Privacy-Preserving Predicate Proof of Attributes with CL-Anonymous Credential

Nan Guo[1]*, Jia Wang[1], Tianhan Gao[1], and Kangbin Yim[2]
[1] Northeastern University, Shenyang, China
guonan@mail.neu.edu.cn, wang_4027@126.com, gaoth@mail.neu.edu.cn
[2] Soonchunhyang University, Asan, Republic of Korea
yim@sch.ac.kr

Abstract

The anonymous credential system allows users to convince relying parties the possession of a credential released by an issuer. To adhere to the minimal information disclose principle, the anonymous credential facilitates predicate proofs of attributes without revealing the values. In this paper, we extend the pairing-based CL-anonymous credential system and present a series of attributes proof protocols. They enable users to prove to relying parties the AND and OR relations over multiple attributes, as well as equality to a given value and lying into a given interval over some single attribute.

Keywords: anonymous credential, attributes proof, predicate proof

1 Introduction

The information exchanged via the Internet has dramatically changed, from exchanging scientific and professional information to enormous amount of personal information. The management of identity attributes raises a number of challenges. On one hand, identity attributes need to be shared to speed up and facilitate user authentication and access control. On the other hand, they need to be protected as they may convey sensitive information about an individual and can be a target of identity theft. Identity theft means the act of impersonating others' identities by presenting stolen identifiers or proofs of identities[1]. In particular, the insiders of relying parties can easily make user profile, so the identity theft and misuse of user's personal information is at high risk.

The anonymous credential is a privacy-preserving technology that meets these requirements. It is proposed to provide more privacy during the verification of users' attributes. In contrast to classical authentication, the identity of attribute holders is never released, nor is any other private information which might be abused by verifiers. The reason of the anonymous credentials having become so popular is that they allow users to anonymously prove the possession of a credential, and adhere to minimal information disclosure principle as users can only disclose the minimal amount of personal information necessary for the transaction.

In the literature, there exit various anonymous credential systems. However, there are only two kinds of practical anonymous credential systems, the CL Idemix by IBM based on group signature and the Brands U-Prove by MS based on blind signature. In 2004, Camenisch and Lysyanskaya came up with an efficient CL signature scheme and constructed a CL anonymous credential system from bilinear mappings[5]. It enables selective disclosure and unlinkable multi-use. In 2012, Camenisch and Grob proposed a RSA-based anonymous credential[4], where the AND and OR relations are proved with

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 1, pp. 37-46
*Corresponding author: 3-11, Wenhua Road, Heping District, Shenyang, Liaoning Province, China, 110006, Tel: +86-15040150871

value complexity in the number of finite-set attributes using zero-knowledge proofs of integer relations on prime numbers. Due to the lower efficiency of RSA assumption, to prove predicates over attributes with pairing-based anonymous credential attracts more research. In 2011, Sudarsono utilized extended BBS+ signatures to certify a set of attributes as the accumulator, and used zero-knowledge proofs of BBS+ signatures and accumulators to prove AND and OR relations with value complexity in the number of finite-set attributes[12]. However, they did not offer comparison predicate proof; besides, the size of public key is dependent on the number of attribute values, and the number of pairings involved in this BBS+ signature and accumulator-based anonymous credential is much larger than in CL anonymous credential. There are also some researches[11, 6, 9] about the ABS signature introducing the proofs of predicates such as NOT, AND, OR, and Threshold gates. However, they work in a traceable and linkable way and are not available for anonymous environment. Li constructed OCBE protocols[7, 8] which offers proofs of comparison predicates such as $=$, $\neq$, $\geq$ and $\leq$. Unfortunately, the OCBE protocols for predicates suffer from linear complexity in the binary number of user's attribute values. Bichsel, Camenisch and Preiss[3] showed the details of comparison predicates supported in the Identity Mixer and the U-Prove technologies, which are implemented using Boudot-interval proofs[2] with value complexity. To the best of our knowledge, there has not yet an attributes proof scheme on both logic relations, i.e. AND and OR relations over multiple attributes, and comparison relations, i.e. equality to a given value and lying into a given interval, over some certified attribute, in an untraceable and unlinkable way.

