Designated Attribute-Based Proofs for RFID Applications*

Gergely Alpár[1,2], Lejla Batina[1,3], and Wouter Lueks[1,2]

[1] Radboud University Nijmegen, ICIS/Digital Security group
Heyendaalseweg 135, 6525 AJ Nijmegen, The Netherlands
{gergely, lejla, w.lueks}@cs.ru.nl
[2] TNO Information and Communication Technology, The Netherlands
[3] K.U.Leuven ESAT/SCD-COSIC and IBBT
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
lejla.batina@esat.kuleuven.be

Abstract. Recent research has shown that using public-key cryptography in order to meet privacy requirements for RFID tags is not only necessary, but also now practically feasible. This has led to the development of new protocols like the Randomized Schnorr [6] identification protocol. This protocol ensures that the identity of a tag only becomes known to authorised readers.
In this paper we generalize this protocol by introducing an attribute-based identification scheme. The proposed scheme preserves the designation of verification (i.e., only an authorised reader is able to learn the identity of a tag) while it allows tags to prove any subset of their attributes to authorised readers. The proposed scheme is proven to be secure and narrow-strong private.

Keywords: RFID, identification, authentication, elliptic curve cryptography, security, privacy, attribute-based credential

1 Introduction

We rely on the security of embedded systems in our daily lives when using, e.g., public transportation, mobile phones, e-banking applications and pay TV systems. Typically, these systems are implemented using smart cards and Radio Frequency IDentification (RFID) tags that are extremely limited in resources such as area, memory and power consumption. As a result of these limitations, ensuring security and privacy in RFID systems is one of the most difficult challenges today.

Recently, with the development of privacy-sensitive RFID services the attention of the research community has yet again returned to Public-Key Cryptography (PKC) for RFID systems. The main reason is the need to give the users more privacy, but other properties such as scalability and anti-counterfeiting are also very important. Although critics still consider public-key systems too expensive for passive tags, a number of companies and academic groups have already designed PKC-based chips

* To be published in **RFIDsec 2012**, Nijmegen, The Netherlands, July 1-3, 2012, Revised Selected Papers. Springer 2012 LNCS

for RFID protocols [5, 10, 11]. While the first performance results are promising, the design of new PKC-based protocols is necessary to get viable solutions. One of the reasons for this is that standard solutions for authentication, e.g., signatures, typically require a hash function as well, which adds additional burden in terms of gates and power consumption.

Elliptic Curve Cryptography (ECC) has typically been the preferred setting for creating PKC-based protocol. Numerous protocols were designed aiming at security and privacy of RFID systems based (exclusively) on the Elliptic Curve (EC) point multiplication [6, 15]. Starting from an authentication of a single tag, a number of more complex protocols emerged such as grouping proofs [13] and hierarchical proofs [1]. It has become obvious that this trend will continue as lightweight cryptography is turning into the main component of modern communication networks and new applications are ever emerging.

Attribute-based credentials[1] (ABCs) in combination with selective disclosure can be used to solve many of the existing privacy problems. Furthermore, showing an ABC does not require more exponentiations on the tag's side than some other protocols demonstrated to be computationally feasible on RFID chips [1, 3]. We demonstrate how RFID systems can benefit from the concepts of ABCs in such a way that a tag proves all or a subset of its secret attributes to designated verifier readers. Our protocols are proved to be secure against impersonation attacks and narrow-strong private.

1.1 Related work

The discrete logarithm (DL) problem is considered to be hard[2], that is, finding the exponent a of a random point $A = aP$ with respect to a publicly-known base point P is computationally infeasible [14]. A related hard problem can be stated with respect to more base points: in the discrete logarithm representation (DL-REP) problem, introduced by Brands [4] and employed in Microsoft's U-Prove technology [16], given a random point A and base points $P_0, \ldots, P_l$ one has to find exponents $a_0, \ldots, a_l$ such that $A = \sum_0^l a_i P_i$. While in a DL problem the exponent a is uniquely determined, in a DL-REP problem there are several tuples $(a'_0, \ldots, a'_l)$ for which $A = \sum_0^l a'_i P_i$.

Zero-knowledge proofs of knowledge are cryptographic techniques to prove the knowledge of a secret value without revealing any information about the secret itself. Schnorr [18] proposed an interactive protocol that enables a prover to show the knowledge of a DL value to a verifier, that is, a secret scalar corresponding to a public point. A similar method by Brands [4] can be applied to prove the knowledge of a DL-REP of a point with respect to a tuple of base points. A prover can also reveal a subset of scalars in a DL-REP while only proving knowledge about the others; this procedure is called *selective disclosure* which is one of the most relevant functionalities in relation to ABCs [7].

[1] Attribute-based credential: (aka. anonymous credentials) An ABC is a composite commitment that carries multiple values, so-called attributes, and signed by a trusted authority; in this paper the signing is ignored as the initialization of RFID tags are out of scope of this study.

[2] Although in this paper we discuss schemes in an ECC setting, they work in any groups in which the discrete logarithm problem is hard.

While the techniques above provide a high-degree of security for the prover by not necessarily revealing secret pieces of data, any party interacting with the prover (or eavesdropping) can learn selectively disclosed information. In some scenarios, prior verifier authentication is not possible (i.e., a secure channel cannot be assumed between the prover and the intended verifier) and, therefore, this may not be desirable. In particular, in the context of RFID systems, possibly malicious readers can interrogate RFID tags. *Designated verifier proofs* are proofs of knowledge where only a designated verifier can obtain identity information. Bringer et al. [6] present a scheme that extends a Schnorr identification to a designated verifier proof. Since their technique randomizes the messages for a party that does not know the secret key, they call it the "Randomized Schnorr" scheme.

