Security and Privacy in Identification and Mobile Payments

Manuel Rego
manuel.rego@ist.utl.pt

Instituto Superior Tecnico
Av. Prof. Dr. Anibal Cavaco Silva
Oeiras, Portugal

Abstract. Based on proliferation of mobile telecommunications technology, the interest on Mobile Payments as an alternative to traditional payment methods such as cash, check or credit cards has been raising significantly on the last few years as evidenced by the interest of mobile communication companies, financial institutions and Internet powerhouses like Google on the development of such systems.
The objective of this work is the development of an off-line untraceable and compact Mobile Payment system implemented on a secure and anonymous compact E-cash scheme. This system was designed designed with the foremost concern for Security, Privacy, retaining the Privacy of Users at all times during normal usage, while simultaneously allowing for efficient and indisputable identification of double-spenders. Another major concern was the Portability of this system to different mediums. To this effect the system relies on a modulated architecture, allowing for the system to be ported and adapted to distinct systems with different resources at their disposal.
Keywords: Mobile Payments, E-Cash, Security, Privacy, Portability

1 Introduction

Mobile payments allow for new and unforeseen ways of convenience and commerce and are steadily becoming complement to cash, credit and debit cards, and will surely replace them, sooner or later. Testifying for the recent interest in these systems a large number of mobile communication companies, financial institutions and Internet powerhouses like Google are developing, or already have implemented, mobile payment solutions.

This work then proposes a mobile payment system primarily focused in Privacy, offering total anonymity to its Users, while still being able to efficiently and doubtlessly identify those that try to undermine the correct functioning of the system.

With this work we aim to accomplish the development of an off-line untraceable and compact Mobile Payment system implemented on a secure and anonymous compact E-cash scheme, with major concerns on User privacy and the portability of the system to different mediums.

2 Related Work

In this thesis, the current state of the art of Radio Frequency (namely, RFID and NFC) systems is analyzed in order to fully understand their capacities and limitations. The present standing of E-Cash and Mobile payment schemes is also dissected, in order to understand what solutions exist today and the differences between such protocols.

2.1 RFID Systems

An RFID System is composed of the elements: the RFID Tag, the RFID Reader and the Back-end. The *RFID Tag* consists of a small microchip, embedded in an integrated circuit, used for storage and performing simple logical operations, an antenna, and a connection between both components. RFID Tags can be divided into 3 main categories: *Passive*, when there is no form of power supply in the Tag; *Semi-Passive*, when a battery is used to boost response signal; and *Active*, when a battery is used to allow advanced processing abilities and/or to increase range and autonomy of the Tag. *RFID Readers* consist of a radio frequency module, a control unit and a coupling element to interrogate electronic Tags via radio frequency communication [8], most of them including some internal storage and processing power. They are deployed in strategic locations where the data from the Transponders needs to be read, e.g., in public transportation. Transceivers continuously emit an interrogation signal, creating a zone within which the Transponders can be read. The area of this zone is dependent on both Reader and Tag characteristics.

2.2 Near Field Communication

NFC, like RFID, is a short-range, standards-based wireless connectivity technology, employing magnetic field induction to enable communication between electronic devices in close proximity. Unlike RFID, however, which is based in a fixed reader-tag structure, an NFC device is able to impersonate two different roles, *initiator* or *target* with the NFC communication protocol being based on a message and reply concept. An NFC system can also operate in two distinct modes of communication, active and passive, similar to the ones of RFID Systems. These modes and roles of NFC systems can be mingled, with the exception of the combination of Initiator and Passive.