In this paper, we propose a series of attributes proof protocols with the extended pairing-based CL-anonymous credential system. Users are able to prove logic and comparison relations over attributes in an untraceable and unlinkable way. Precisely, they can prove (1) possession of all of the multiple attributes, i.e. AND relation of the attributes. For example, when submitting a resume, a person has to be a female, the nationality is French, and have a Ph.D. degree[4], (2) possession of one of multiple attributes, i.e. OR relation of the attributes. For example, one person can enjoy the free tickets with his ID-card only if his minority is blind or social benefit is unemployed or the type is kids card[4], and (3) comparison predicates over some attribute, the value of which is equal to a given value or lies into a given interval. For example, a junior citizen has to prove that his age is not smaller than 18 when entering a bar.

The organization of the remained is as follows. In section 2, we give the preliminaries about bilinear maps, Pedersen Commitment scheme, DLREP, the CL-anonymous credential system, and the Boudot-interval proof protocols. In section 3, we give the attributes proofs of logic relations and comparison relations over attributes certified in the CL-anonymous credential system. Finally, section 4 is the conclusion.

2 Preliminaries

Before presenting the proposed protocols, we first review a few cryptographic primitives.

2.1 Bilinear Maps

Let G_1 and G_2 be two multiplicative cyclic groups, with an additional group G_T such that $|G_1|=|G_2|=|G_T|$. A bilinear map is a map e: $G_1 \times G_2 \rightarrow G_T$ with the following properties:

- *Bilinear*: for all $u \in G_1, v \in G_2$, and $a, b \in Z_q, e\left(u^a, u^b\right) = e(u,v)^{ab}$
- *Non-degenerate*: $e(g_1, g_2) \neq 1$

2.2 Pedersen Commitment

In the Pedersen Commitment scheme[10], which is an unconditionally hiding and computational binding commitment scheme and based on the discrete logarithm problem, there is a finite multiplicative cyclic group G of prime order q involved along with a generator $g \in G$ and an element $h \in G$ such that it is hard to find an integer α such that $h = g^{\alpha}$. Given a message x, the User picks $r \in_R Z_q$ and computes the commitment $M = g^x h^r$. The User runs a zero-knowledge proof of knowledge protocol to open the commitment without showing the values(x,r):

$$PK\{(x,r) : M = g^x h^r\} \tag{1}$$

2.3 Discrete Logarithm Representation, DLREP

G is a multiplicative cyclic group of prime order q, let $g_0, g_1, ..., g_l$ and y be element of group G. The tuple $(x_0, x_1, ..., x_l) \in Z_q$ is called a DL-representation of the product $y = {g_0}^{x_0} {g_1}^{x_1} \dots {g_l}^{x_l} mod q$ with respect to the generators $(g_0, g_1, ..., g_l)$. The User runs the zero-knowledge proof of knowledge protocol to prove the DL-representation of y.

$$PK\{(x_0, x_1, \dots, x_l) : y = {g_0}^{x_0} {g_1}^{x_1} \dots {g_l}^{x_l}\} \tag{2}$$

2.4 The CL-Anonymous Credential

The CL-anonymous credential is first introduced in[5]. It presents a signature scheme on a block of messages, and provides a protocol to obtain a signature on a committed value that is based solely on discrete-logarithm-related assumptions. The CL-anonymous credential scheme is as follows.

KeyGen. Select bilinear groups G, G' with a prime order q and a bilinear map e, g and g' are generators of group G and G'. Choose $x \in Z_q$,$y \in Z_q$, let $X = g^x, Y = g^y$, and for $1 \le i \le l$, set $Z_i = g^{z_i}$ and $W_i = Y^{z_i}$. Set the secret key $sk = (x, y, z_1, ..., z_l)$, and the public key $pk = (q, G, G', g, g', e, X, Y, \{z_i\}, \{W_i\})$.

Issuance protocol.

Common Input. The public key $pk = (q, G, G', g, g', e, X, Y, \{z_i\}, \{W_i\})$ and a commitment M.

User's Input. Values $m_0, m_1, ..., m_l$ such that $M = g^{m_0} \prod_{i=1}^{l} Z_i^{m_i}$.

