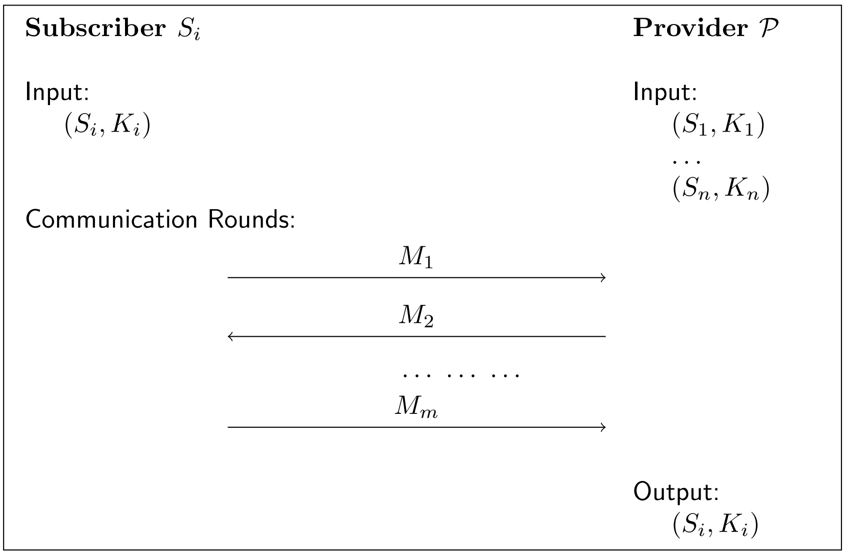
We consider a strong adversary that can reveal private information belonging to others subscribers that not take part to a given session. This is a natural assumption, as the adversary can simply buy access to services (e.g.: the adversary can buy USIM cards from a mobile network operator). For similar reasons, coalition between the subscribers must be accepted too.

Finally, we try to avoid here an assumption that is very frequent in the mobile communication network settings and that asks the adversary not to be omnipresence, in the sense that he can follow the subscriber up to a limited number of locations only. We now target a solution that works regardless of the area controlled by the adversary.

3.4 Problem definition

Let $\mathcal{S} = \{S_1, \ldots, S_n\}$ be a set of pre-registered subscribers to a service provider $\mathcal{P}$. Each subscriber is uniquely identified by its identity S_i, $1 \leq i \leq n$ and shares a private key K_i with $\mathcal{P}$. The parameters (S_i, K_i) are available both to the subscriber and the provider as the output of a correct registration of the subscriber S_i to the service provider $\mathcal{P}$. Therefore, $\mathcal{P}$ stores the complete set of values associated to registered subscribers $\{(S_i, K_i)\}_{1 \leq i \leq n}$. As previously explained, we assume that the values are stored perfectly secure on both the subscriber and the provider side, and they can only be tampered with or disclosed if they are exchanged via the communication medium subsequent to the registration phase. We also assume independence between the identity and the key of a subscriber and independence between the parameters of different subscribers. All assumptions are without loss of generality, because registration in practice mainly consists in the service provider provisioning the values to some devices and then distribute them to users (e.g.: the SIM card is first programmed by the mobile operator with an IMSI and a private key K_i, and only then delivered to the user).

We call a *private identification protocol* a protocol between a subscriber $S_i \in \mathcal{S}$ and a provider $\mathcal{P}$ that allows S_i to successfully identify itself to $\mathcal{P}$ without disclosing its identity or its private key on the communication medium. We decouple the protocol from the registration phase to gain independence in design and analysis. This extends the applicability to various scenarios, independently from the way registration is conducted or the relation between the parameters output by the registration phase up to some premises. The protocol consists in one or several communication rounds; without loss of generality we assume S_i to be the initiator of the first and last rounds.



We describe the problem in terms of symmetric settings. This is because a trivial solution exists with public key primitives, but such asymmetric crypto-primitives have not been accepted in mobile systems because of real-time performance and efficiency requirements (see Section 4 for details).