2.3 RF Security and Privacy

Having analyzed the characteristics and architecture of RFID and NFC systems, the most important characteristic of these systems is yet to be mentioned. Unlike bar-code technology that preceded it, RF devices have the ability to be read without line-of-sight contact and without precise positioning [5]. While easy to infer, because the RF systems are based on wireless communication, this *detail*

is what gives RF most of its utility. One can easily picture how much the logistics and other everyday usage can improve by upgrading from Bar-codes, that require optical scanning and thus careful positioning of the scanned objects, to RFID and NFC systems, that can be read much faster, from greater distances and without such concerns. The flip-side of this is that by not requiring line-of-sight, systems can be read without any evidence, creating a range of privacy threats from unauthorized data access, to snooping on communications between devices, and location tracking of physical objects and their association with people. This translates into the urgent need to seriously consider Security and Privacy issues in the development any RF system.

2.4 RF Security Threats

Besides the privacy issues detailed before, RFID and NFC systems are based on an Air Interface, and, as such, are liable to a number of attacks. Unlike RFID, where the Tag is, in most cases a very low cost device, in NFC the system (or part of it) is often embedded in a device which has moderate to high value. *Physical attacks*, such as the system host being stolen and/or destroyed, must then be considered in the development of any solution using those systems. Not only the losses can be far greater (e.g. a rogue user gaining access to a mobile payment system connected to a user's bank account), but also because as the device itself is valuable it becomes more prone to arouse the interest of others. Regarding the *Air Interface*, the already mentioned contactless nature of RF devices can allow for a number of different types of attack, such as Denial of Service (DDOS), Eavesdropping and Man in the Middle.

2.5 Mobile Payments

Mobile payments, defined by Karnouskos et al. [6] as any payment where a mobile device is used in order to initiate, activate, and/or confirm this payment. These mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to mobile telecommunication network and make it possible for payments to be made.

Mobile payments may be classified based on a number of criteria, namely the Interaction type (Remote and Proximity payments), Basis of payment (Account based or Wallet based) and transaction type (On-line, Off-line or Semi-Offline).

3 E-Cash

Conceived by Chaum in the beginning of the Eighties [2], electronic cash has been wide and extensively studied ever since by numerous authors. The core idea behind the concept being that while an entity , e.g., a bank, is responsible for distributing coins and afterwards collecting or receiving them for deposit, the withdrawal and spending protocols are designed in such a way that makes it impossible to identify when one particular coin was spent, i.e., making any

tracing or identification of the spender impossible. That is, of course, unless any user double-spends a token, which is a problem in the electronic world due to the easiness in duplicating data, in which case the scheme must allow for the revokement of the anonymity of the rogue user. Merchants must also be prevented from depositing the same token more than once.

Most E-Cash schemes are said to be *divisible*, which means that users can withdraw coins of 2^L value and spend said coin in several transactions, by dividing the value of the coin, allowing users to efficiently spend a coin of monetary value 2^l, with $0 \leq l \leq L$, i.e., much more efficiently than repeating a spending protocol 2^l times. [7].

4 Camenish Compact E-Cash Scheme

Camenish et. al, on the other hand, proposed a secure *off-line* anonymous compact E-Cash scheme [1] aimed to address the efficiency issue in a concise use of resources. This scheme, allows a user to withdraw a wallet with 2^l coins, such that the space required to store these coins, and the complexity of the withdrawal protocol, are proportional to l, rather than to 2^l.

As such, in this proposal, a wallet containing k coins can be withdrawn and spent with $O(l + k)$ complexity, while the it also takes $O(l + k)$ to store all the coins, based on the *Strong RSA Assumption* [4] and the *Decisional Diffe-Hellman Inversion*(y-DDHI) [3] assumptions in the random-oracle model.

4.1 E-cash Primitives

Having presented the all the building blocks, we shall now enumerate, characterize and describe the main protocols used to implement the E-cash scheme designed by Camenish et. al [1].

Withdraw ($U(pk_B,sk_U,n)$, $B(pk_U,sk_B,n)$) - In this protocol the user U withdraws a wallet W of n coins from the bank B. The user's output is the wallet W, or an error message. B's output is some information T_W which will allow the bank to trace the user should this user double-spend some coin, or an error message.

