Anonymous Deniable Predicate Authentication Scheme with Revocability *

Hiroaki Anada[1†] and Yoshifumi Ueshige[2]
[1]University of Nagasaki, Nagasaki, Japan
anada@sun.ac.jp
[2]Nagasaki University, Nagasaki, Japan
yueshige@nagasaki-u.ac.jp

Received: May 23, 2021; Accepted: July 24, 2021; Published: August 31, 2021

Abstract

In authentication protocols, anonymity is for privacy, while deniability is for anti-forensics after completion of the protocols. We propose a syntax and security definitions of an anonymous deniable predicate authentication scheme with *revocability* (rADPA). This new cryptographic primitive is to attain revocation function and strong privacy guarantee with predicate authentication, where a predicate is a boolean function over attributes of participants. We also give a generic construction of our rADPA scheme. Our approach is to build-in the revocable attribute-based encryption scheme proposed by K.Yamada et al. (ESORICS2017) into the anonymous deniable predicate authentication scheme proposed by S.Yamada et al. (PKC2012). Finally, we discuss how our rADPA scheme can be instantiated by employing concrete building blocks in our generic construction.

Keywords: anonymous authentication, attribute, deniability, revocation

1 Introduction

For our activity on networks involving private devices, authentication is one of the three fundamental processes for security (i.e. identification, authentication and authorization). We have been receiving benefits of information using communication devices and infrastructures such as smartphones and the internet in our daily lives, and those benefits are basically after logging-in to the networks and devices. There the authentication mechanisms is running with hash functions, symmetric-key schemes, public-key infrastructures and various cryptographic protocols.

Recently, more need of privacy protection is arising among participants of networks. One motivating trend is expansion of social networking services (SNSs). The participants, using pseudonyms, are communicating with each other on the networks, but they are under the fear of being traced and punished due to some unsuitable behaviors. This is actually a serious problem because there are news that famous SNS companies leak personal data of participants in response to demands of governments.

To solve the above problem on privacy protection, we propose a cryptographic scheme which we call an anonymous deniable predicate authentication scheme with revocability (rADPA). An anonymous

Journal of Internet Services and Information Security (JISIS), volume: 11, number: 3 (August 2021), pp. 1-15
DOI:*10.22667/JISIS.2021.08.31.001*

*The preliminary version [2] of this paper was presented at SecITC 2019 under the title "Generic Construction of Anonymous Deniable Predicate Authentication Scheme with Revocability". This paper provides significant technical contributions over [2] at two points. The first point is that it gives detailed procedures of our generic construction. The second point is that it corrects and discusses instantiations of our generic construction in the settings of bilinear groups about which concrete ABE schemes are suitable to be employed and how the schemes are modified so that it can be building blocks.

†Corresponding author: Division of Computer Science, Graduate School of Regional Design and Creation, University of Nagasaki, 1-1-1, Manabino, Nagayo-cho, Nagasaki, 851-2195 Japan, Tel: +81-95-813-5500

authentication is already well-known technique based on tokens issued by authorities. Especially, a cryptographic primitive called *attribute-based encryption scheme (ABE)* [17] can be used to execute an anonymous challenge-and-response authentication protocol. In a key-policy ABE scheme (KP-ABE) introduced by the work of Goyal, Pandey, Sahai and Waters [14, 16], a secret key is associated with an access policy which is a boolean formula over attributes, while a ciphertext is associated with a set of attributes. In a dual manner, in a ciphertext-policy ABE scheme (CP-ABE) [14, 21], a ciphertext is associated with access policy over attributes, while a secret key is associated with a set of attributes. In a KP-ABE or CP-ABE scheme, a secret key works to decrypt a ciphertext if and only if the associated set of attributes satisfies the associated access policy, and hence the challenge-and-response protocol works for a prover to be authenticated based on attributes and policies. This protocol resembles the traditional role-based access control (RBAC). However, the feature of the ABE-based protocol is that it attains *attribute privacy*; in the case of CP-ABE, the verifier in the authentication protocol can not decide which satisfying assignment of attributes is used for a boolean formula after a session, and vice versa in the case of KP-ABE. Attribute privacy is a strong privacy notion, and anonymity is assured by attribute privacy [14]. Currently the notion of an ABE scheme is generalized into a broader notion of a *predicate encryption scheme (PE)* [24], where key attributes and ciphertext attributes are used instead of attributes and policies.