Issuer's Input. Signing key $sk = (x, y, \{z_i\})$.

1. The User gives a zero-knowledge proof of the opening of the commitment:

$$PK\{(m_0, \dots, m_l) : M = g^{m_0} \prod_{i=1}^{l} Z_i^{m_i}\} \tag{3}$$

2. The Issuer chooses a random value $\alpha \in_R Z_q$, and sets $a = g^{\alpha}$. Then for $1 \le i \le l$, Let $A_i = a^{z_i}, b = a^y, B_i = (A_i)^y, c = a^x M^{\alpha xy}$ Then the Issuer outputs the signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$ as an anonymous credential.

Showing protocol.

Common Input. The public key $pk = (q, G, G', g, g', e, X, Y, \{z_i\}, \{W_i\})$.

Prover's Input. The blocks of messages $m_0, m_1, ..., m_l$, and signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$.

1. The Prover randomly chooses $r', r'' \in_R Z_q$, then sets:

$$\tilde{a} = a^{r'}, \tilde{A}_i = A_i^{r'}, \tilde{b} = b^{r'}, \tilde{B}_i = B_i^{r'}, \tilde{c} = c^{r'}, \hat{c} = \tilde{c}^{r''}, \text{for} 1 \le i \le l \tag{4}$$

The blinded signature $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$, is distributed independently of everything else. Then the Prover sends the blinded signature $\tilde{\sigma}$ to the Verifier.

2. The Prover and Verifier carry out the following zero-knowledge proof protocol:

$$PK\{(m_0,\ldots,m_l,r'') : e(g,\hat{c})^{1/r''} = e(X,\tilde{a})e(X,\tilde{b})^{m_0}\prod_{i=1}^{l} e(X,\tilde{B}_i)^{m_i}\} \tag{5}$$

3. The Verifier accepts if it accepts the proof above and $\tilde{A}_i$, $\tilde{b}$ and $\tilde{B}_i$ were formed correctly as follows:

$$e(\tilde{a},Z_i) = e\left(g,\tilde{A}_i\right), e(\tilde{a},Y) = e\left(g,\tilde{b}\right), e\left(\tilde{A}_i,Y\right) = e\left(g,\tilde{B}_i\right) \tag{6}$$

2.5 Boudot-Interval Proofs

For the proofs that a committed number lies in an interval, we now list a few proofs of knowledge protocols introduced in[2].

Prove that two commitments hide the same secret. Given two commitments $E = E(x,r_1) = g^x h^{r_1}$ and $F = E(x,r_2) = g^x h^{r_2}$ to the message x. The Prover proves to the Verifier that E and F hide the same secret x as follows:

$$PK\{(x,r_1,r_2) : E = g^x h^{r_1} \wedge F = g^x h^{r_2}\} \tag{7}$$

Prove that a committed number belongs to an interval. Given a commitment $E = E(x,r) = g^x h^r$, the Prover proves to the Verifier that the committed number x belongs to the interval $[a,b]$ as follows:

$$PK\{(x,r) : E = g^x h^r \wedge x \in [a,b]\} \tag{8}$$

3 The Proposed Protocols

In this section, we describe a series of attributes proof protocols based on the CL-anonymous credential system. The anonymous credential system (depicted in Figure 1) allows a user to obtain a credential from an issuer (also denoted as *Identity Provider*) on a number of attributes and prove possession of a credential to a verifier (also denoted as *Relying Party*). They also enable a user to only release and prove a subset of the certified attributes while others are hidden completely.

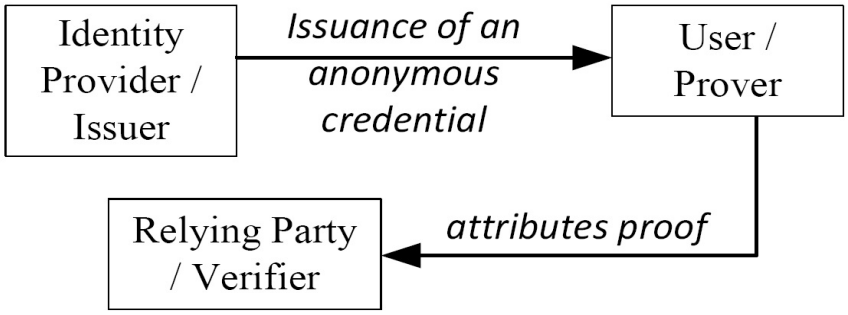


Figure 1: The fundamental structure of anonymous credential systems

When talking about identity attributes or attributes for short, it is important to distinguish between weak and strong attributes[1]. A strong attribute uniquely identifies an individual in a population, whereas a weak attribute can be applied to many individuals in a population. Whether an attribute is