A private identification protocol PIP is *perfectly secure* if its execution gives no extra information about the subscriber that takes part at the execution of the protocol: for any adversary $\mathcal{A}$, the probability to identify S_i before and after running the protocol is the same; analogous, the knowledge on the private key K_i of the subscriber before and after the execution of the protocol is the same. The security can of course be defined in computational settings, which is of value in practice: the adversary $\mathcal{A}$ is computationally bounded and the gain in knowledge on S_i and K_i can be up to negligible higher after the execution of the protocol than before its execution. Moreover, the adversary is given permanent access to the communication medium and can ask a limited number of queries to gather additional information (e.g.: private parameter of subscribers, others than the one that participates to the test session, transcription of other sessions of the protocol, etc.). Both are natural assumptions in the mobile environment, where the communication is wireless, and the access to services is open to public. For example, even if the SIM cards acquisition should not reveal the private provisioned information K_i, it allows direct access to the IMSI.

The *private identification challenge* (in the symmetric settings) asks to find if it possible to design an efficient private identification protocol PIP that is secure for a given distribution of (S_i, K_i), and if yes to give its description. We do not challenge perfect security, but the existence of such a solution in the computational settings, for example. We can state the private identification problem both in *decisional* (prove the existence or inexistence of such a solution) and *descriptive* (if such a solution exists, describe the protocol) versions. We will see in Section 4 that simple solutions that perform in linear time in the number of subscribers exists, but they are not acceptable in practice. In a nutshell, we are interested in an efficient protocol PIP as follows:

1. Input:
   - Each subscriber S_i, $1 \leq i \leq n$ owns a pair (S_i, K_i)
   - $\mathcal{P}$ owns the pairs associated to all subscribers $\{(S_i, K_i)\}_{1 \leq i \leq n}$
2. A subscriber S_i runs one or more instances of PIP with the service provider $\mathcal{P}$
3. Output:
   - $\mathcal{P}$ learns the identity S_i
   - For any adversary $\mathcal{A}$, PIP is secure.

Besides distinct security requirements (perfect secrecy, computational security, etc.), the private identification problem can be stated in different flavours. One possible valuable approach in practice might be to accept probabilistic identification success: $\mathcal{P}$ correctly identifies S_i with a probability $p < 1$, where the value of p is given by the use case.

Because of the possibility of modelling the problem in multiple settings, we avoid more rigorous formalisation here. However, we list some of the informal properties a private identification protocol should satisfy:

- *Privacy.* The protocol must not leak any information that can help in identifying the subscriber or learning the private shared key.
- *Unlinkability.* Two or more messages exchanges cannot not be linked to the same subscriber.

- *Protection against location disclosure or tracking.* Tracking a subscriber's location must not be possible.
- *Protection against cloning and impersonation.* The subscribers must not be prone to cloning or impersonation after one or more runs of the private identification protocol. Impersonation performed by replay attacks could be up to some point avoided by the subsequent authentication mechanisms.
- *Efficiency.* The private identification protocol must comply in speed, computational power, number of rounds, etc. with the requirements.
- *Scalability.* The identification protocol must be scalable to very large sets of subscribers (hundreds of millions).

For the case of mobile networks, the efficiency and scalability requirements should be measured against the 5G specifications, where throughput on the downlink will be 20 Gbps per cell, the signal latency less than 4 ms, and the density of mobile devices is set to 10^6 connections per km^2.

3.5 Use Cases

LTE (Long Term Evolution). In LTE, $\mathcal{S}$ is the set of UEs (User Equipments) registered to the 4G services provided by a mobile operator $\mathcal{P}$. More exactly, $\mathcal{P}$ can be seen as the HSS (Home Subscriber Service) that stores users' identification and authentication information such as the IMSI and the private key K_i. Same parameters are stored both in the USIM card and in the HSS, allowing for correct authentication and access control to mobile services. The problem asks if a UE can efficiently identify itself to the mobile network without disclosing its permanent identifier IMSI or any other temporary identifiers (e.g.: TMSI, GUTI, etc.) or metadata that would allow linkage to its identity and therefore break its privacy.