Deniability is a different aspect of privacy protection. As is defined in Dodis et al. [10], a deniable authentication scheme guarantees a seemingly paradoxical property: Upon completion of the protocol the verifier in an authentication server is convinced that the prover is certainly a one who has satisfying key attributes in the case of our scenario. However, neither party can convince anyone else (a third entity) that the other party took part in the protocol. Thus, deniability is a property of anti-forensics, and it is useful for participants who want to feel free of putting any message in SNS without any fear. We stress that deniability is not implied by anonymity, and vice versa. This is because anonymity of a prover might be broken by the server log-data. Nonetheless, deniability guarantees that the log-data can not be witness for the server to claim to a third entity that the prover actually logged in. Conversely, if the timing analysis is executed, then deniability might be broken. Nonetheless, anonymity guarantees that the prover can not be identified among the set of possible provers that have attributes satisfying a policy of the verifier.

Anonymous deniable predicate authentication schemes (ADPAs) with the above two properties were studied by S. Yamada et al. [24]. Actually they gave a generic construction of an ADPA scheme, and discussed instantiations. The idea in [24] is to enhancing the challenge-and-response authentication protocol (which uses a predicate encryption scheme) by adding another four rounds of message-transactions employing a perfectly binding commitment scheme.

1.1 Our Contribution

Following the previous work [24], we further pursue a must function of authentication schemes; that is, *revocation*. In an authentication scheme an authority has to activate a participant, and has to revoke a participant when it is needed in the cases such as expiration of attributes and irregular behavior of participants. To attain the revocability we look into another previous work by K. Yamada et al. [22, 23], in which they proposed a *revocable attribute-based encryption scheme (rABE)*. Combining the previous schemes for our purpose, we propose an *anonymous deniable predicate authentication scheme with revocability (rADPA)*. That is, we substitute the pair of a ciphertext attribute and a revocation list $(Y, \mathscr{RL})$ of rABE with the original ciphertext attribute Y of the predicate encryption scheme. We note that our new scheme is not a trivial combination of two schemes from previous works. This is because we has to check verifiability and chosen-ciphertext security when combining the two schemes, which will be explained in Section 5.

Practicality and Feasibility In a session of our authentication protocol, we need six rounds of interaction between a prover and a verifier. If we would not pursue deniability, then only two rounds were needed (i.e. challenge-and-response). Thus, to attain deniability, we add four more rounds. Computational overhead is mostly occupied by that of encryption-and-decryption of a random message with rABE and that of generation of commitments. More precisely, their asymptotic behaviors are as follows. Let λ be the security parameter and κ be the attribute index. The former is linear to $\lambda \cdot \kappa$, and the latter is linear to λ^2. As for data lengths, they are mostly occupied by that of a ciphertext of rABE and that of 2λ commitments. In the similar way, the former is linear to $\lambda \cdot \kappa$, and the latter is linear to λ^2. However, if we employ a constant-size ciphertext ABE (such as [18, 19]), then the above estimation of asymptotic behaviors changes.

A remark on feasibility is that, in our rADPA scheme, a revocation list $\mathscr{RL}$ can be maintained by a verifier. This feature, which is called *direct revocation* in [23], is actually useful compared with a certificate revocation list (CRL) maintained by a certificate authority (CA).

1.2 Organization of This Paper

In Section 2 we summarize the needed notions and notations. In Section 3 we define the syntax and security of our rADPA. In Section 4 we give a generic construction of our rADPA. In Section 5 we discuss how our rADPA can be instantiated. In Section 6 we conclude our work, and mention our future work.

2 Preliminaries

In this section, we prepare for the needed notations and notions to describe and discuss our scheme in the remaining sections.