strong or weak depends upon the size of the population and the uniqueness of the identity attribute. Examples of strong attributes are a user's passport number or social security number. Examples of weak attributes are age, profession and gender. The disclosure of their values is not able to break anonymity inherently. However, for minimal information disclosure reason, the proofs of weak attributes still need to guarantee such requirements as follows.

- **Untraceability.** Issuers are unable to trace issued attributes and their owners. In the other word, the issuance of a credential and the showing of a credential are mutually unlinkable. It is able to prevent the insiders of relying parties from tracing the user's transactions.

- **Unlinkability.** Multiple attributes proof sessions of a single user are mutually unlinkable by the Verifiers even they collude.

- **Selective disclosure of attributes.** Users can select which portions of a credential to reveal, which portions to keep hidden, and what relations between certified items are exposed during attribute proofs. It is able to avoid the users from disclose more personal information than necessary.

The attribute proofs need to facilitate such predicate proofs as comparison relations and logic relations. Logic relation proofs refer to prove AND and OR relations over multiple certified attributes. Comparison relation proofs refer to prove the value of a single one attribute equal to a given value and lying into a given interval.

3.1 Extended CL-Anonymous Credential

Before presenting the protocols, we define an extended CL-anonymous credential with the number of l attributes $\{m_1,...,m_l\}$ encoded as messages $m_i \in Z_q$, and a secret value $r \in_R Z_q$ randomly chosen by the user and encoded as message m_0 which is always kept secret during attributes proof. Distinct to the Issuance protocol introduced in section 2.4, the User's input is $(m_1,...,m_l)$ and $\tilde{M}$, where $\tilde{M} = g^r$. Prior to the issuance, the User needs to prove it can open $\tilde{M}$ through a zero-knowledge proof with the Issuer. Then the Issuer certifies the attributes encoded as $M = \tilde{M}\prod_{i=1}^{l} Z_i^{m_i}$.

For simplifying attributes proof, we assume there are not any two types of attributes with identical values. In the other word, we can recognize different types of attributes from the values. Let $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$ be the blinded version of the originally issued signature, formed as Equation 4, that the Prover transforms each time when showing the anonymous credential. The blinded signature is distributed independently of everything else, so the attributes proof meets the requirements of untraceability and unlinkability. For further privacy enhancement, the items in the blinded signature are shuffled and in the different order from the ones in the original signature.

3.2 Logic Relation Proofs

In this section, we show the proofs of AND and OR relations over multiple attributes certified in the CL-anonymous credential system. Before presenting the protocols, we define two sets, *RA* and *RI*. *RA* is specified by the Verifier and made up of the values of the proved attributes. The Prover needs to prove that the values specified in *RA* are certified in the credential. *RI* is specified by the Prover and made up of the indexes of the proved attributes. It indicates which items of the signature, i.e. $(\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$, are corresponding to the proved attributes, so the Verifier can distinguish the proved attributes from others. We also set n the length of *RI* and *RA*, i.e. $n = |RI| = |RA|$.

3.2.1 AND Relation

The Prover is needed to prove that a subset of attributes are all embedded into the user's credential. The AND relation proof implies to reveal the values of the proved attributes in clear.

Common Input. The public key $pk = (q, G, G', g, g', e, X, Y, \{Z_i\}, \{W_i\})$, $RA = \{a_1, ..., a_n\}$, $RI = \{j_1, ..., j_n\}$, $\{m_{j_k} | m_{j_k} = a_k, k \in [1,n], j_k \in RI\}$

Prover's Input. The signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$

Protocol.

1. The Prover generates the blinded signature $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$ as Equation 4, then sends the blinded signature $\tilde{\sigma}$ to the Verifier.