RFID (Radio-Frequency Identification). RFID tags are chips with radio capabilities that store a unique identifier that is sent to a reading device, enabling identification of objects without physical contact. In RFID systems, $\mathcal{S}$ is the set of tags, and $\mathcal{P}$ is the system reader. Subsequent authentication relies on a symmetric key K_i shared between each tag and the reader. The private identification challenge in RFID systems asks that a RFID device identifies itself to the reader without disclosing its tag (and the private shared key).

4 Possible solutions

The problem of private identification can be approached from different perspectives, with respect to the underlying idea and cryptographic primitives. As the PRIME project explains:

> *Individuals can limit the information collected about them by using pseudo-identities, certifications and cryptography when performing online transactions [22].*

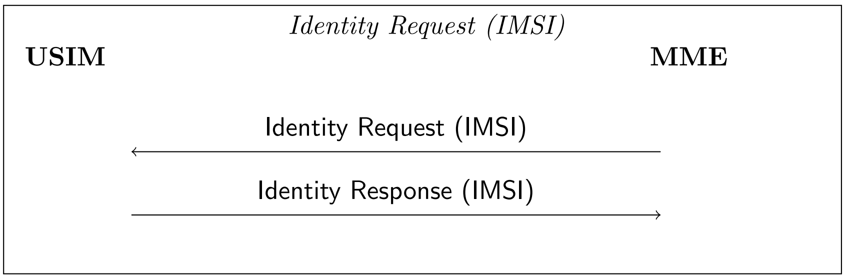
We now discuss various existing approaches to solve the problem.

4.1 Pseudonyms or Temporary Identifiers

A pseudonym is a name, different from the long-term identifier, by which a subscriber S_i is known to the service provider. It might be generated both at the subscriber's side and the service provider's side and might be temporary, so valid for a limited amount of time only and exchanged periodically.

In mobile communication systems, several types of temporary identifiers have been used starting with 2G. The most popular example is the TMSI (Temporary Mobile Subscriber Identity), a local temporary identifier in the area where the phone is located. TMSI reallocation procedure should be performed after the initialisation of the ciphering so that TMSI is not communicated in cleartext. The TMSI reallocation procedure is explained in [23].

In LTE, TMSI is contained in GUTI (Global Unique Temporary User Equipment Identity). The goal of GUTI is to provide unambiguous identification of the UE that does not reveal its permanent identity to the network [24]. The periodicity of changing the temporary identifiers is at the choice of the network operator, and it has been shown that this is sometimes done too less frequently, resulting in privacy exposure [25]. However, such mechanisms can be overpassed, user identification by the permanent identity being possible when the serving network cannot be identified by the temporary identity GUTI [8]. The mechanism of requesting the IMSI is initiated by the MME (Mobile Management Entity) and the UE responds with the IMSI in cleartext, which is clearly a privacy breach.


Identity Request (IMSI)

Among others, we have successfully impersonated a base station and reveal IMSIs in the LTE communication network by setting up a IMSI Catcher [3–7].

Kesdogan et al. proposes to use temporary subscriber identities generated by a Trusted Third Party (TTP) to solve what they called the private localisation problem [26]. Their solution assumes initial mobile network access to one or more of these TTPs can be done, and therefore does not solve our problem of identification before communication access.

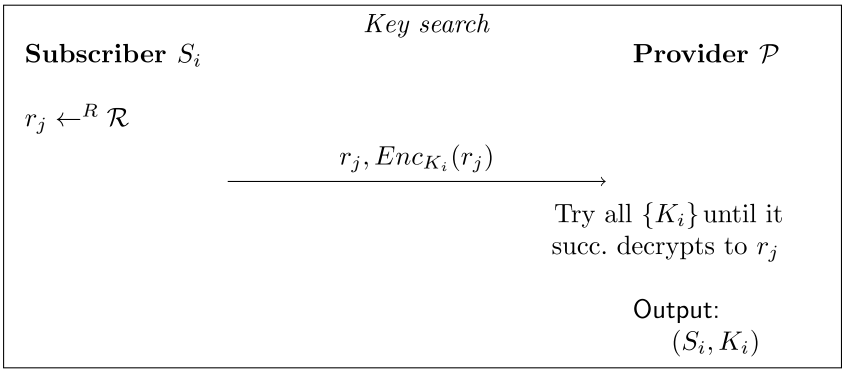
Khan and Mitchell introduce a solution that requires no change in the architecture of the mobile communication network, but it requires changes in the USIM and the authentication centre [27]. Their solution is based on the existence of several IMSIs for each individual USIM, which introduces some pseudonymity for the user. An IMSI change can be initiated either by the USIM, or by the network. This limits the scenarios where the IMSI is sent in clear over the air interface, but does not represent a solution to our challenge. As the authors admit, their aim is to limit the degree to which the use of IMSI compromises the user privacy, but it is a trade-off between the validity of an IMSI and the overhead in terms of database management. The change of IMSIs and their synchronization must be done with care, not to end in a DoS attack when an active attacker is either able to change the IMSI to an invalid value or to trigger the consumption of all list of IMSIs.