The set of natural numbers is denoted by $\mathbb{N}$. The security parameter is denoted by λ, where $\lambda \in \mathbb{N}$. The residue class ring of integers modulo a prime number p is denoted by $\mathbb{Z}_p$. The number of elements of a set S is denoted by $|S|$. The bit length of a string s is denoted by $|s|$. The inverted value of a bit b is denoted by $\bar{b}$ (i.e. $\bar{b} := 1 - b$). A uniform random sampling of an element a from a set S is denoted as $a \in_R S$. The expression $a =_? b$ returns a value 1 when $a = b$ and 0 otherwise. When an algorithm A on input a outputs z, we denote it as $z \leftarrow A(a)$, or, $A(a) \to z$. When a probabilistic algorithm A on input a and with randomness r returns z, we denote it as $z \leftarrow A(a;r)$ When two probabilistic interactive algorithms A and B, on common input x and private input a to A, interact with each other and B outputs z, we denote it as $z \leftarrow \langle A(a), B \rangle(x)$. When an algorithm A accesses an oracle $\mathscr{O}$, we denote it as $A^{\mathscr{O}}$. A probability P is said to be negligible in λ if for any given positive polynomial $\mathrm{poly}(\lambda)$ $P < 1/\mathrm{poly}(\lambda)$ for sufficiently large λ. Two probabilities P and Q are said to be computationally indistinguishable if $|P - Q|$ is negligible in λ, which is denoted as $P \approx_{\mathrm{c}} Q$.

2.1 Terminologies

- $\mathscr{ID} = \{0,1\}^k$: The space of identity strings of bit-length k.
- $m := |\mathscr{ID}|$: The total number of possible identity strings; $m = 2^k$.
- $\mathscr{RL}$: The revocation list, which is a subset of $\mathscr{ID}$.
- B : The upper bound of the number of revoked identity strings. That is, $|\mathscr{RL}|$ should be less than B ($|\mathscr{RL}| < B$).
- κ : The index which describes an attribute set and also a predicate function. $\kappa \in \mathbb{N}^c$ for a constant c.
- $\mathbb{X}^\kappa$: The set of all key attributes under the index κ.
- $\mathbb{Y}^\kappa$: The set of all ciphertext attributes under the index κ.

• $\mathsf{R}^\kappa : \mathbb{X}^\kappa \times \mathbb{Y}^\kappa \to \{0,1\}$: A predicate function on $\mathbb{X}^\kappa \times \mathbb{Y}^\kappa$, which determines a relation under the index κ (i.e. a subset $R^\kappa := \{(X,Y) \in \mathbb{X}^\kappa \times \mathbb{Y}^\kappa \mid \mathsf{R}^\kappa(X,Y) = 1\}$).
• $\mathscr{RF} := \{\mathsf{R}^\kappa\}^{\kappa \in \mathbb{N}^c}$: The family of the predicate functions, that is, a relation family.

2.2 Revocable Attribute-Based Encryption Scheme [22, 23]

A revocable attribute-based encryption scheme rABE is defined with a given relation family $\mathscr{RF}$. rABE consists of four probabilistic polynomial-time algorithms (PPTs for short): $\mathsf{rABE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.
• $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$. This PPT algorithm takes as input the security parameter 1^λ and the attribute index κ which describes a predicate function. It returns a public key PK and a master secret key MSK.
• $\mathsf{KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK}) \to \mathrm{SK}^X_{\mathtt{id}}$. This PPT algorithm takes as input a key attribute X, an identity string $\mathtt{id}$, the public key PK and the master secret key MSK. It returns a private secret key $\mathrm{SK}^X_{\mathtt{id}}$.
• $\mathsf{Enc}((Y, \mathscr{RL}), \mathrm{PK}, M) \to CT$. This PPT algorithm takes as input a ciphertext attribute Y, the revocation list $\mathscr{RL}$, the public key PK and a plaintext M. It returns a ciphertext CT.
• $\mathsf{Dec}(\mathrm{SK}^X_{\mathtt{id}}, (Y, \mathscr{RL}), \mathrm{PK}, CT) \to \tilde{M}$. This deterministic polynomial-time algorithm takes as input a private secret key $\mathrm{SK}^X_{\mathtt{id}}$, the public key PK and a ciphertext CT. It returns a decryption result $\tilde{M}$.

