Designated Attribute Proofs with the Camenish-Lysyanskaya Signature

Kostas Papagiannopoulos, Gergely Alpár, Wouter Lueks

Institute for Computing and Information Sciences (iCIS), Digital Security Group, Radboud University Nijmegen, The Netherlands

Attribute-Based Credentials and the Designation Property

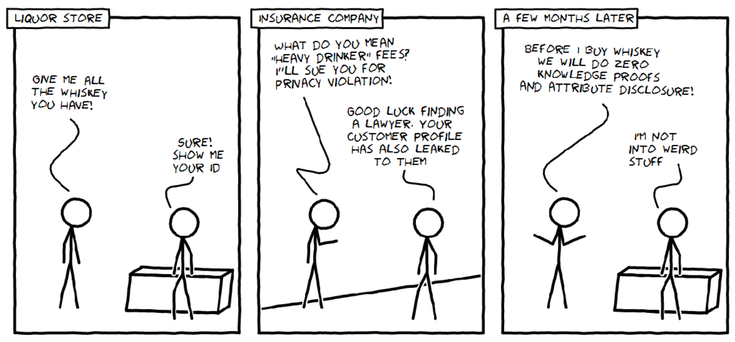

Figure 1: Identifier leakage

Traditional authentication mechanisms have the shortcoming that they label users with a unique identifier. Transactions from the same user can be linked together, with various ramifications to his privacy, anonymity and security.

Attribute-based credentials provide a privacy-friendly alternative:

- The user can prove that he possesses a specific attribute without revealing his unique identifier.
- He is in charge of his private data, choosing where and what to reveal.

Thus, attribute-based credentials can offer user-centric authentication, implementing privacy by design.

Zero-knowledge proof forms the core component behind attribute-based credentials. It is a method by which one party (the User) can prove to another party (the Verifier) that a given statement is true, without conveying any additional information.

Since the ZK proof is not encrypted/authenticated, everyone can verify the proof, thus, they are susceptible to attribute eavesdropping and Verifier impersonation attacks. Existing solutions employ an additional layer of authentication/encryption to mitigate the attacks, however, the established secure channel presents several deficiencies:

- For resource-limited devices the induced overhead may be undesirable.
- The authentication layer re-introduces the unique identifier issue.

Proposed Solution

Our solution integrates public key cryptography within the zero-knowledge proof, thus attributes are revealed only to the designated Verifier. The proposed solution reduces computational cost and solves the identifier issue.

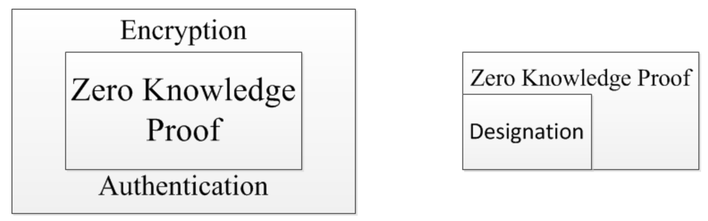

Figure 2: Old solution (left) *vs.* proposed solution (right)

Designated Camenish-Lysyanskaya (CL) Protocol

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

Figure 3: Designated, multi-attribute, zero-knowledge Camenish-Lysyanskaya protocol, using key pair (k, V). We use **bold** typesetting to denote the extra computations compared to the original CL scheme. To designate, the User employs the Verifier's public key V and as a result only the Verifier possessing secret key k can verify the proof.

- We proposed a new cryptographic scheme, the designated multi-attribute CL, rendering a user capable of revealing his attributes only to a designated verifier, without risking identification.
- The proposed scheme is secure under the strong RSA assumption.
- Adding the designation property has minimal impact on the original CL protocol.
- The new protocol between User and Verifier does not require an additional secure channel to perform zero-knowledge proofs.
- Issuer-Show and Multi-Show unlinkability properties of the original scheme are retained in designated CL.
- The designation computational penalty for the proposed protocol consists of a single modular exponentiation.

For future work, we suggest establishing a solid consensus on the required cryptographic schemes and properties.
We encourage efforts in standardizing ABC protocols, usage, system deployment and interoperability to assist this nascent technology in becoming mainstream and fruitful.

Details in: Designated Attribute Proofs with the Camenish-Lysyanskaya Signature, 34th WIC Symposium on Information Theory, 2013. Full paper is accessible via QR code or at http://tinyurl.com/designatedCL. Contact us via kostaspap88@gmail.com

k3rckhoffs 1nst1tute

Radboud Universiteit Nijmegen