Several other solutions are based on mitigating the exposure of IMSIs on the air interface. Recent examples include the work of Choudhury et al. that propose the usage of DMSI (Dynamic Mobile Subscriber Identities) [28], or the work of van den Broek et al. that introduces PMSI (Pseudo Mobile Subscriber Identifier) [29], which requires significant changes in the HSS and the authentication exchanged messages. A very recent proposal similar to the work of Choudhury et al. makes use of temporary identifiers called CMSI (Changing Mobile Subscriber Identity) that only the HSS can change to the IMSI permanent identity [30]. The authors claim their solution is more efficient in terms of changes rather than previous solutions because the structure of the messages remains unchanged, making it transparent to intermediate networks.

Surveys and recent papers on RFID privacy give a nice overview of the existing solutions for RFID systems [13, 18, 19, 31, 32]. Many solutions based on pseudonyms in RFID systems are in fact key-search, requiring linear complexity in the number of the tags. As an example of logarithmic complexity, we refer to the work of Molnar et al. [33]. They introduce a *pseudonym protocol* that makes the RFID tag to send a different pseudonym generated by a pseudorandom function each time it is queried. The reader sends the pseudonym to a Trusted Centre, that decodes it and return the identity to the reader. The solution assumes the readers are authenticated to the Trusted Centre, avoiding the trivial scenario where false readers asks for pseudonym decoding. It allows *time-limited delegation* in the sense that the RFID reader can decode the pseudonyms for a limited time without any help from the Trusted Centre and *ownership transfer*, which allows the owner of the tag to change in time, while the old owner should not have access to read the tag anymore.

4.2 Key search

We can construct private identification crypto-protocols that make computational trade-offs between directly and indirectly revealing identifying bits, somewhat similar to the computational puzzle work idea used elsewhere. Here we describe what is called the *key search* solution, which is straightforward. In the simplest settings, the subscriber S_i randomly selects a value r_j and encrypts it under his private key, then sends the value and its encryption to the provider. $\mathcal{P}$ searches the full set of keys until it finds one that successfully decrypts to r_j. If the registration is correctly defined, then the keys are all distinct and there is a single one that correctly decrypts to r_j. The subscriber is identified in linear time in the number of the subscribers, so this is not a feasible practical solution for large sets of subscribers. Also, the only advantage of $\mathcal{P}$ over an adversary $\mathcal{A}$ is that it knows the set of keys that belong to subscribers, while the adversary has to perform a brute force attack on the whole set of possible keys. Correctly parametrisation hence implies that the set of all possible keys must be chosen considerable larger than the set of subscribers. To avoid replay attacks and possible impersonations of the user by the adversary, the value r_j must differ for each session, but this verification is costly and not so easy to perform in practice.