Restriction of verification has a long history in cryptography. Undeniable signatures have been introduced in 1989 by Chaum and van Antwerpen [9] and have been enhanced to zero-knowledge proofs of ownership by Chaum [8]. An undeniable signature cannot be verified without interacting with its signer. Furthermore, during the proving protocol no external parties learn anything about the validity or invalidity of the signature. Jacobsson et al. [12] propose a more general notion, the designation of verification that a statement is true. The idea is that the prover generates a zero-knowledge proof that can only be produced by him and the verifier. Since the verifier knows that she was not the one who created the proof, she becomes convinced about the validity of the statement; however, she cannot convince any third party that the proof was produced by the prover and not by herself. Saeednia et al. [17] improve the notion of designated verifier signatures, in which not only the verifier but anybody can simulate transcripts of valid proof conversations. They also propose an efficient designated verifier signature using the Fiat–Shamir heuristic.

In the context of RFID schemes, Bringer et al. [6] present a similar but interactive scheme, in which a tag demonstrates its identifier. While the tag proves the knowledge of a secret key, it reveals its identifier only to the designated verifier. Our schemes are also designated verifier proofs. More precisely, we generalize the scheme of Bringer et al., but we allow for multiple attributes. To our best knowledge, we introduce the first designated selective disclosure protocol in which a prover can reveal any subset of attributes but only to a verifier that knows all corresponding secret keys.

1.2 Our contribution

By encoding several attributes as exponents a_i's in a point $A = \sum_0^l a_i P_i$, the number and variety of applications increase considerably. As Lee et al. [15] have shown that multiple point multiplications are feasible on a passive RFID tag, DL-REP related protocols also become realizable in such limited environments. In this paper we propose designated verifier proofs of knowledge of DL-REPs. Furthermore, by applying a new proof technique, a subset of exponents can also be shown to a designated verifier.

Unlike in Brands' selective disclosure schemes, a prover cannot send the revealed exponents in advance or during a protocol run in clear; however, those exponents have to be computable for an eligible verifier. Table 1 shows a summary of these

zero-knowledge proofs. Although a trivial solution to reveal certain attributes would be to send them encrypted to the verifier, this causes significant overhead.

Table 1. Designated proofs of knowledge of discrete logarithm values; highlighted protocols are presented in this paper for the first time.

Problem	**ZK proof**	**Designated ZK proof**
DL	Schnorr [18]	Randomized Schnorr [6]
DL-REP	U-Prove showing [4]	Designated DL-REP proof
DL-REP	U-Prove selective disclosure [4]	Designated partial DL-REP proof

We prove that the proposed designated verifier schemes are zero-knowledge, secure against impersonation, and narrow-strong private. Moreover, we show how these general building blocks can be employed to design secure RFID applications.

The remainder of the paper is organized as follows. First we describe the cryptographic background and relevant protocols in Section 2. Second we introduce the new Designated Verifier DL-REP and Designated Verifier Partial DL-REP proofs in Section 3. Then we study feasibility of our schemes and some possible RFID applications in Section 4. Finally, we conclude the paper in Section 5.

2 Cryptographic Background

An identification scheme is an interactive protocol in which a prover, i.e., a tag in this setting, convinces a verifier that it has the identity it claims to have. Before we introduce our proposal for a designated attribute-based proof system in Section 3, we describe cryptographic requirements and prior relevant protocols.

2.1 Basic set-up

Throughout this paper let E be an elliptic curve defined over a finite field $\mathbb{F}_{q^k}$, where $q = 2$ or a large prime (in this case $k = 1$). Let $(G, +)$ denote a cyclic group of prime order p of points on the curve E, generated by a point P. The fields of characteristic 2, i.e., when $q = 2$, are more suitable for hardware implementations and hence for RFID tags, but ECC protocols conceptually apply for arbitrary fields.

We use capital letters, like A and P to denote points on the elliptic curve. Scalars are written using lower case letters. We write kP to denote the point P added k times to itself. Finally, we denote by $x \in_R \mathbb{Z}_p$ that x is chosen uniformly at random from the set $\mathbb{Z}_p$.

We use a number of hardness assumptions to prove the security and privacy of our systems. We assume that the following problems are hard[3].

Definition 1 (Discrete Logarithm (DL) problem). *Given a generator $P \in G$ and a multiple $A = aP$ of P, where $a \in_R \mathbb{Z}_p$, determine a.*

[3] We state these assumptions in the ECC setting.

Definition 2 (Decisional Diffie-Hellman (DDH) problem). *Given a generator P, and the points $A = aP$, $B = bP$ and $C = cP$, where $a, b \in_R \mathbb{Z}_p$, determine whether $c = ab$.*

2.2 Security and Privacy model

The protocols we consider are typical authentication protocols. This means that the tag and the reader engage in a protocol, at the end of which the reader will either be convinced about the identity of the tag (and in our case also the validity of the attributes) or it will report failure. In this paper we show that our two new protocols satisfy two different requirements: security and privacy. The former roughly means that it is difficult for an adversary to pretend to be a valid tag, while the latter means that an adversary cannot distinguish legitimate tags from simulated tags.