Spend ($U(W, pk_M)$,$M(sk_M, pk_B, n)$) - A user U gives one of the coins from his wallet W to the merchant M. Here, the merchant obtains a serial number S of the coin, and a proof π of validity of the coin. The user's output is an updated wallet W'.

Deposit ($M(sk_M, S, p, pk_B)$, $B(pk_M, sk_B)$) - A merchant M sends to bank B a coin (S,π=(R,T,ϕ)). If ϕ verifies and R is fresh (i.e. the pair *(S,R)* is not already in the list L of spent coins), then B accepts the coin for deposit, adds (S,π) to the list L of spent coins, and credits the account of pk_M; otherwise, B sends M an error message.

Identify (*params*, S, π_1, π_1) - This algorithm allows to identify double-spenders using a serial number S and two proofs of validity of this coin, π_1 and π_2, possibly submitted by malicious merchants. This algorithm outputs a public key pk_U and a proof Π_G.

4.2 Pseudo-random Function

Another of the fundamental building blocks of the proposed E-Cash system are the pseudo-random functions proposed by Dodis and Yampolskiy [3]. For every n, a function $f \in F_n$ is defined by the tuple (G,q,g,s), where G is a group of order q, q is an n-bit prime, g is a generator of G and s is a seed (i.e. a random element) in $\mathbb{Z}_q$. For any input $x \in \mathbb{Z}_q$ (except for x=-1 mod q), the function $f_{G,q,g,s}()$, which we simply denote as $f_{g,s}^{DY}(?)$ for fixed values of (G,q,g), is defined as:

$$f_{g,s}^{DY}(x) = g^{1/(s+x+1)} \tag{1}$$

4.3 CL Signatures

In order for the E-Cash system to accomplish the identification of double-spenders without comprimising the privacy of legitimate users, Camenisch et al. devised a secure signature scheme based in the Pedersen commitment scheme. This Pedersen commitment requires that, in order to commit the values $(v_1, ...v_m) \in \mathbb{Z}_q^m$, one should pick a random $r \in \mathbb{Z}_q$, define g_0 and g_i as the generators of group G and set:

$$C = PedCom(v_1, ..., v_m; r) = g_0^r \prod_{i=1}^{m} g_i^{vi} \tag{2}$$

This effort by Camenisch and Lysyanskaya resulted in a secure signature scheme with two protocols: an efficient *signature* protocol between a user and a signer with keys and an efficient *proof of knowledge* of a signature protocol between a user and a verifier.

4.4 Coin Generation

As mentioned before, one of the advantages of the E-Cash scheme used in our solution lies in its efficiency. As such, one of the goals of the scheme is to adapt single-use electronic cash schemes so that a coin can be used at most 2^l times. The trivial solution would be to obtain 2^l coins. However, this would be inefficient since 2^l may be quite large (e.g., 1024), therefore undermining the performance,of the scheme.

The idea underlying our system is that the values s and t implicitly define several (pseudo-random) serial numbers S_i and blinding values B_i, respectively. The user then gets 2^l pseudo-random serial numbers with the corresponding

double-spending equations defined by (s, t). Here, the double-spending equation for coin i is:

$$T_i = g^{sk_U}(B_i)^R \tag{3}$$

With R being chosen by the merchant. This leaves us with a very specific technical problem. The challenge is to find a pseudo-random function such that, given a commitment to (skU, s, t), a commitment to i and the values S_i and T_i, the user can efficiently prove that she derived the values S_i and T_i, correctly from sk_U, s, and t, i.e. $S_i = F_s(i)$ and $T_i = g^{sk_U}$.

4.5 Double-Spending Identification

Following the steps of the coin generation, if S_i and T_i are computed through the above mentioned constructions they are members of G rather than of $\mathbb{Z}_q$. This leaves us with the following protocol: to withdraw a coin, a user obtains a signature on (sk_U, s, t).