2. The Prover carries out a zero-knowledge proof of a blinded signature,$\tilde{\sigma}$, with the Verifier as follows.

$$PK\{(m_i | i \notin RI, r, r'') : e(X, \tilde{a})^{-1} e(X, \prod_{1 \le i \le l}^{i \in RI} \tilde{B}_i^{m_i})^{-1} = e(g, \hat{c})^{-1/r''} e(X, \tilde{b})^r \prod_{1 \le i \le l}^{i \notin RI} e(X, \tilde{B}_i)^{m_i}\} \tag{9}$$

Along with Equation 6, it is to prove the possession of a valid anonymous credential with n revealed attributes and $l - n$ hidden attributes. If Equation 6 and Equation 9 hold, the AND relation proof outputs TRUE, otherwise FALSE.

3.2.2 OR Relation

The Prover needs to prove that one of the subset of attributes is signed in the credential. Given n items of elementary predicates, i.e. $(m_{j_1} = a_1), ..., (m_{j_n} = a_n)$, the OR relation proof implies to prove one out of n items of elementary predicates holds, i.e. one of the specified attributes $(a_1, ..., a_n)$ is embedded into the user's credential, while the Verifier cannot recognize which one does. It is required that the proved attribute be committed in an information-semantically secure way and retrieved from the credential.

Prior to the proof, the Verifier does some pre-computation. It runs **KeyGen**, introduced in 2.4, to generate a secret key $sk' = (x', y', \{z_i'\})$, and a public key $pk' = (q, G, G', g, g', e, X', Y', \{Z_i'\}, \{W_i'\})$, $1 \le i \le n$, then chooses a random value $r \in_R Z_q$ and uses **Issuance**, introduced in 2.4, to give a signature on the values in RA. Let $\sigma_v = (a', \{A_i'\}, b', \{B_i'\}, c')$ be the signature on $g^{r_v} \prod_{1 \le i \le n} Z_i'^{a_i}$ where $r_v, \alpha' \in_R Z_q, a' = g^{\alpha'}, A_i' = a'^{z_i'}, b' = a'^{y'}, B_i' = A_i'^{y'}, c' = a'^{x'} (g^{r_v} \prod_{1 \le i \le n} Z_i'^{a_i})^{\alpha' x' y'}$.

Common Input. The public key $pk = (q, G, G', g, g', e, X, Y, \{Z_i\}, \{W_i\})$, $RA = \{a_1, ..., a_n\}$. $RI = \{j | 1 \le j \le l\}$, which indicates the proved attribute.

Prover's Input. The signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$.

Protocol.

1. The Prover chooses random values $r', r'' \in_R Z_q$ and generates a blinded version of the signature σ_v, as referred in Equation 4, $\tilde{\sigma}_v = (\tilde{a}', \{\tilde{A}_i'\}, \tilde{b}', \{\tilde{B}_i'\}, \hat{c}')$. Then it chooses random values $r_i \in_R Z_q, 1 \le i \le n$ and computes the Pedersen commitments of each value in RA, i.e. $M_i' = g^{a_i} h^{r_i}, 1 \le i \le n$. Then it sends $\{M_i'\}$ and $\tilde{\sigma}_v$ to the Verifier. Note that the items in the blinded signature $\tilde{\sigma}_v$ need to be shuffled to be in different order from RA, so the Verifier cannot distinguish the values from each other.

2. The Prover carries out a zero-knowledge proof of the blinded signature $\tilde{\sigma}_v$ with the Verifier as follows.

$$PK\{(a_{i_1}, ..., a_{i_n}, r_{i_1}, ..., r_{i_n}, r'') : e(X', \tilde{a}')^{-1} e(X', \tilde{b}'^{r_v})^{-1} = e(g, \hat{c}')^{-1/r''} \prod_{1 \le i_k \le n} e(X', \tilde{B}_{i_k}')^{a_{i_k}}, \{M_{i_k}' = g^{a_{i_k}} h^{r_{i_k}}\}\} \tag{10}$$

Along with Equation 6, it is to prove the validity of an anonymous credential. We refer to Equation 7 to prove that two commitments,$e(X',\tilde{a}')^{-1}e(X',\tilde{b}'^{r_v})^{-1}$ and M'_{i_k}, hide the same secret for each i_k, $1 \leq i_k \leq n$.