2.2.1 Correctness of Revocable Attribute-Based Encryption Scheme

Correctness of rABE is defined as the correctness as an attribute-based encryption scheme in the following way. First we extend the predicate function R^κ on a key attribute X and a ciphertext attribute Y into $\bar{\mathsf{R}}^\kappa$ by doing substitution $X \leftarrow (X, \mathtt{id})$ and $Y \leftarrow (Y, \mathscr{RL})$ so that $\bar{\mathsf{R}}^\kappa$ captures whether the $\mathtt{id} \in \mathscr{RL}$ holds or not:

$$\bar{\mathsf{R}}^\kappa((X,\mathtt{id}),(Y,\mathscr{RL})) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } \mathsf{R}^\kappa(X,Y) = 1 \wedge \mathtt{id} \notin \mathscr{RL}, \\ 0 \text{ otherwise.} \end{cases}$$

rABE is said to be correct when, for any $\lambda \in \mathbb{N}$, any $\kappa \in \mathbb{N}^c$, any $(X, \mathtt{id}) \in \mathbb{X}^\kappa \times \mathscr{ID}$ and any $(Y, \mathscr{RL}) \in \mathbb{Y}^\kappa \times 2^{\mathscr{ID}}$, s.t. $\bar{\mathsf{R}}^\kappa((X,\mathtt{id}),(Y,\mathscr{RL})) = 1$, and any message M, it holds that $\Pr[M = \tilde{M} \mid \mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK}), \mathsf{Enc}((Y, \mathscr{RL}), \mathrm{PK}, M) \to CT, \mathsf{KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK}) \to \mathrm{SK}^X_{\mathtt{id}}, \mathsf{Dec}(\mathrm{SK}^X_{\mathtt{id}}, (Y, \mathscr{RL}), \mathrm{PK}, CT) \to \tilde{M}] = 1$.

2.2.2 IND-CCA Security of Revocable Attribute-Based Encryption Scheme

Security of indistinguishability against chosen-ciphertext attacks (IND-CCA security) of rABE is defined by the following experimental algorithm on rABE and a given algorithm $\mathbf{A}$.

$$\begin{aligned}
&\mathsf{Expr}^{\text{ind-cca}}_{\mathsf{rABE},\mathbf{A}}(1^\lambda, \kappa) \\
&\quad (\mathrm{PK}, \mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda, \kappa) \\
&\quad ((M_0, M_1), (Y^*, \mathscr{RL}^*), St) \leftarrow \mathbf{A}^{\mathbf{DEC},\mathbf{KG}}(\mathrm{PK}, \kappa) \\
&\quad b \in_R \{0,1\}, CT^* \leftarrow \mathsf{Enc}((Y^*, \mathscr{RL}^*), \mathrm{PK}, M_b),\ b^* \leftarrow \mathbf{A}^{\mathbf{DEC},\mathbf{KG}}(CT^*, St) \\
&\quad \text{If } b = b^* \text{ then return } \textsc{Win} \text{ else return } \textsc{Lose}
\end{aligned}$$

The two chosen plaintexts should be equal length: $|M_0| = |M_1|$. $\mathbf{A}$ accesses two oracles. One is the decryption oracle **DEC**. Sending $((X_i, \mathtt{id}_i), (Y_i, \mathscr{RL}_i, CT_i))$, $\mathbf{A}$ queries **DEC** for the decryption of CT_i. The other is the key-generation oracle **KG**. Sending $(X_j, \mathtt{id}_j)$, $\mathbf{A}$ queries **KG** for a private secret key

$\mathrm{SK}_{\mathtt{id}_j}^{X_j}$. The numbers q_{dec} and q_{key} of the both queries ($i = 1,\ldots,q_{\mathrm{dec}}, j = 1,\ldots,q_{\mathrm{key}}$) are bounded by a polynomial in λ. The declared $(Y^*, \mathscr{RL}^*)$ are called the target ciphertext attribute and the target revocation list, respectively. Two restrictions are imposed: First, $\mathbf{A}$ is not allowed to issue a decryption query $((X_i,\mathtt{id}_i),(Y_i,\mathscr{RL}_i,CT_i))$ s.t. $\bar{\mathsf{R}}^{\kappa}((X_i,\mathtt{id}_i),(Y_i,\mathscr{RL}_i)) = 1$ and $(Y_i,\mathscr{RL}_i,CT_i) = (Y^*,\mathscr{RL}^*,CT^*)$. Second, $\mathbf{A}$ is not allowed to issue a key-extraction query $(X_j,\mathtt{id}_j)$ s.t. $\bar{\mathsf{R}}^{\kappa}((X_j,\mathtt{id}_j),(Y^*,\mathscr{RL}^*)) = 1$. The advantage $\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{rABE},\mathbf{A}}(\lambda,\kappa)$ of $\mathbf{A}$ over rABE is defined as the winning probability: $\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{rABE},\mathbf{A}}(\lambda,\kappa) \stackrel{\text{def}}{=} \Pr[\mathsf{Expr}^{\text{ind-cca}}_{\mathsf{rABE},\mathbf{A}}(1^\lambda,\kappa)$ returns WIN$]$. rABE is said to be IND-CCA secure if, for any given PPT algorithm $\mathbf{A}$, $\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{rABE},\mathbf{A}}(\lambda,\kappa)$ is negligible in λ.