Key search
Subscriber S_i
Provider $\mathcal{P}$
$r_j \leftarrow^R \mathcal{R}$
$r_j, Enc_{K_i}(r_j)$
Try all $\{K_i\}$ until it succ. decrypts to r_j
Output: (S_i, K_i)

Weis et al. are the first to introduce this solution, in a slightly different version: instead of encryption, they use a hash of S_i concatenated to a random value [34]. Similar proposals improve search complexity, but with the cost of diminishing security properties, assuming special dependencies between the keys of the subscribers or space-time trade-off. Juels resumes and classifies previous work on RFID private identification as trade-offs to the key search solutions, in 3 types: (1) tree-based solutions; (2) synchronization-based solutions; (3) time-space trade-off approach [18]. Tree-based solutions improve the search complexity from linear to logarithmic in the number of subscribers. One example of such a scheme was introduced for RFIDs by Dimitroiu [35]. An immediate drawback of the solution is its incompatibility to existing architecture in the sense that it can only be applied to systems that comply with the special structure of the pre-shared secrets to allow tree modelling. The synchronisation approach assumes at most a Δ desynchronization between a counter maintained both on the subscriber and the provider side, while the time-space trade-off approach is defined in the natural sense of precomputed tables.

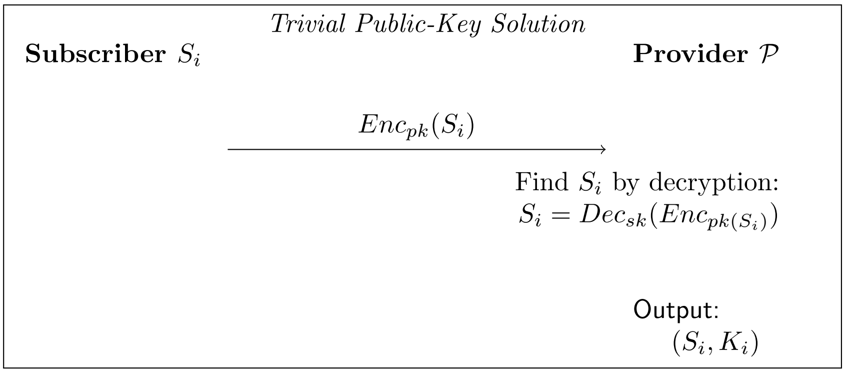
All these proposals have been introduced as candidates for private identification protocols in RFID systems. Existing surveys give a good overview of the proposed solutions and their limitations [18, 19]. None of these proposals can be considered a practical solution to the private identification problem in general, or to the mobile communication systems in particular, without important changes in the architecture of the network or the USIM cards.

4.3 Public-key solutions

Mutual authentication can impose that a subscriber will not identity itself to the provider until the provider authenticates itself first. There are many settings were this is natural: the mobile operator authenticates to the subscriber, the web bank authenticates to the customer, the roadside equipment authenticates the tag in a toll road setting, the payee/shop authenticates to the payer/customer. Public-key cryptography offers an elegant and trivial solution for authentication. Suppose (pk, sk) the public-private key pair of the provider $\mathcal{P}$. Then, the subscriber can simply send its identity encrypted under the public key of $\mathcal{P}$. The solution assumes that the cryptosystem is CCA-secure and the public key of $\mathcal{P}$ is certified in a PKI (Public Key Infrastructure), which makes it not compliant to the existing infrastructure. This is the case of LTE, where 3GPP rejected such a solution, assuming a breach in the security of the system:

> *[...] the only effective means seemed to be the use by the UE [User Equipment] of public key certificates. [...] While this would be possible in theory, 3GPP felt that mandating such an infrastructure would be too high a price to pay.* [36]

Although 3GPP denied to accept it as a viable solution for LTE, public-key cryptography is considered feasible for the intelligent transport systems [37].



Trivial Public-Key Solution

Subscriber S_i — **Provider** $\mathcal{P}$

$$\xrightarrow{Enc_{pk}(S_i)}$$

Find S_i by decryption:
$S_i = Dec_{sk}(Enc_{pk(S_i)})$

Output:
(S_i, K_i)

Abadi and Fournet proposed two protocols that use the idea of public key encryption, but in a more complicated form, aiming to achieve also authentication of the parties [9]. Their solution is too complicated for our purpose here. The standard use of TSL/SSL on the web, with server certificate, and client then communicating within a cryptographic secured channel is an instantiation of the solution. By using a TLS / SSL connection, a subscriber avoids sending its identity in cleartext and he only communicates the identity in encrypted form [9].