Just as Bringer et al. [6], we follow the security model proposed by Vaudenay [19]. In his model, Vaudenay describes how adversaries can interact with a set of tags. Besides offering methods for communicating with and choosing from the tags as well as communicating with the reader, the model also exposes two additional oracle calls. The level of access to these two additional oracles defines the type of the adversary.

The first additional oracle is the result-oracle. As it is typical in identification protocols, the reader draws one of the following two conclusions at the end of the protocol. It either concludes that the tag it communicated with has been successfully identified as the tag with identity I, or it reports failure. The result-oracle will return only the success/failure status of the reader. In our protocols we do not allow this type of queries, hence resulting in a *narrow* adversary (as opposed to a *wide* one that is allowed to make such queries).

The second additional oracle is the corruption oracle. This allows the adversary to corrupt a tag, and hence learn all its secrets. We consider only *strong* attackers, i.e., attackers that can obtain the secrets of any tags they choose. In the privacy game, further attacks on the privacy of these tags are allowed afterwards, while they are (of course) explicitly prohibited in the security game.

Given this model we can now give games to define the security model.

Definition 3 (Security game). *Assume that there exists a system of t tags that can be interrogated via the identification protocol, then the game consists of two phases:*

1. *In the first phase, the adversary is allowed to interrogate any tag multiple times. Furthermore, it is allowed to corrupt any tags of its choosing.*
2. *In the second phase, the adversary communicates with the verifier to impersonate one of the uncorrupted tags of the system.*

An RFID scheme is secure if no adversary can win the Security game above with non-negligible probability.

Intuitively, our notion of privacy for these types of protocols means that it is not possible to link two different executions of the protocol. This property is often referred to as unlinkability. In the Vaudenay model it is captured as follows. Even though the adversary is given the identifiers of the tags it talked to at the end of the game, it cannot distinguish between the setting in which it communicates with

actual tags and the setting in which it communicates with simulated tags. Note that in the latter case the simulator didn't know the identifiers. Hence, any information leak on the identifiers can be used by the adversary to gain an advantage. A system has narrow-strong privacy if no adversary can win the following game against a challenger with non-negligible probability.

Definition 4 (Narrow-Strong Privacy Game). *Assume that there exists a system of t tags that can be interrogated via the identification protocol. First, the challenger generates a bit $b \in_R \{0,1\}$ and depending on b, it runs different experiments:*

- *If $b = 0$, the adversary is allowed to directly talk to any tag of its choice.*
- *If $b = 1$, the adversary is not allowed to interrogate tags directly but the challenger, without interacting with the actual tags, simulates them.*

Then in the corruption phase, the adversary can receive all the tag's private information by corrupting it. At the end of the game, the adversary must guess the value of bit b.

Since we are in a strong setting, the challenger can obtain the tags identifiers using the corruption query; therefore, this is not mentioned separately in the game.

2.3 Randomized Schnorr scheme

Bringer et al.'s Randomized Schnorr [6] scheme is secure and narrow-strong private by the definitions above. Each prover (tag) has a secret key x and an identifier $I = xP$, while each verifier has a secret key v and a corresponding (designating) public key $V = vP$. Verifiers store a list of valid tag identifiers.

During a protocol run (see Fig. 1), not only does a tag prove the knowledge of its secret key, but it also hides its identifier from any external party. Using its secret key v, the verifier can compute the tag's identifier. Therefore, the prover's secret key and its identifier are protected: First, as this scheme is a modified Schnorr identification, no adversary can learn anything about the tag's secret key x. Second, without the knowledge of v, no adversary can compute I.

Prover $x, I = xP$	P, $V = vP$	**Verifier** v
$\alpha, \beta \in_R \mathbb{Z}_p$		
$A_1 := \alpha P$		
$A_2 := \beta V$	$\xrightarrow{A_1, A_2}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_p^*$
$r := c \cdot x + \alpha + \beta \pmod p$	$\xrightarrow{r}$	Verification:
		$I = c^{-1}(rP - A_1 - v^{-1}A_2)$
		check whether I is a valid identifier

Fig. 1. Randomized Schnorr [6] identification, i.e., Designated Verifier Schnorr identification. (There are 2 point multiplications on the Prover's side.)

2.4 Discrete logarithm representation (DL-REP)

Discrete logarithm representations [4] were introduced by Brands[4]. Given a set of $l+1$ generators (base points, in case of ECC) $P_0, \ldots, P_l$ in a group, participants can commit to l (attribute) values $x_1, \ldots, x_l$. We say that the DL-REP of I is $(x_0, \ldots, x_l)$ with respect to $(P_0, \ldots, P_l)$ if $I = \sum_0^l x_i P_i$.

While the identifier I (as a cryptographic commitment) hides the attributes $(x_1, \ldots, x_l)$ because of the extra scalar x_0 unconditionally, it binds the prover only computationally. However, this computation is infeasible as any oracle that, after changing some exponents, can compute a new DL-REP $x'_0, \ldots, x'_l$ with respect to the same base points $P_0, \ldots, P_l$ can be used to break the discrete logarithm problem.