The notion of *semi-adaptive* IND-CCA security [9, 13] is defined by imposing $\mathbf{A}$ to declare the target *after* seeing PK and public parameters but *before* issuing any queries.

$$
\begin{aligned}
&\mathsf{Expr}^{\text{ind-semiad-cca}}_{\mathsf{rABE},\mathbf{A}}(1^\lambda,\kappa)\\
&\quad(\mathrm{PK},\mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda,\kappa),\ ((M_0,M_1),(Y^*,\mathscr{RL}^*),St) \leftarrow \mathbf{A}(\mathrm{PK},\kappa)\\
&\quad b \in_R \{0,1\}, CT^* \leftarrow \mathsf{Enc}((Y^*,\mathscr{RL}^*),\mathrm{PK},M_b),\ b^* \leftarrow \mathbf{A}^{\mathbf{DEC},\mathbf{KG}}(CT^*,St)\\
&\quad\text{If } b = b^* \text{ then return WIN else return LOSE}
\end{aligned}
$$

The advantage $\mathbf{Adv}^{\text{ind-semiad-cca}}_{\mathsf{rABE},\mathbf{A}}(\lambda,\kappa)$ is defined in the same way.

2.2.3 Verifiability of Revocable Attribute-Based Encryption Scheme [24]

Verifiability of rABE is defined as the following property. For any $\lambda \in \mathbb{N}$, any $\kappa \in \mathbb{N}^c$, any $(\mathrm{PK},\mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda,\kappa)$, any $(X,\mathtt{id}),(X',\mathtt{id}') \in \mathbb{X}^\kappa \times \mathscr{ID}$, any $(Y,\mathscr{RL}) \in \mathbb{Y}^\kappa \times 2^{\mathscr{ID}}$, any $\mathrm{SK}^X_{\mathtt{id}} \leftarrow \mathsf{KeyGen}((X,\mathtt{id}),\mathrm{PK},\mathrm{MSK})$ and any $\mathrm{SK}^{X'}_{\mathtt{id}'} \leftarrow \mathsf{KeyGen}((X',\mathtt{id}'),\mathrm{PK},\mathrm{MSK})$, if $\bar{\mathsf{R}}^{\kappa}((X,\mathtt{id}),(Y,\mathscr{RL})) = \bar{\mathsf{R}}^{\kappa}((X',\mathtt{id}'),(Y,\mathscr{RL}))$, then for any $CT \in \{0,1\}^*$ it holds that $\mathsf{Dec}(\mathrm{SK}^X_{\mathtt{id}},(Y,\mathscr{RL}),\mathrm{PK},CT) = \mathsf{Dec}(\mathrm{SK}^{X'}_{\mathtt{id}'},(Y,\mathscr{RL}),\mathrm{PK},CT)$.

2.3 Commitment Scheme [8, 12]

A commitment scheme CmtSch consists of three PPT algorithms: $\mathsf{CmtSch} = (\mathsf{Cmt.Setup},\mathsf{Cmt.Com},\mathsf{Cmt.Open})$. Let $\mathscr{M}$, $\mathscr{R}$ and $\mathscr{C}$ be the message, randomness and commitment spaces, respectively.

• $\mathsf{Cmt.Setup}(1^\lambda) \to \mathrm{CK}$. This PPT algorithm takes as input the security parameter 1^λ. It returns a commitment key CK.

• $\mathsf{Com}(\mathrm{CK},M;\gamma) \to C$. This PPT algorithm takes as input the commitment key CK and a message $M \in \mathscr{M}$. It returns a commitment $C \in \mathscr{C}$ and an opening key $\gamma \in_R \mathscr{R}$ which is the randomness used to generate C.

• $\mathsf{Open}(C,\gamma) \to \hat{M}$. This deterministic polynomial-time algorithm takes as input a commitment $C \in \mathscr{C}$ and the opening key $\gamma \in \mathscr{R}$ It returns an opened message $\hat{M}$ that should be in $\mathscr{M}$.

