Designated Attribute Proofs with the Camenisch–Lysyanskaya Signature

Kostas Papagiannopoulos, Gergely Alpár, and Wouter Lueks

Institute for Computing and Information Sciences (iCIS), Radboud University Nijmegen, The Netherlands.

Abstract. An attribute-based credential (ABC), an authentic personal electronic piece of information to perform transactions, offers a secure and privacy-preserving method to authorize user transactions. One of the most important techniques to realize ABCs is the Camenisch–Lysyanskaya signature. In this paper we extend its underlying cryptographic algorithms with the *designation* property. As a result, the showing protocol between a user and a verifier does not require an additional secure channel to perform credential proofs.

1 Introduction

Our modern, fully-interconnected, always-online society relies on a huge number of daily electronic transactions in order to operate, develop and thrive. Internet-based transactions enable e-banking, online commerce and digital communications, while embedded systems and smart cards enable and enhance transactions with public transport, mobile services, electronic purses and TV services.

Authentication methods are required in most of these applications. Although digital credentials provide authenticity, they often include a unique identifier which allows electronic transactions performed by the same user to be linked. Notably, the user may be subject to targeted advertisement without established consent. Racial, medical or personal traits can lead to discrimination and the user's location may be determined.

In order to address and mitigate the aforementioned privacy threats, several public agencies encouraged advances in credential technology. The European Network and Information Security Agency (ENISA) emphasized the need for "privacy-respecting" use of unique identifiers in European identity cards, the Ontario Privacy Commissioner underlined the necessity of a user-centric approach that embeds privacy into the design and architecture of credential systems [9], while National Institute of Standards and Technology (NIST) issued a strategy towards a user-centric "identity ecosystem" [8]. Last, the European Union promoted legislation (Directive 95/46/EC, General Data Protection Regulation) that enforces the user's control over his personal data and credentials and establishes privacy by design.

Attribute-Based Credentials (ABCs) emerged as a viable privacy-enhancing technique that implements the new requirements. An attribute based credential is issued to the user by a trusted identity provider. The user's ABC contains his personal attributes, similar to physical identity documents. The structure of the ABC allows the user to prove to a third party that he possesses a specific attribute *without actually revealing the credential identifier*. In particular, he is capable of using a *zero-knowledge* protocol to prove that

he is older than 18 years old, without making his name or identity number public. Moreover, by employing the *selective disclosure* feature, he can always reveal the minimum required subset of personal attributes in each transaction. Several, cryptographic primitives implement ABC functionality: Microsoft's U-Prove, based on the discrete logarithm representations (DL-REPs) and the Schnorr signature [3,5,11], and IBM's Idemix, based on the Camenisch–Lysyanskaya (CL) signature [1,10]. The focus of this research is the CL scheme's existing and desirable functionalities.

Specifically, since only recent efforts try to move ABCs from cryptography to real-world solutions, no general consensus has been reached with respect to the desired properties of the underlying zero-knowledge protocols. Both Schnorr-based and the CL schemes are vulnerable to information leakage (e.g. learning if a user possesses a certain attribute or not), since the selective disclosure procedure can be eavesdropped if an insecure channel is used. The Schnorr-based protocols are more susceptible to identifier leakage, due to the static nature of the signature—as we will see later, it does not provide multi-show unlinkability. Moreover, the current cryptographic basis cannot detect or stop a malicious terminal that impersonates a legitimate one.

These issues can be solved, to a certain extent, by employing an additional layer of authentication and encryption below the zero-knowledge proof, using standard public key cryptography. However, this approach is not efficient when it comes to resource-limited devices such as embedded systems and smart cards. Even in a modern desktop computer, where the computational overhead is small, an additional layer of authentication may leak identifiers. To tackle this problem, we added *designation* [4] to the CL scheme. Instead of the additional layer, we *integrated public key cryptography within the zero-knowledge proof*. This allows a user to share attributes only with a particular party, making sure that these attributes are revealed only to the designated verifier and does not leak elsewhere. Previous research by Alpár et al. [2] has extended the cryptographic basis of DL-REP with the designation feature. Still, the internal structure of Schnorr-based schemes does not allow a credential to be shown more than once as it does not offer multi-show unlinkability. On the other hand, the CL signature is randomized in every transaction, which provides inherent multi-show unlinkability. By adding designation, we can achieve the best of both worlds.

In summary, our research extends the cryptographic basis of the CL signature used in Idemix by adding the designation feature. The resulting zero-knowledge proof is secure assuming the CL signature is secure, which in turn relies on the strong RSA assumption.

2 Technical Background

In this section we introduce attribute based credentials in more detail, and explain the basis of Idemix: the Camenisch Lysyanskaya signatures.