In [4] Brands builds an anonymous credential system on commitments in which a credential is a commitment, like I above, (blindly) signed by a credential authority. Using such a credential and zero-knowledge proof techniques, a prover is able to demonstrate to a verifier that she knows the secret values in the commitment without actually showing them. Moreover, a prover can selectively disclose values corresponding to a disclosure index set $\mathcal{D} \subseteq \{1, \ldots, l\}$ (see Fig. 2). Having these values $(x_i)_{i \in \mathcal{D}}$, the verifier can compute a partial commitment $com - \sum_{i \in \mathcal{D}} x_i P_i$ and the prover can prove the knowledge of all other secret values. Note that in case of $\mathcal{D} = \emptyset$, this scheme is a proof of knowledge of all exponents – we will refer to this protocol as *U-Prove showing protocol*.

Prover		**Verifier**
$x_0, \ldots, x_l$	$P_0, \ldots, P_l$, $\mathcal{D}$ $I = \sum_0^l x_i P_i$	
$\alpha_i \in_R \mathbb{Z}_p \; \forall i \notin \mathcal{D}$ $A := \sum_{i \notin \mathcal{D}} \alpha_i P_i$	$\xrightarrow{A}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_p^*$
$\forall i \notin \mathcal{D}: \quad r_i := c \cdot x_i + \alpha_i \pmod p$	$\xrightarrow{(r_i)_{i \notin \mathcal{D}}, (x_i)_{i \in \mathcal{D}}}$	Verification: $A \stackrel{?}{=} \sum_{i \notin \mathcal{D}} r_i P_i$ $\quad -c\left(I - \sum_{i \in \mathcal{D}} x_i P_i\right)$

Fig. 2. Selective disclosure protocol in [4] where attributes (committed values) in $\mathcal{D}$ are disclosed, while for all the others only a proof of knowledge is given. Here l is the number of attributes; d is the size of the disclosure set $\mathcal{D}$, and I is the commitment following the identification notation. (There are $l - d + 1$ point multiplications on the Prover's side.)

3 Designated Verifier DL-REP Proofs

A designated verifier DL-REP proof is an interactive identification protocol in which a prover reveals his unique identifier and at the same time proves knowledge of the

[4] We will often refer to schemes by Brands as U-Prove since basically, they are the main building blocks in Microsoft's U-Prove technology [16].

identifier's DL-REP with respect to points $P_0, \ldots, P_l$ in a way that only the verifier can verify the proof and compute the identifier I. Finally, the verifier checks I in his database that stores all valid tag identifiers. Note that, unlike in the Schnorr proof [18] or the U-Prove showing protocol [4] in which the identifier is a common input value and it is confirmed by the verification equation, only the verifier learns the identifier in this scheme.

Firstly, we show that the Randomized Schnorr scheme can be generalized in a natural way resulting in a secure and narrow-strong designated verifier DL-REP proof. Secondly, we introduce the designated selective disclosure, i.e., a protocol that allows for a Designated Verifier Partial DL-REP proof.

3.1 Designated Verifier DL-REP Proof

Setup

- $\mathsf{SetupSystem}(1^k) \longrightarrow par$ outputs parameters par with the group description and the base points $P_0, \ldots, P_l$.
- $\mathsf{SetupVerifier}(par) \longrightarrow (v, V)$ generates a private/public key pair for the Verifier, where the public key $V = v \cdot \sum_0^l P_i$. If the key pair has already been generated in the system, the algorithm outputs that.
- $\mathsf{SetupTag}(par) \longrightarrow ((x_0, \ldots, x_l), I)$ generates attributes $(x_0, \ldots, x_l)$ and an identifier I for a tag, where the identifier $I = \sum_0^l x_i P_i$.

Prover		**Verifier**
$x_0, \ldots, x_l$	$P_0, \ldots, P_l$	v
$I = \sum_0^l x_i P_i$	$V = v \cdot \sum_0^l P_i$	
$\alpha_0, \ldots, \alpha_l, \beta \in_R \mathbb{Z}_p$		
$A_1 := \sum_0^l \alpha_i P_i$		
$A_2 := \beta V$	$\xrightarrow{A_1, A_2}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_p^*$
$\forall i \in 0, \ldots, l:$		
$r_i := c \cdot x_i + \alpha_i + \beta \pmod p$	$\xrightarrow{r_0, \ldots, r_l}$	Verification:
		$I := c^{-1}(\sum_0^l r_i P_i - A_1 - v^{-1} A_2)$
		check whether I is a valid identifier

Fig. 3. Designated verifier DL-REP proof; i.e., proof of knowledge of a DL-REP of I w.r.t. $P_0, \ldots, P_l$ (There are $l + 2$ point multiplications on the Prover's side.)

Protocol The Designated Verifier DL-REP proof in Figure 3 is clearly correct as the value computed by the verifier in the last step will be always equal to the prover's identifier I. Furthermore, the proof is zero-knowledge since, given I, the verifier herself could generate a valid transcript by selecting $r_0, \ldots, r_l$ and c uniformly at

random from $\mathbb{Z}_p$ and A_2 uniformly at random from G. Then $A_1 := \sum_0^l r_i P_i - cI - v^{-1}A_2$ will be distributed uniformly in G.

To use the full potential of DL-REPs, we want to make selective disclosure proofs, that is, a scheme in which a prover should be able to prove the knowledge of any subset of attributes. In U-Prove, the revealed attributes are either common input, or they are sent through a private channel to the verifier. While the former releases information to an external party, the latter presumes some encryption with the verifier's key. Since neither of these solutions is suitable in an RFID set-up, we should extend designated verification to include selective disclosure.