3. Assume that m_j is the value of the proved attribute, which is equal to one of the values specified in RA. The Prover chooses a random value $r_j \in_R Z_q$ and computes the Pedersen commitment of m_j, i.e. $M = g^{m_j}h^{r_j}$, then sends M to the Verifier. Note that the items in the blinded signature are in the different order from the ones in the original signature, so the Verifier cannot determine which one the jth attribute actually is.

4. The Prover generates the blinded signature $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$ as Equation 4, then sends the blinded signature $\tilde{\sigma}$ to the Verifier.

5. The Prover carries out a zero-knowledge proof of a blinded signature, $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$, with the Verifier as follows.

$$PK\{(m_1,...,m_l,r,r'',r_j) : e(X,\tilde{a})^{-1} = e(g,\hat{c})^{-1/r''}e\big(X,\tilde{b}\big)^{r}e\big(X,\tilde{B}_j\big)^{m_j}\prod_{1\leq i\leq l}^{i\neq j}e\big(X,\tilde{B}_i\big)^{m_i}, M = g^{m_j}h^{r_j}\} \tag{11}$$

Along with Equation 6, it is to prove the possession of a valid anonymous credential. We refer to Equation 7 to prove that two commitments, $e(X,\tilde{a})^{-1}$ and M, hide the same secret.

6. Assume that the elementary predicate $m_j = a_{i_p}, 1 \leq i_p \leq n$ is chosen to prove by the Prover, the Prover indicates i_p and carries out a zero-knowledge proof of knowledge protocol with the Verifier to prove this predicate.

$$PK\{(r_{i_p}, r_j) : M/M_{i_p}{}' = h^{r_j - r_{i_p}}\} \tag{12}$$

We refer to the Equation 7 to prove that two commitments, M and M'_{i_p}, hide the same secret. If Equation 12 holds, the OR relation proof outputs TRUE, otherwise FALSE.

3.3 Comparison Predicate Proofs

In this section, we show the comparison predicate proofs over some attribute certified in the CL-anonymous credential system. Suppose that the Prover is requested to prove one of his attributes satisfies the specific comparison predicate including equality to a given value and lying into a given interval.

3.3.1 Equality

In order to prove the equality predicate, we need to prove that the value of a certified attribute is equal to a given value. In the other words, proving the equality predicate of a certified attribute implies to revealing the value in clear.

Common Input. The public key $pk = (q, G, G', g, g', e, X, Y, \{Z_i\}, \{W_i\})$, a given value a. $RI = \{j | 1 \leq j \leq l\}$, which indicates the proved attribute.

Prover's Input. The signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$.

Protocol.

1. The Prover generates the blinded signature $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$ as Equation 4, then sends the blinded signature $\tilde{\sigma}$ to the Verifier.

2. The Prover carries out a zero-knowledge proof of a blinded signature, $\tilde{\sigma} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \hat{c})$, with the Verifier as follows.

$$PK\{(m_1,\ldots,m_{j-1},m_{j+1},\ldots,m_l,r,r'') : e(X,\tilde{a})^{-1} e\left(X,\tilde{B}_j^a\right)^{-1} = e(g,\hat{c})^{-1/r''} e\left(X,\tilde{b}\right)^r \prod_{1\le i\le l}^{i\neq j} e(X,\tilde{B}_i)^{m_i}\} \tag{13}$$

Along with Equation 6, it is to prove the possession of a valid anonymous credential with one of the attribute values is equal to a given value. If Equation 6 and Equation 13 hold, the equality proof outputs TRUE, otherwise FALSE.

3.3.2 Interval

The interval proof expresses that the value of a given attribute lies into a given interval. For privacy protection reason, the Prover is able to prove interval predicate without revealing the value of the attribute in clear. The Boudot-interval proofs[2] are applied to construct the protocol. It is required that the proved attribute be committed in an information-semantically secure way and retrieved from the credential.