2.1 ABCs and their features

An attribute-based credential (ABC) is a cryptographically protected collection of user attributes. First, an authoritative source, the so-called issuer issues it to a user via an

issuance protocol, and later the user can present it to a relying party, or verifier, via a showing protocol.

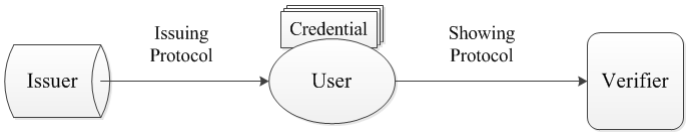

Fig. 1. The core modules of ABCs: issuer, user, verifier.

ABCs need to implement specific cryptographic features that provide security for the system and privacy for the users. Specifically, *unforgeability* prevents non-authoritative parties to issue valid credentials. *Non-transferability* ensures that users cannot share their credentials. *Issuing unlinkability* makes sure that the issuer cannot recognize credentials when they take part in showing protocols. *Multi-show unlinkability* renders it impossible for verifiers to link activities of the same user, meaning also that a credential cannot be inherently correlated with its uses.

This paper adds an additional feature to ABCs, namely the *designation* feature. In the context of a zero-knowledge proof used in ABCs, designation integrates public key cryptography inside the proof. As a result, the improved showing protocol can ensure that only the *designated* verifier will be able to verify the user's credential. Adding the designation property has minimal impact on the aforementioned scheme (Figure 1), since it affects only the showing protocol between the user and the verifier, while the issuing protocol remains unaltered.

2.2 Camenisch–Lysyanskaya signature

Existing ABC technologies [10] use the signature scheme proposed by Camenisch and Lysyanskaya (CL scheme) [1]. Its security relies on the strong RSA assumption and it provides efficient zero-knowledge proofs. Before presenting our designated variant, we briefly recall the CL scheme.

The scheme requires a system parameter $n = pq$, where p, q are safe primes, generated randomly by the issuer and kept secret. All computations are performed in the quadratic residue QR_n subgroup of $\mathbb{Z}_n^*$. The issuer also generates the public constants $R_0, \ldots, R_l, S, Z \in QR_n$. A basic CL signature on a block of $l+1$ messages is constructed as follows.

Signature generation: *Signature verification:*

$$A := \left(\frac{Z}{R_0^{m_0} \ldots R_l^{m_l} S^v}\right)^{1/e} \mod n \qquad Z \stackrel{?}{\equiv} A^e R_0^{m_0} \ldots R_l^{m_l} S^v \pmod{n}$$

By knowing the prime factors p and q, the issuer can compute $1/e \pmod{\varphi(n)}$ (e and v are random numbers) and then A. The resulting signature on a block of messages

$m_0, \ldots, m_l$ is (e, A, v). Given a signature and the system parameters, a signature can efficiently be confirmed by the verification equation.

When the CL signature is used for creating attribute-based credentials, l attributes are represented as numbers $m_1, \ldots, m_l$ and m_0 is the user's secret key. To achieve the desired privacy properties, the credential issuing (signing) and its verification happen in a more intricate way than in the basic signature scheme. As the issuing protocol is in fact a blind signature, the issuer does not learn the user's secret key m_0 and the resulting signature (e, A, v). This provides the *issuing unlinkability* feature. By using randomization and zero-knowledge-proof techniques while showing a credential, a user can achieve *multi-show unlinkability*.

3 Designated Showing Protocol with CL

In this section we present the new credential showing protocol that integrates the designation property (Table 1). The user proves possession of a credential with l attributes, while keeping the value of all the attributes secret. This prove is designated to the verifier. We followed similar techniques as Bringer [4] and Alpár *et al.* [2]. Every verifier has a private-public key pair (k, V). During the showing protocol V is used to derive a designator De. The verifier is the only one that possesses the secret key k, and thus, he is the only one capable of verifying the zero-knowledge proof.

The designated showing protocol's public input consists of the CL constants $(Z, S, R_0, \ldots, R_{l-1})$, the RSA modulus n and the public key V, used for designation purposes. The private input to the scheme contains the corresponding designation private key k and the secret attributes $m_0, \ldots, m_l$. After the standard randomization process, the ZK commitment phase commits to the secret attributes (using values $s, t, \{w_i\}$) and generates the designator De. The User sends the commitment Co and designator De and upon receival of the Verifier's challenge c he generates the response, based on the secret attributes $\{m_i\}$, the values $s, t, \{w_i\}$ and the designator exponent b. Following that, the Verifier computes the verification equation using the commitment Co, the designator De and the secret designation key k.

The verification equation needs to be adapted because the designation value De would require to take k-th root. This is not a problem in [2,4] where the order of the group, which is essential in taking roots, is a public system parameter. In the CL setting, where the strong RSA assumption holds, it is impossible to take roots; therefore, we need to restructure the verification equation.