A naive approach to selective disclosure is the following. The prover proves the knowledge of a reduced set of attributes (e.g., without attribute x_2) which would enable the verifier to compute a partial identifier. Adding to it possible attribute points (e.g., x_2P_2) by trial and error. The verifier then tries all possible attribute points until it obtains a valid identifier. However, this solution clearly does not scale for several attributes with a lot of possible values.

In the next section we extend the current scheme to a designated selective disclosure scheme that does not have the drawback mentioned above. The security and narrow-strong privacy for this designated DL-REP scheme will follow from the corresponding results for the scheme in the next section.

3.2 Designated Selective Disclosure

In the previous section we introduced a designated zero-knowledge proof of knowledge of a DL-REP. The prover tag does not reveal its attributes, only the fact that it actually knows them. To make the construction more practical, we propose another scheme, the Designated Verifier Partial DL-REP scheme, or simply designated selective disclosure.

In this scheme a verifier can compute and check the identifier of a tag. Furthermore, it can compute an attribute points[5] only if the prover disclosed it and the verifier is entitled to see it according to a so-called entitlement set $\mathcal{E}$ (by which we mean a set of indices that defines which attributes a verifier is entitled to see). Note that even if the verifier does not have all designated attribute private keys v_i, he can compute the identifier I and those attributes he is entitled to see, as determined by $\mathcal{D} \cap \mathcal{E}$.

Setup The algorithm $\mathsf{SetupVerifier}$ in the Setup is slightly modified because of the designated attribute verification.

- $\mathsf{SetupVerifier}(par, \mathcal{E}) \longrightarrow (v, V, (v_i, V_i)_{\mathcal{E}})$ generates a private/public key pair and a set of pairs for the Verifier, where the latter set depends on the entitlement index set $\mathcal{E}$. If the identification key and the entitlement keys have already been generated in the system, the algorithm outputs those.

[5] Unlike in traditional selective disclosure, not the actual attributes x_j but the corresponding points x_jP_j are disclosed. However, note that the proof includes the fact that the tag stores attributes x_j.

Prover		**Verifier**
$x_0, \ldots, x_l$	$P_0, \ldots, P_l$	$v, (v_i)_{i \in \mathcal{E}}$
	$\forall i \in \mathcal{D}: \ V_i = v_i P_i$	
$I = \sum_0^l x_i P_i$	$V = v \cdot \sum_0^l P_i$	
$\alpha_0, \ldots, \alpha_l, \beta \in_R \mathbb{Z}_q^*$		
$A_1 := \sum_0^l \alpha_i P_i$		
$A_2 := \beta V$		
$B_i = (\alpha_i + \beta) V_i \quad \forall i \in \mathcal{D}$	$\xrightarrow{A_1, A_2, (B_i)_{i \in \mathcal{D}}}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_q^*$
$\forall i \in 0, \ldots, l:$		
$r_i := c \cdot x_i + \alpha_i + \beta \pmod p$	$\xrightarrow{r_0 \ldots r_l}$	First verify that the identifier is correct: $I = c^{-1}(\sum_0^l r_i P_i - A_1 - v^{-1} A_2)$ Then for each $j \in \mathcal{D} \cap \mathcal{E}$ compute attribute C_j: $C_j = I - c^{-1}(\sum_{i \neq j} r_i P_i - A_1 - v^{-1} A_2 + v_j^{-1} B_j)$

Fig. 4. Designated verifier DL-REP proof in which attributes in $\mathcal{D}$ are disclosed. (There are $l + 2 + d$ point multiplications on the Prover's side.)

Protocol Assume that a tag is interrogated to reveal a set of attributes corresponding to the disclosure index set $\mathcal{D}$ (see Figure 4). Then it has to perform an identification in which the designated verifier, who is entitled to read attributes in $\mathcal{E}$, can compute the following values:

- identifier I of the prover tag;
- disclosed attribute points $C_i = x_i P_i$ that were disclosed by the prover and for which the verifier has the corresponding attribute verifier key v_i.

After generating random values for all attributes and for the designation, the prover can compute the commitment points A_1, A_2 for the DL-REP and $(B_i)_{i \in \mathcal{D}}$ for the designated selective disclosure. Following the challenge–response phase, the verifier can first compute identifier I like in the normal Designated Verifier DL-REP scheme, that is, without the use of the entitlement set $\mathcal{E}$. Second, the verifier can reconstruct attribute points $C_j = x_j P_j$ in case $j \in \mathcal{D} \cap \mathcal{E}$, that is, both the prover included B_j in the proof and the verifier is entitled to see the attribute point of index j. We note that the entitlement set $\mathcal{E}$ can be empty.

Security against impersonation We show that it is not possible for an adversary to impersonate any valid tag, even though it was allowed to communicate with valid tags before.

Theorem 1. *Assuming the original Selective Disclosure U-Prove scheme is secure against active impersonation attacks the Designated Verifier Partial DL-REP proof is also secure against active impersonation attacks.*

Proof (Sketch.). We show how an adversary against the Designated Verifier Partial DL-REP system can be used to break the security of the U-Prove Selective Disclosure scheme. To do so, we build an adversary $\mathcal{B}$ that essentially translates between these

two systems. For the disclosed attributes we can easily 'un-disclose' them to mimic the Designated Verifier Partial DL-REP scheme. To go back we simply remember which attribute value corresponds to which public value. The other direction is the same as in Bringer et al. [6].