Common Input. The public key $pk = (q, G, G', g, g', e, X, Y, \{Z_i\}, \{W_i\})$, two given values a and b ,$a < b$. $RI = \{j | 1 \le j \le l\}$, which indicates the proved attribute.

Prover's Input. The signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$.

Protocol.

1. The interval proof is dependent on the given attribute, so the public parameters $\{W_i\}$, where $W_i = Z_i{}^y$,$1 \le i \le l$, referred to the **KeyGen** introduced in 2.4, are used to prove the validity of the proved attribute. The Prover indicates the jth attribute which is to be proved and corresponding to the signature $\tilde{B}_j$ then the Verifier checks the form of $\tilde{B}_j$ to affirm that j truly indicates the proved attribute, while the Prover cannot give a fraudulent substitution of any other attribute in the proof.

$$e\left(\tilde{B}_j, g\right) = e(W_j, \tilde{a}) \tag{14}$$

If it holds, the Verifier affirms the validity of the proved attribute.

2. The Prover chooses a random value $r_j \in_R Z_q$ and computes the Pedersen commitment $M = g^{m_j} h^{r_j}$ on the jth attribute. Then, it sends M to the Verifier.

3. The Prover generates the blinded signature $\tilde{\sigma}$, then sends the blinded signature $\tilde{\sigma}$ to the Verifier.

4. The Prover carries out a zero-knowledge proof of a blinded signature, $\tilde{\sigma}$ with the Verifier as follows.

$$PK\{(m_1,..,m_l,r,r'',r_j) : e(X,\tilde{a})^{-1} = e(g,\hat{c})^{-1/r''} e\left(X,\tilde{b}\right)^r e(X,\tilde{B}_j)^{m_j} \prod_{1\le i\le l}^{i\neq j} e(X,\tilde{B}_i)^{m_i}, M = g^{m_j} h^{r_j}, m_j \in [a,b]\} \tag{15}$$

Along with Equation 6, it is to prove the possession of a valid anonymous credential. We refer to Equation 7 to prove that two commitments, $e(X,\tilde{a})^{-1}$ and M, hide the same secret, and Equation 8 to prove that a committed number m_j lies into the interval $[a,b]$. If Equation 6 and Equation 15 hold, the equality proof outputs TRUE, otherwise FALSE.

4 Conclusion

In this paper, we propose a series of privacy-preserving attributes proof protocols with the extended pairing-based CL-anonymous credential system. Users are able to prove logic and comparison relations over attributes in an untraceable and unlinkable way, at the meanwhile, selectively disclose the minimal personal information to the relying parties. Therefore, the proposed protocols are of identity information leakage prevention. Besides, they can avoid the insiders of relying parties either tracing the user's transaction or impersonating the legal user by showing its credential.

Our further works will focus on inequality proof, where the Verifier cannot even know the interval the proved attribute belongs to. Besides, the linear complexity in the number of attributes during attributes proof will be concerned.

Acknowledgments The first two authors are supported by the Fundamental Research Funds for the Central Universities under Grant No.N100404004 and No. N120404010. The third author is supported by the Fundamental Research Funds for the Central Universities under Grant No.N120417003 and China Natural Science Foundation of Liaoning Province under Grant No.201202069.

References

[1] A. Bhargav-Spantzel, A. C. Squicciarini, R. Xue, and E. Bertino. Multifactor identity verification using aggregated proof of knowledge. *The IEEE Transactions on Systems, Man, and Cybernetics Part C: Applications and Reviews*, 40(4):372–383, July 2010.

[2] F. Boudot. Efficient proofs that a committed number lies in an interval. In *Proc. of the International Conference on the Theory and Application of Cryptographic Techniques Advances in Cryptology (EUROCRYPT'00), Bruges, Belgium, LNCS*, volume 1807, pages 431–444. Springer-Verlag, May 2000.

[3] J. Camenisch and P. Bichsel. A comprehensive framework enabling data-minimizing authentication. In *Proc. of the 7th ACM workshop on Digital identity management (DIM'11), Berlin, Germany*, pages 13–22. ACM, July 2011.