The primary goal of designation is to make it impossible for any external parties to verify the validity of a proof. This can also be achieved by encrypting the whole conversation using a shared key between the user and the verifier. We note, however, that this might not be efficient – due to the large amount of communication overhead and possible identifier leakage during a prior key setup phase. On the user's side the computational costs of designation is only one modular exponentiation V^b when compared with the CL scheme, which is feasible even on devices with limited resources, such as smart cards.

User	**Public**	**Verifier**
m_0: secret key	$Z, S, R_0, \ldots, R_{l-1} \in QR_n$	**k: Verifier's private key**
$m_1, \ldots, m_l$: attributes	n: RSA modulus, size l_n bits	$V = (\Pi_{i=0}^{l-1} R_i)^k$
Signature (A, e, υ)	**V: Verifier's public key**	
υ , size l_υ bits	$l_\emptyset$: size of security interval	
e , size l_e bits	l_H: length of hash function	
Randomization		
$r \in_R \{0,1\}^{l_n + l_\emptyset}$		
$\hat{\upsilon} = \upsilon - er \ (in\ \mathbb{Z})$	A'	
$A' = AS^{-r}$	$\longrightarrow$	
ZK Proof		
$t \in_R \{0,1\}^{l_e + l_\emptyset + l_H}$		
$s \in_R \{0,1\}^{l_\upsilon + l_\emptyset + l_H}$		
$w_i \in_R \{0,1\}^{l_m + l_H + l_\emptyset}$		
$Co = A'^t S^s R_0^{w_0} \ldots R_l^{w_l}$		
$\mathbf{b} \in_\mathbf{R} \{\mathbf{0,1}\}^{\mathbf{l_m + l_H + l_\emptyset}}$		
$\mathbf{De = V^b}$	$\{Co, \mathbf{De}\}$	
	$\longrightarrow$	
	c	$c \in_R \{0,1\}^{l_c}$
	$\longleftarrow$	
$r_t = c * e + t$		
$r_s = c * \hat{\upsilon} + s$		
$\forall m_i, w_i, i \in \{0, \ldots, l\}$		
$r_{m_i} = c * m_i + w_i + \mathbf{b}$	$\{r_t, r_s, r_{m_0}, \ldots, r_{m_l}\}$	
	$\longrightarrow$	Verification:
		$\mathbf{Z^{kc}} =$
		$(\mathbf{A'^{r_t} S^{r_s} R_0^{r_{m_0}} \ldots R_l^{r_{m_l}}})^\mathbf{k} *$
		$\mathbf{Co^{-k} * De^{-1}}$

Table 1. Designated, multi-attribute, zero-knowledge CL protocol in which no attribute is revealed. We use **bold** typesetting to denote the extra computations compared to the CL scheme. By removing the bold parts and replacing the verification equation with $A'^{r_t} S^{r_s} R_0^{r_{m_0}} \ldots R_l^{r_{m_l}} = Z^c Co$, one obtains the original, non-designated, multi-attribute CL scheme.

4 Security Analysis and Discussion

In this section we discuss the security of the proposed scheme and provide a comparison between the designated CL protocol and the existing designated DL-REP scheme, with respect to the offered security features and performance. The comparison is summarized in Table 2.

Security. The security of the designated CL zero-knowledge proof relies on the security of the original CL scheme which is secure under the strong RSA assumption.

We give an informal description of a security reduction to the security of the showing protocol of the original CL scheme. The additional elements in the transcript of the zero-knowledge proof of the designated scheme are De and the modified responses $\{r_{m_i}\}_{i=0,\ldots,l}$. De is a commitment to a random element b which is added to each original $cm_i + w_i$. These elements can easily be added to the original CL scheme by an outside party. Therefore, an

adversary that can break the security of the designated scheme can be used to break the security of the original CL scheme.

The properties of completeness, zero-knowledge, and special soundness hold for the designated CL.

Designation. While the techniques applied in the Schnorr/DL-REP schemes and in the CL scheme to make designation possible are similar, there is a surprisingly substantial difference. Consider the validation of credentials in the two designated schemes. We recall that in [2,4], after a proof of an identifier, the verifier has to look it up in a database of all valid identifiers . This additional step and the extra database are not required here. While a DL-REP can be produced by anyone, a CL signature can only be computed by the issuer. Therefore, proving a CL signature immediately proves validity of a credential. Furthermore, since Schnorr identifiers and DL-REPs cannot be randomized like a CL signature, a proof of knowledge directly exposes the identifier. (Essentially, they prove that the user knows the exponent(s) of the public value $I = g^x$ or $I = g_0^{x_0} \dots g_l^{x_l}$ in the Schnorr or the DL-REP schemes, respectively.)