Narrow-strong privacy This proof uses a somewhat similar approach as the privacy proof of the Randomized Schnorr scheme [6]. There the authors show that the game in Definition 4 can be reduced to the following. If an adversary breaks the narrow-strong privacy of their Randomized Schnorr scheme, then it has to be able to distinguish tuples of the form $(A_1 = \alpha P, A_2 = \beta P, r = \alpha + \beta)$, where α and β are random from tuples of the form $(A_1 = \alpha P, A_2 = \beta P, r)$, where also r is random. Furthermore, they show that any adversary that can do so can be used to break DDH.

Theorem 2. *Assuming the hardness of the DDH-problem the Designated Verifier Partial DL-REP scheme is narrow-strong private.*

Proof (Sketch.). We extend traces for the Randomized Schnorr scheme to full traces for the Designated verifier DL-REP scheme. We do this in such a way that the new responses are random if and only if the response of the original instance was random. Hence any adversary against the Designated Verifier DL-REP scheme can be converted into a Randomized Schnorr adversary. Since the latter is secure under the DDH-assumption, the result follows.

4 Feasibility and Applications

In this section we discuss practical implications of our proposal. First we describe possible implementations and we follow up with some applications.

4.1 Feasibility of our proposal

To show the feasibility of the proposed protocols for RFID tags, we consider an ECC-based architecture, for example, the one presented in [2]. The EC processor described is very compact and the performance of 1 point multiplication, even when frequency is lowered enough to keep the total power low, is still acceptable. More precisely, the ECC-based grouping proofs as in [2] require two or three point multiplications and, even in the latter case, running time to complete the proof should stay below 300 ms. In addition our selective disclosure protocol achieves similar performance as hierarchical proofs [1] in which the performance depends on the number of levels in the hierarchy.

Similar remarks are valid for the memory requirements of a single tag. Assuming l attributes, a tag has to store $l + 1$ values where each is 160 bits long as the group keys in the hierarchical proof protocols. Having, for instance, 4 attributes to store, a tag requires 800 bits memory (assuming a curve over a 160-bit field). This is completely acceptable even for passive tags as attributes could be stored in the ROM memory, which is (unlike registers) considered very cheap, in the same way as the ECC parameters.

4.2 Envisioned RFID Applications

As mentioned above, new RFID security applications requiring a strong level of privacy are emerging constantly. Examples from previous works include yoking (or grouping) proofs and hierarchical proofs. Hence, an immediate need for designated attribute-based proofs is clear.

Considering the example of hierarchical proofs, our solution could be deployed meeting exactly the same requirements as envisioned by the tree structure of the hierarchical proofs [1]. To obtain the same functionality, one could sort the attributes according to their order of importance. More precisely, choose x_1 to be less important i.e. less privacy/security critical and therefore, the first secret verification key v_1 can be stored on a lot of readers, while v_3, for example, only at a very limited set of verifiers, etc. This infrastructure is easily incorporated in the designated attribute-based proofs as introduced above. In this way, we achieve not just a more fine-grained access control for tags, but also more fine-grained permissions for readers.

A typical real-life scenario can be found in the medical domain. Patients carry medicines that can be scanned (and sometimes should) by legitimate authorities (e.g., customs officers) while maintaining some privacy for the user. In this case, the highest level of verification, i.e., the lowest index is left for medical staff providing first aid in accidents or other emergency cases.

5 Conclusions

We proposed a new scheme, the Designated Verifier (Partial) DL-REP proof: a tag, storing a DL-REP of its unique identifier, can reveal an arbitrary subset of its attributes to a designated verifier. This scheme relies on recent designs of RFID chips that allows for the use of elliptic curve cryptography. While any authentic verifier can check the tag's validity, it can only compute those attribute points that it is entitled to. On the one hand, a tag can contain many semantically different attributes, a reader, on the other hand, can gain access only certain subset of these.

We proved that the protocol is secure and narrow-strong private in the Vaudenay model. Therefore, the scheme is powerful and reliable and it enables further architectural developments in which tags and verifiers can have fine-grained permissions.

In Section 4.2, we show that the scheme enables the development of new protocols for specific applications. Nevertheless, in the context of RFID systems further study is needed to examine whether extentions to the attribute-based proofs, such as proving predicates and linear dependencies among attributes, or verifying more tags at the same time, can be applied in a meaningful manner.

5.1 Future work

An actual implementation of the protocol offers new opportunities for research. It allows us to obtain results (in terms of timing, power consumption, area, memory, code size, battery time) and to test applicability of the protocols on RFID tags. Moreover, an implementation on other mobile devices, such as smart cards or mobile phones can offer interesting results as well.

We are aware that the protocols proposed in this paper are computationally demanding for most RFID systems. We believe, however, that RFID applications can be designed that are tailored and simplified to the specific hardware and yet they preserve required security and privacy properties of our schemes.

Our schemes could be deployed in privacy-sensitive contexts, such as electronic health records. Patients' physical characteristics, permanent and temporary conditions and their medication can be stored in credentials, and revealed only in circumstances and to recipients only if it is really necessary. Furthermore, given more expensive user devices, computational problems emerge to a smaller extent than with RFID tags.

6 Acknowledgements

This work was supported in part by the research program Sentinels[6] as projects *Mobile IDM* (10522) and *Revocable Privacy* (10532) and by the European Commission under contract number ICT-2007-216676 ECRYPT NoE phase II.