[4] J. Camenisch and T. Groß. Efficient attributes for anonymous credentials. In *Proc. of the 15th ACM conference on Computer and Communications Security (ACM CCS'08), Alexandria, Virginia, USA*, pages 345–356. ACM, December 2012.

[5] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Proc. of the 24th Annual International Cryptology Conference Advances in Cryptology (CRYPTO'04), Santa Barbara, California, USA, LNCS*, volume 3152, pages 56–72. Springer-Verlag, August 2004.

[6] J. Herranz, F. Laguillaumie, B. Libert, and C. Rafols. Short attribute-based signatures for threshold predicates. In *Proc. of the Cryptographers'Track at the RSA Conference 2012 Topics in Cryptology (CT-RSA'12), San Francisco, California, USA, LNCS*, volume 7178, pages 51–67. Springer-Verlag, February-March 2012.

[7] J. Li and N. Li. Oacerts: Oblivious attribute certificates. In *Proc. of the 3th International Conference Applied Cryptography and Network Security (ACNS'05), New York City, New York, USA, LNCS*, volume 3531, pages 301–317. Springer-Verlag, June 2005.

[8] J. Li and N. Li. Ocbe: A construction for general and efficient oblivious commitment based envelope protocols. In *Proc. of the 3th International Conference Information and Communications Security (ICICS'06), Raleigh, North Carolina, USA, LNCS*, volume 4307, pages 122–138. Springer-Verlag, December 2006.

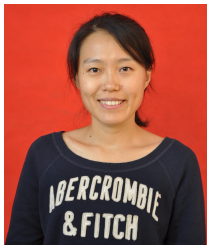
[9] H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures. In *Proc. of the Cryptographers'Track at the RSA Conference 2011 Topics in Cryptology (CT-RSA'11), San Francisco, California, USA, LNCS*, volume 6558, pages 376–392. Springer-Verlag, February 2011.

[10] T. P. Pedersen. Non-interactive and information-theoretic secure veriable secret sharing. In *Proc. of the International Crytology Conference Advances in Cryptology (CRYPTO'91),Verlag Berlin Heidelberg, LNCS*, volume 576, pages 129–140. Springer-Verlag, May 1992.

[11] A. Sudarsono, T. Nakanishi, and N. Funabiki. Efficient attribute-based signatures for non-monotone predicates in the standard model. In *Proc. of the 11th International Symposium Privacy Enhancing Technologies (PETS'11),Waterloo, Ontario, Canada,LNCS*, volume 6794, pages 246–263. Springer-Verlag, July 2011.

[12] A. Sudarsono, T. Nakanishi, and N. Funabiki. Efficient proofs of attributes in pairing-based anonymous credential system. In *Proc. of the 11th International Symposium Privacy Enhancing Technologies (PETS'11), Waterloo, Ontario, Canada, LNCS*, volume 6794, pages 246–263. Springer-Verlag, July 2011.

Author Biography



Nan Guo received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2005, respectively. She joined Northeastern University in September 2005. She has been an associate professor since 2008. She has been a visiting scholar at department of Computer Science, Purdue, from August 2010 to August 2011. She is the author or co-author of more than 30 research publications. Her primary research interest is digital identity management.

Jia Wang received the BE in Computer Science & Technology from Liaoning University, China, in 2011. She is the master candidate in Computer Software and Theory, from Northeastern University, China. Her research interest is digital identity management.

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He is the author or co-author of more than 30 research publications. His primary research interests are next generation network security, MIPv6/HMIPv6 security, wireless mesh network security, Internet security, as well as security and privacy in ubiquitous computing.

Kangbin Yim received his B.S., M.S., and Ph.D. from Ajou University, Suwon, Korea in 1992, 1994 and 2001, respectively. He is currently an associate professor in the Department of Information Security Engineering, Soonchunhyang University. He has served as an executive board member of Korea Institute of Information Security and Cryptology, Korean Society for Internet Information and The Institute of Electronics Engineers of Korea. He also has served as a committee chair of the international conferences and workshops and the guest editor of the journals such as JIT, MIS, JISIS and JoWUA. His research interests include vulnerability assessment, code obfuscation, malware analysis, leakage protection, secure hardware, and systems security. Related to these topics, he has worked on more than fifty research projects and published more than a hundred research papers.