Issuer-Show Unlinkability. This property guaranteed by the blind signature produced by the issuer during issuance. The issuer does not learn the secret key nor the resulting signature corresponding to the credential. Therefore, the issuer cannot recognize the credential when it is later shown. As blind signature can be realized in (designated) Schnorr-like schemes as well as in the (designated) CL scheme, they both meet this requirement.

Multi-show Unlinkability. As mentioned, the user is capable of fully randomizing the signature before sharing it with a verifier. Thus, it fulfills the requirements for multi-show unlinkability and this property is retained under designation. Designated Schnorr does not provide this feature and it recommends the usage of multiple signature tokens in order to 'randomize' each transaction [11], which requires more storage.

Performance. One of the main drawbacks of CL schemes is its reliance on RSA groups, which require at least 1024-bit keys to achieve an appropriate level of security. On the other hand, Schnorr/DL-REP/U-Prove schemes operate in groups where the DL assumption holds, which means at least a 1024-bit prime-group size or a 160-bit elliptic-curve group. A U-Prove (prime group) implementation on MULTOS smart cards [6] achieved a showing protocol (five attributes proof of knowledge) less than 0.7 second computation time, while the CL scheme for similar parameters [13] resulted in almost 1.3 seconds. Moreover, the U-Prove results can be even further improved with an elliptic group implementation.

5 Conclusions

We proposed a new cryptographic scheme, the designated multi-attribute CL, rendering a user of Idemix capable of revealing his attributes only to a designated verifier, without risking identity leakage or identification. The scheme does not modify the issuing and

Property	Designated DL-REP	Designated CL
Designation	applied on signature	applied on identifier
Issuer-showing unlinkability	fulfilled	strongly fulfilled
Multi-show unlinkability	not fulfilled	fulfilled
Performance	faster	slower

Table 2. Comparison table between designated Camenisch–Lysyanskaya scheme and designated DL-REP/Schnorr schemes [2].

causes just a slight overhead in the showing protocol. We also examined the security and privacy properties of the suggested scheme and compared it with the existing designated DL-REP protocols. In general, we consider the attribute based credentials to be a viable and secure solution for privacy-sensitive applications which are in-line with technical and legal guidelines for privacy protection. On the other hand, there are still several open issues regarding the desired ABC properties and device deployment. For future work, we suggest establishing a solid set of the required cryptographic schemes and make sure that all of them are compliant with the current regulation. Furthermore, we encourage efforts in standardizing ABC protocols, usage, system deployment and interoperability to assist this nascent technology in becoming mainstream.

References

1. J. Camenisch. *Direct Anonymous Attestation Explained.* 2007.
2. G. Alpár, L. Batina, W. Lueks. *Designated Attribute-Based Proofs for RFID Applications* Workshop on RFID Security, RFIDSec'12, 2012.
3. S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, US, 2000.
4. J. Bringer, H. Chabanne, T. Icart. *Cryptanalysis of EC-RAC, a RFID Identification Protocol.* In Matthew Franklin, Lucas Hui, and DuncanWong, editors, Cryptology and Network Security, volume 5339 of LNCS, pages 149161. Springer Berlin, Heidelberg, 2008.
5. C.P. Schnorr. *Efficient Identification and Signatures for Smart Cards.* In Gilles Brassard, editor, Advances in Cryptology, CRYPTO 89 Proceedings, volume 435 of LNCS, pages 239252. Springer Berlin, Heidelberg, 1990.
6. W. Mostowski, P. Vullers. *Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards.* 7th International ICST Conference, SecureComm 2011, London, UK, September 7-9, 2011.
7. P. Bichsel, J. Camenisch, T. Groß and V. Shoup. *Anonymous Credentials on a Standard Java Card.* In ACM Conference on Computer and Communications Security, 2009.
8. H. A. Schmidt. *The National Strategy for Trusted Identities in Cyberspace and Your Privacy.* April 26, 2011.
9. A. Cavoukian. *Privacy by Design. The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario. 2008.
10. IBM Research Zurich Security Team. *Specification of the Identity Mixer Cryptographic Library Version 2.3.0.* Research Report, IBM Research, Zurich. 2010.
11. C. Paquin. *U-Prove Cryptographic Specification V1.1.* Technical Report, Microsoft. 2011.
12. C. Paquin. *U-Prove Technology Overview V1.1* Microsoft. 2011.
13. P. Vullers and G. Alpár. *Efficient Selective Disclosure on Smart Cards Using Idemix.* In Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell editors, Policies and Research in Identity Management (IDMAN), 3rd IFIP WG 11.6 Working Conference, London, UK, IFIP AICT 396, pages 5367. Springer, 2013.