References

1. Lejla Batina, Yong Lee, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede. Privacy-Preserving ECC-Based Grouping Proofs for RFID. In Mike Burmester, Gene Tsudik, Spyros Magliveras, and Ivana Ilic, editors, *Information Security*, volume 6531 of *LNCS*, pages 159–165. Springer Berlin / Heidelberg, 2011.
2. Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede. Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. *Personal and Ubiquitous Computing*, 16(3):323–335, 2012.
3. Lejla Batina, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede. Hierarchical ECC-Based RFID Authentication Protocol. In Ari Juels and Christof Paar, editors, *RFID. Security and Privacy*, volume 7055 of *LNCS*, pages 183–201. Springer Berlin / Heidelberg, 2012.
4. Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, MA, USA, 2000.
5. Michael Braun, Erwin Hess, and Bernd Meyer. Using Elliptic Curves on RFID Tags. *IJCSNS International Journal of Computer Science and Network Security*, 8(2):1–9, 2008.
6. Julien Bringer, Hervé Chabanne, and Thomas Icart. Cryptanalysis of EC-RAC, a RFID Identification Protocol. In Matthew Franklin, Lucas Hui, and Duncan Wong, editors, *Cryptology and Network Security*, volume 5339 of *LNCS*, pages 149–161. Springer Berlin / Heidelberg, 2008.
7. Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Kai Rannenberg, and Zwingelberg Harald. D2.1 Architecture for Attribute-based Credential Technologies. Deliverable, ABC4Trust EU Project, December 2011.
8. David Chaum. Zero-Knowledge Undeniable Signatures (extended abstract). In Ivan Damgård, editor, *Advances in Cryptology - EUROCRYPT '90*, volume 473 of *LNCS*, pages 458–464. Springer Berlin / Heidelberg, 2006.

[6] Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

9. David Chaum and Hans van Antwerpen. Undeniable Signatures. In Gilles Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, volume 435 of *LNCS*, pages 212–216. Springer Berlin / Heidelberg, 1990.
10. Junfeng Fan, Miroslav Knezevic, Dusko Karaklajic, Roel Maes, Vladimir Rozic, Lejla Batina, and Ingrid Verbauwhede. FPGA-based testing strategy for cryptographic chips: A case study on Elliptic Curve Processor for RFID tags. In *15th IEEE International On-Line Testing Symposium (IOLTS 2009), 24-26 June 2009, Sesimbra-Lisbon, Portugal*, pages 189–191. IEEE, 2009.
11. Daniel M. Hein, Johannes Wolkerstorfer, and Norbert Felber. ECC Is Ready for RFID - a proof in silicon. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *LNCS*, pages 401–413. Springer, 2009.
12. Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated Verifier Proofs and Their Applications. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, volume 1070 of *LNCS*, pages 143–154. Springer Berlin / Heidelberg, 1996.
13. A. Juels. "Yoking-Proofs" for RFID Tags. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW '04)*, pages 138–143. IEEE Computer Society, 2004.
14. Neil Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.
15. Yong Ki Lee, Lejla Batina, Dave Singelée, and Ingrid Verbauwhede. Low-Cost Untraceable Authentication Protocols for RFID. In *Proceedings of the third ACM conference on Wireless network security*, WiSec '10, pages 55–64, New York, NY, USA, 2010. ACM.
16. Christian Paquin. U-Prove Cryptographic Specification V1.1. Technical report, Microsoft, 2011.
17. Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch. An Efficient Strong Designated Verifier Signature Scheme. In Jong-In Lim and Dong-Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003*, volume 2971 of *LNCS*, pages 40–54. Springer Berlin / Heidelberg, 2004.
18. C. Schnorr. Efficient Identification and Signatures for Smart Cards. In Gilles Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, volume 435 of *LNCS*, pages 239–252. Springer Berlin / Heidelberg, 1990.
19. Serge Vaudenay. On Privacy Models for RFID. In Kaoru Kurosawa, editor, *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 68–87. Springer, 2007.

A Security and Privacy Proofs

A.1 Proof of Theorem 1

Proof. (Theorem 1.) Suppose we are given an adversary $\mathcal{A}$ that wins the active impersonation game for the Designated Verifier DL-REP proof, we show how to construct an adversary $\mathcal{B}$ that wins the active impersonation game for the U-Prove selective disclosure scheme. We need to show how $\mathcal{B}$ answers the identification requests from $\mathcal{A}$ using only the U-Prove oracle. Furthermore, we show how the impersonated identification protocol, run by $\mathcal{A}$ against the Designated Verifier DL-REP scheme, is converted by $\mathcal{B}$ into an identification protocol for the U-Prove selective disclosure scheme.

Initially, adversary $\mathcal{B}$ generates a random private key v and sets the public key V to $V = v \sum P_i$. Furthermore, for any disclosed attribute $i \in \mathcal{D}$ adversary $\mathcal{B}$ generates v_i at random and sets $V_i = v_i P_i$, and sends these V_i's together with V to adversary $\mathcal{A}$.