Note that protocols proved secure in RFID privacy models are based on public key cryptography (e.g. the protocol of Hermans et al. [10]). Similar constructions exist in the settings of the mobile communication network, where the IMSI is sent encrypted under the public key of the network provider, which can be stored in the USIM. An example includes the work of Arapinis et al., that uses lightweight public key cryptography [38].

Chandrasekaran and Subramanian describe a decentralised PKI that eliminates the need of a CA (Certified Authority) by allowing each subscriber to prove its identity to others by mutual trust [39]. They introduce SMI (Secure Mobile Identities), a protocol in which each participant generates its own identity that is certified its uniqueness and credibility based to different cryptographic primitives such as key exchange, zero-knowledge poof of knowledge [39,40]. However, their solution is not applicable to our problem, as they aim to establish end-to-end solutions between subscribers, and it is not clear at all how it could be applied to identify a UE to the network. Their solution was implemented and tested for end-to-end encryption scenarios very different from our scope, such as secure messaging, secure image transfer or transactions [40].

5 Conclusions and open problems

Existing proposals to the private identification challenge suffer from one or several drawbacks: (1) necessity of changes in the architecture of the systems; (2) significant modifications to the protocols and the exchanged messages; (3) high computational costs and difficult management caused by public key cryptography; (4) particularity to specific scenarios and impossibility to generalise.

Up the now there is no symmetric-key solution to achieve all security requirements compared to the ones based on public-key cryptography, which in reverse are cost expensive and inappropriate for the existing architectures. Lightweight solutions must be sought because of the demanding practical conditions: efficiency in time and computation, simplicity in implementing, compliance to the existence architecture or backup compatibility.

Future research directions in the public key settings include changes in the architecture of the network to accommodate PKI, or even elimination of the certificate authorities, by usage of CertificateLess public-key cryptography (CL-PKC).

References

1. EUDirective: Directive 2002/58/EC of the European Parliament and of the Council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications). `http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_en.pdf` (2002)
2. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European Data Protection: Coming of Age. (2013) 3–32
3. Mjølsnes, S.F., Olimid, R.F.: Easy 4G/LTE IMSI Catchers for Non-Programmers. In: Computer Network Security - 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017. (2017) 235–246
4. Mjølsnes, S.F., Olimid, R.F. In: Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT. (2017) 507–512
5. Shaik, A., Seifert, J., Borgaonkar, R., Asokan, N., Niemi, V.: Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In:

23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. (2016)
6. Jover, R.P.: Security attacks against the availability of LTE mobility networks: Overview and research directions. In: Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on, IEEE (2013) 1–9
7. Lichtman, M., Jover, R.P., Labib, M., Rao, R., Marojevic, V., Reed, J.H.: LTE/LTE-a jamming, spoofing, and sniffing: threat assessment and mitigation. IEEE Communications Magazine **54**(4) (2016) 54–61
8. ETSI TS 133 401 V10.3.0 (2012-07): Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 10.3.0 Release 10) (2012)
9. Abadi, M., Fournet, C.: Private authentication. Theor. Comput. Sci. **322**(3) (2004) 427–476
10. Hermans, J., Peeters, R., Preneel, B.: Proper RFID privacy: Model and protocols. IEEE Trans. Mob. Comput. **13**(12) (2014) 2888–2902
11. Vaudenay, S.: On privacy models for RFID. In: Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings. (2007) 68–87
12. Canard, S., Coisel, I., Etrog, J., Girault, M.: Privacy-preserving RFID systems: Model and constructions. IACR Cryptology ePrint Archive **2010** (2010) 405
13. Yang, X., Xu, C., Li, C.: A privacy model for RFID tag ownership transfer. Security and Communication Networks **2017** (2017)
14. Ensure, G.: 5G enablers for network and system security and resilience (2017)
15. Research, C.C., Service), D.I.: PRIME: Privacy and identity management for Europe. `http://cordis.europa.eu/project/rcn/71383_en.html` (2004)
16. PrimeLife: Bringing sustainable privacy and identity management to future networks and services. `http://primelife.ercim.eu/` (2011)
17. IBM Research: Identity mixer - a cryptographic algorithm to protect your privacy. `http://www.research.ibm.com/labs/zurich/idemix/index.html`
18. Juels, A.: RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications **24**(2) (2006) 381–394
19. Langheinrich, M.: A survey of RFID privacy approaches. Personal and Ubiquitous Computing **13**(6) (2009) 413–421
20. Ramadan, M., Du, G., Li, F., Xu, C.: A survey of public key infrastructure-based security for mobile communication systems. Symmetry **8**(9) (2016) 85
21. Kasper, T., Oswald, D., Paar, C.: New methods for cost-effective side-channel attacks on cryptographic RFIDs. In: Workshop on RFID Security, Citeseer (2009)
22. Camenisch, J., shelat, a., Sommer, D., Fischer-Hübner, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., Tseng, J.: Privacy and identity management for everyone. In: Proceedings of the 2005 Workshop on Digital Identity Management. DIM '05, New York, NY, USA, ACM (2005) 20–27
23. ETSI TS 133 102 V8.7.0 (2015-01): Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 version 8.7.0 Release 8) (2015)
24. ETSI TS 123 003 V10.5.0 (2012-04): Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.5.0 Release 10) (2012)
25. Arapinis, M., Mancini, L.I., Ritter, E., Ryan, M.: Privacy through pseudonymity in mobile telephony systems. In: 21st Annual Network and Distributed System

Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014. (2014)

26. Kesdogan, D., Reichl, P., Junghärtchen, K.: Distributed temporary pseudonyms: A new approach for protecting location information in mobile communication networks. In: Computer Security - ESORICS 98, 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, September 16-18, 1998, Proceedings. (1998) 295–312
27. Khan, M.S.A., Mitchell, C.J.: Improving air interface user privacy in mobile telephony. In: Security Standardisation Research - Second International Conference, SSR 2015, Tokyo, Japan, December 15-16, 2015, Proceedings. (2015) 165–184
28. Choudhury, H., Roychoudhury, B., Saikia, D.K.: Enhancing user identity privacy in LTE. In: 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2012, Liverpool, United Kingdom, June 25-27, 2012. (2012) 949–957
29. van den Broek, F., Verdult, R., de Ruiter, J.: Defeating IMSI catchers. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015. (2015) 340–351
30. Muthana, A.A., Saeed, M.M.: Analysis of user identity privacy in LTE and proposed solution. International Journal of Computer Network and Information Security **9**(1) (2017) 54
31. Song, B., Mitchell, C.J.: Scalable RFID pseudonym protocol. In: Third International Conference on Network and System Security, NSS 2009, Gold Coast, Queensland, Australia, October 19-21, 2009. (2009) 216–224
32. Song, B., Mitchell, C.J.: Scalable RFID security protocols supporting tag ownership transfer. Computer Communications **34**(4) (2011) 556–566
33. Molnar, D., Soppera, A., Wagner, D.: A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In: Proceedings of the 12th International Conference on Selected Areas in Cryptography. SAC'05, Berlin, Heidelberg, Springer-Verlag (2006) 276–290
34. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. In: Security in Pervasive Computing, First International Conference, Boppard, Germany, March 12-14, 2003, Revised Papers. (2003) 201–212
35. Dimitriou, T.: A secure and efficient RFID protocol that could make big brother (partially) obsolete. In: 4th IEEE International Conference on Pervasive Computing and Communications (PerCom 2006), 13-17 March 2006, Pisa, Italy. (2006) 269–275
36. Forsberg, D., Horn, G., Moeller, W.D., Niemi, V.: LTE security. John Wiley & Sons (2012)
37. ETSI TS 102 942 V1.1.1 (2012-06): Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management (2012)
38. Arapinis, M., Mancini, L.I., Ritter, E., Ryan, M., Golde, N., Redon, K., Borgaonkar, R.: New privacy issues in mobile telephony: fix and verification. In: the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012. (2012) 205–216
39. Chandrasekaran, V., Subramanian, L.: A decentralized PKI in A mobile ecosystem. IACR Cryptology ePrint Archive **2017** (2017) 28
40. Chandrasekaran, V., Amjad, F., Sharma, A., Subramanian, L.: Secure mobile identities. CoRR **abs/1604.04667** (2016)