During the spending protocol, the user reveals S_i and the result of the double-spending Equation 3 where sk_U is the user's secret key and $pk_U = g^{sk_U}$ the corresponding public key. Now, with two double-spending equations (T2 and T1) for the same coin, we can infer the following:

$$\left(\frac{T_2^{R_1}}{T_1^{R_2}}\right)^{(R_1-R_2)^{-1}} = \left(\frac{g^{uR_1+R_1R_2\alpha}}{g^{uR_2+R_1R_2\alpha}}\right)^{(R1-R2)^{-1}} = g^{\frac{u(R1-R2)}{(R1-R2)}} = g^u = pk_U \tag{4}$$

The result of the calculation of the two double-spending equations is pk_U, the public key of the User that has double-spent, sufficient proof for identification of said user.

5 Architecture and Implementation

The main goal of this work is to offer users an efficient mobile payment system that assures user privacy at all times and that, while designed to be used on an NFC enabled system, it is capable of fitting smoothly with existing systems, offering *interoperability* without the need of costly hardware updates, while at the same time being portable to related systems (e.g. Java Cards) and/or different wireless means (e.g. Wi-Fi, Bluetooth).

We accomplished this through the implementation of the off-line divisible and unlinkable electronic cash scheme, presented in Section 3, embedded in a multi-layered architecture, with independent *Security* and *Communication* modules, as depicted in Fig. 1. This architecture enables implementation in a vast array of platforms, with more or less computing capacities, because these modules can be moved around the system (e.g. in a system with very limited resources, most security related computing can be moved to the back-end structure).

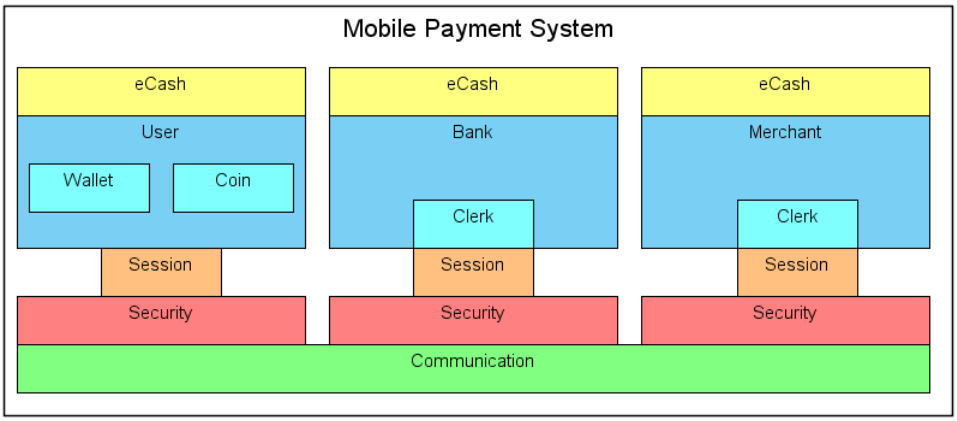

Fig. 1. Overview of System Architecture

The proposed system considers the three main actors, namely: User, Bank and Merchant. These actors perform distinct roles in the system while sharing the architecture that bonds them together, namely the Security and Communication modules.

The Security module is responsible for all the encryption and authentication procedures necessary for the secure functioning of the system. The Communication module handles the establishment of the connection between Agents and the subsequent transmission of messages, in the most transparent way possible. Lastly, the E-Cash module comprehends the operations necessary to the implementation of the compact E-Cash presented in Section 3, namely the Pedersen Commitment, the CL signature and the Pseudo Random Function.

According to the above motivations, the solution was implemented in Java, a programming language notorious for its portability.