During the first phase $\mathcal{B}$ answers interrogation queries for a tag as follows. First, it queries its own oracle, who sends a commitment A. Adversary $\mathcal{B}$ generates $\alpha_i \in_R \mathbb{Z}_p$ for $i \in \mathcal{D}$ and $\beta \in_R \mathbb{Z}_p$ and sends to $\mathcal{A}$ the values

$$\begin{aligned} A_1 &= A + \sum_{i \in \mathcal{D}} \alpha_i P_i \\ A_2 &= \beta V \\ B_i &= (\alpha_i + \beta) V_i \qquad i \in \mathcal{D}. \end{aligned}$$

Subsequently, $\mathcal{B}$ receives c from $\mathcal{A}$ which it passes along to its oracle. In return it receives r_i' for $i \notin \mathcal{D}$ and x_i for $i \in \mathcal{D}$. It then sends to $\mathcal{A}$ the responses

$$r_i = \begin{cases} r_i' & \text{for } i \notin \mathcal{D} \\ cx_i + \alpha_i + \beta \pmod p & \text{for } i \in \mathcal{D}. \end{cases}$$

For future reference $\mathcal{B}$ will store the tuples $(x_i, x_i P_i)$ for every disclosed attribute. Clearly, this construction is a perfect simulation of the designated verification protocol.

In the second phase adversary $\mathcal{A}$ will impersonate a tag. The goal of adversary $\mathcal{B}$ is to transform this communication such that it in turn impersonates a valid tag for the U-Prove selective disclosure protocol. First, $\mathcal{A}$ will generate two commitments A_1 and A_2, which are converted by $\mathcal{B}$ into $A = A_1 + v^{-1} A_2$ before sending it to the original U-Prove verifier. The verifier responds with a challenge c, which $\mathcal{B}$ relays unchanged to $\mathcal{A}$. Finally, $\mathcal{A}$ replies with the r_i values. For $i \notin \mathcal{D}$, $\mathcal{B}$ forwards these values to the challenger. Note that they should equal $r_i = cx_i + \alpha_i + \beta$ and are therefore appropriate responses to the commitment A. For the disclosed attributes ($i \in \mathcal{D}$), $\mathcal{B}$ can calculate

$$x_i P_i = I - c^{-1} (\sum_{j \neq i} r_j P_j - A_1 - v^{-1} A_2 + v_i^{-1} B_i).$$

Using its stored tuples, $\mathcal{B}$ can then recover the values x_i before forwarding them to the challenger according to the U-Prove protocol (see Figure 2). This completes the proof.

A.2 Proof of Theorem 2

Proof. (Theorem 2.) A transcript in our designated verifier partial DL-REP proof has the form $A_1 = \sum \alpha_i P_i, A_2 = \beta V, (B_i)_{i \in \mathcal{D}}, c, (r_i = cx_i + \alpha_i + \beta)_{i=0}^{l}$. We would like to show that the adversary cannot distinguish between properly constructed r_i's and randomly chosen ones. Following the argument in Bringer et al. [6], we can take out the attribute values x_i. Hence, the adversary has to distinguish instances from

the actual distribution

$$D_A^l = \{(A_1^S = \sum_{i=0}^{l} \alpha_i P_i, A_2^S = \beta V, (B_i)_{i\in\mathcal{D}}, (r_i = \alpha_i + \beta)) \ : \\ \alpha_i, \beta \in_R \mathbb{Z}_p, 0 \leq i \leq l\}$$

from instances from the simulated distribution

$$D_S^l = \{(A_1^S = \sum_{i=0}^{l} \alpha_i P_i, A_2^S = \beta V, (B_i)_{i\in\mathcal{D}}, (r_i)) \ : \ \alpha_i, \beta, r_i \in_R \mathbb{Z}_p, 0 \leq i \leq l\}$$

where the r_i's are random.

Suppose we have an oracle for distinguishing between these two distributions, we will use this to decide between the corresponding instances for the Randomized Schnorr scheme, which are in fact instances from D_A^0 or D_S^0. The main idea is that we use the instance $(A_1 := \alpha P, A_2 := \beta V, r)$ we obtain as a challenge, to construct a full instance. This instance can then be solved using our oracle. We construct the other attributes in such a way that $\alpha_0 = \alpha$ and $\alpha_i = \alpha + \gamma_i$ where γ_i is random.

Start by setting $P_0 = P$ and $P_i = p_i P$, with p_i random. Then we construct A_1^D as

$$A_1^D = A_1 + \sum_{i=1}^{l} (p_i A_1 + \gamma_i P_i) = \alpha P_0 + \sum_{i=1}^{l} \left[(\alpha + \gamma_i) P_i\right].$$

Similarly, we set $V = \sum_{i=0}^{l} P_i$, with v_i random and construct

$$A_2^D = A_2 + \sum_{i=1}^{l} p_i A_2 = \beta \sum_{i=0}^{l} P_i.$$

For any disclosed attribute $i \in \mathcal{D}$ choose $v_i \in_R \mathbb{Z}_p$ and set $V_i = v_i P_i$. Then the values B_i are constructed as

$$B_i = v_i(p_i A_1 + \gamma_i P_i) = (\alpha + \gamma_i) V_i.$$

Finally, we set $r_0 = r$ and

$$r_i = r + \gamma_i.$$

If $r = \alpha + \beta$, then clearly all other r_i's are correct as well, and we are in the normal situation. However, if r is random, then all the other values are random as well.[7] This construction yields a valid input to our Designated Partial DL-REP oracle, and can hence be used to break the privacy of the Randomized Schnorr scheme.

[7] While it may appear that the γ_i's are fixed by the construction of A_1^D, this is actually not the case: Nothing binds the value of α itself anymore, and hence, A_1^D is actually a commitment to the γ_i's that hides information theoretically.