6 Results

In order to infer the feasibility and usability of the proposed solution a prototype version was implemented in Java. This prototype was then evaluated using a Smartphone, holding the User's side application, and Laptop computer, running the Bank and the Merchant. This assessment comprehended both an analysis of the resource and time consuming initialization of the system, followed by diverse takes on the Withdraw, Deposit and Spending protocols.

6.1 System Initialization

These tests included the generation of the RSA Key Pair necessary to the establishment of a secure communication channel and the Group generation required for the operation of the E-Cash system. The Key Pair generation was fond to be

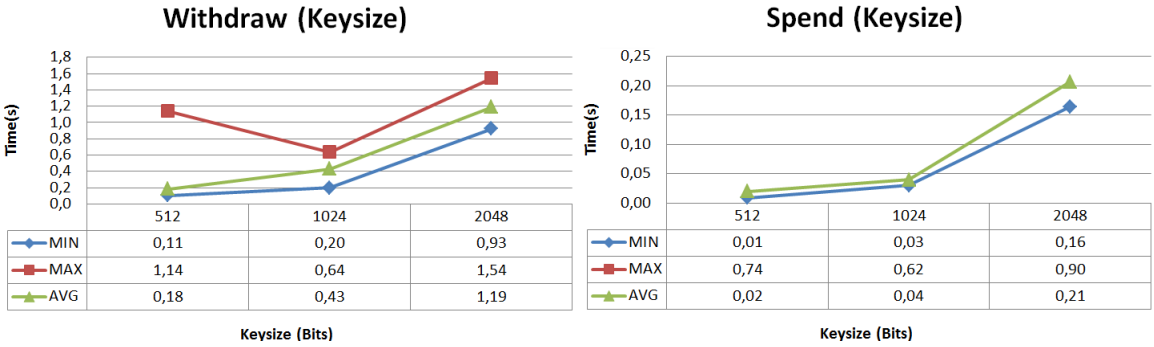

Fig. 2. Evaluation of Group Generation and Spending protocols

possible to implement in a Smartphone, even if they would be required to run as background processes in order to improve security in a in a transparent way to the user and without impairing system usability. The execution of the Group Generation, on the other hand, proved to be too computationally heavy for a mobile system. This would be addressed by having the Back-Office handling the processing and forwarding the results to the User as they were necessary.

6.2 Protocols

Various tests were run on the main protocols of the system: Withdraw, Spend and Deposit. Results were found, expectedly, to increase as the choice in the Keysize used to encode the communication was increased. Further testing, however, showed that it was precisely the encrypting and decrypting of the data generated in these protocols. Nevertheless, it was concluded that, upon reaching a compromise on the Security of the system and the execution time of each protocol, it was feasible for such a system to be ran on a mobile device.

6.3 System Portability

The Mobile Payment system developed in this thesis was designed in a module interface with sights set on offering as much portability and interoperability as possible. Adding to this the research conducted on RF technology it is then possible to analyze and present various directions and systems in which the presented system could be applied and implemented in the future.

6.3.1 Hardware Being the base used in the development of our proof of concept solution and seeing that in a short period of time they will become the *natural habitat* for mobile payment systems, *Smartphones* are the most obvious recipient for the system presented in this thesis. A smartphone implementation of our scheme should be able to independently handle all the components necessary to grant the functionality required for the User role.

Using a Java Card for our Mobile Payment system would translate in the possibility of all of the Users details to be held in the card itself, rather than the Back Office, since Java Cards have a considerable amount data storage space and, more notably, the capacity to independently generate (and hold) a full RSA Key Pair. Most, if not all, the eCash computation, however, hold have to be produced in the Back-Office, since it is way beyond the capabilities of a Java Card.

As per our extensive analysis of this medium, it has been established that the processing capabilities of RFID Tags are very limited. As such, the adaptation of our proposed solution to comprehend the usage of RFID would require all computation and most of the characteristics of the User to be held by the Back Office.

6.3.2 Wireless Technologies A solution based on *Wi-Fi*, like the one developed in the presented prototype, could benefit from the ubiquity of Wi-Fi, while the reduction on the range of the Wi-Fi Hotspots would create smaller areas on which the mobile payment system could be used.

With the early versions of Bluetooth communication allowing data rates of up to 1 and 3 Mbits/s (version 1.2 and 2.0, respectively). Taking into account the results obtained in Section 6.2, we consider that the throughput capacity of Bluetooth is completely able to deal with the amounts of data required for the communication in our proposed E-Cash system.

On NFC, as we noted in Section 2.2, allows for throught put rate of up to 424kbits/s. While being sufficient for the initial establishment of the communication (i.e. the exchange of Public Keys between Agent and Service, the role assertion and the Challenge-response protocol), this procedure should to be prompted to the User as a preamble to the Withdraw and Spend protocols, in order to reduce apearance of time needed to accomplish the protocols. The Withdraw and Spend protocols, on the other hand, as noted in Section 6.2 require an amount of data throughtput that NFC would never be able to handle. There are two general possible workarounds for this issue: the Withdraw and Spend protocols could be ran mostly via the Back Office, with the NFC device contributing only with the data required for the calculations (i.e. group generators, group elements); alternatively, the NFC platform could be used to expedite the establishment of the communication via a more capable connection, such as Wi-Fi or Bluetooth.

6.4 System Evaluation

The presented solution is meant to be the groundwork for a Mobile Payment system, rather than a system meant to be produced and pushed to end-Users. As such, the interface itself inspired little consideration seeing that the concretization of it could be done in a system with substantially different characteristics (e.g. an Apple device with very strict regulations on the interface system) or with no interface whatsoever (e.g. a Java Card or an RFID Tag).

Even so, some inquiries were realized that could render useful insight into the user expectations for this kind of systems. In these queries, while not adding to a large amount of individuals, we managed to target a wide range of the population that would use these systems, with the age of said individuals ranging from 20 to 50 years old.

6.5 Interface considerations

While the interface on the presented solution was far from a final product, a usage test was still realized. Due to said lack of development on the interface it is impossible to provide any accurate metrics. However, feedback gathered from users still provided some interesting insights into concerns that should be held in interface design for such systems.

7 Conclusions

With the current interest in Mobile Payments by big companies such as mobile communication companies, financial institutions and Internet powerhouses like Google this area will undoubtedly experience a very intense development in a short term perspective. However, while the systems developed by these companies will surely be proficient and able to offer Users the advantages of replacing physical currency by a digital medium, it is very unlikely that User Privacy will be a concern.

Our solution, on the other hand, goes against the grain in the setting of User Privacy as a main priority. While it effectively deems the system mostly invaluable for any company we firmly believe that this is the right thing to do, especially in this period in History were personal Privacy is turning from a fundamental right into a mirage.

References

1. J. Camenisch and S. Hohenberger. Compact e-cash. *Science*, 2005.
2. D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto*, volume 82, pages 199–203, 1983.
3. Y. Dodis and A. Yampolskiy. A Verifiable Random Function with Short Proofs an Keys. *Public Key Cryptography*, 2005.
4. E. Fujisaki and O. Tatsuaki. Statistical zero knowledge protocols to prove modular polynomial relations. *Advances in Cryptology CRYPTO 97*, 1997.
5. A. Juels, P. Syverson, and D. Bailey. High-power proxies for enhancing RFID privacy and utility. In *Privacy Enhancing Technologies*, pages 210–226. Springer, 2006.
6. S. Karnouskos and F. Fokus. Mobile payment: a journey through existing procedures and standardization initiatives. *Communications Surveys & Tutorials, IEEE*, pages 44–66, 2004.
7. T Okamoto. An efficient divisible electronic cash scheme. *Advances in Cryptology - CRYPTO 95*, 1995.
8. S. Sarma, S. Weis, and D. Engels. RFID systems and security and privacy implications. *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 1–19, 2003.