Correctness should hold for CmtSch (omitted).

Definition 1 (Perfectly Binding [12])**.** *A commitment scheme CmtSch is said to be perfectly binding if it satisfies the following condition for some unbounded algorithm $\mathsf{Cmt.Open}$: For any security parameter 1^λ, any commitment key $CK \leftarrow \mathsf{Cmt.Setup}(1^\lambda)$ and any message M,*

$$\Pr[M = M' \mid (C,\gamma) \leftarrow \mathsf{Cmt.Com}(M;\gamma), M' \leftarrow \mathsf{Cmt.Open}(C)] = 1.$$

Definition 2 (Computationally Hiding [12]). *A commitment scheme* CmtSch *is said to be computationally hiding if it satisfies the following condition: For any security parameter* 1^λ*, any commitment key* $CK \leftarrow \mathsf{Cmt.Setup}(1^\lambda)$ *and any* PPT *algorithm* $\mathbf{A}$*,*

$$\begin{aligned}&\Pr[\mathbf{A}(St,C)=1 \mid (M,M',St)\leftarrow \mathbf{A}(CK),(C,\gamma)\leftarrow \mathsf{Cmt.Com}(M)]\\ \approx_c\ &\Pr[\mathbf{A}(St,C')=1 \mid (M,M',St)\leftarrow \mathbf{A}(CK),(C',\gamma')\leftarrow \mathsf{Cmt.Com}(M')].\end{aligned} \tag{1}$$

3 Syntax and Security Definitions of Anonymous Deniable Predicate Authentication Scheme with Revocability

In this section, we give a syntax of an anonymous deniable predicate authentication scheme that has the function of revocability. We denote the scheme by rADPA. Then we define three security notions: concurrent soundness, anonymity and deniability. The syntax and security definitions are in accordance with the previous work [24].

3.1 Syntax

Our rADPA consists of four PPTs: $\mathsf{rADPA}=(\mathsf{Setup},\mathsf{KeyGen},\mathsf{P},\mathsf{V})$.

• $\mathsf{Setup}(1^\lambda,\kappa)\rightarrow(\mathrm{PK},\mathrm{MSK})$. This PPT algorithm takes as input the security parameter 1^λ and the attribute index κ which describes a predicate function. It returns a public key PK and a master secret key MSK.

• $\mathsf{KeyGen}((X,\mathtt{id}),\mathrm{PK},\mathrm{MSK})\rightarrow \mathrm{SK}^X_{\mathtt{id}}$. This PPT algorithm takes as input a key attribute X, an identity string $\mathtt{id}$, the public key PK and the master secret key MSK. It returns a private secret key $\mathrm{SK}^X_{\mathtt{id}}$.

• $\langle\mathsf{P}(\mathrm{SK}^X_{\mathtt{id}}),\mathsf{V}\rangle((Y,\mathscr{RL}),\mathrm{PK})\rightarrow 1/0$. These interactive PPT algorithms take as common input a ciphertext attribute and a revocation list $(Y,\mathscr{RL})$ and the public key PK, and as private input to P a private secret key $\mathrm{SK}^X_{\mathtt{id}}$. P and V interact with each other for at most a polynomial number of rounds in λ. Then V finally returns a decision 1 or 0.

3.2 Security Definitions

3.2.1 Concurrent Soundness

Intuitively, concurrent soundness means security against misauthentication caused by an adversary which does not have a satisfying private secret key. Formally a definition is given via the following experimental algorithm $\mathsf{Expr}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}$.

$$\begin{aligned}&\mathsf{Expr}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\\ &(\mathrm{PK},\mathrm{MSK})\leftarrow\mathsf{Setup}(1^\lambda,\kappa),\ ((Y^*,\mathscr{RL}^*),St)\leftarrow\mathbf{A}^{\mathbf{P}_i(\mathrm{SK}^{X_i}_{\mathtt{id}_i})|_{i=1}^{q_\mathrm{P}},\mathbf{KG}}(\mathrm{PK},\kappa)\\ &b\leftarrow\langle\mathbf{A}^{\mathbf{P}_i(\mathrm{SK}^{X_i}_{\mathtt{id}_i})|_{i=1}^{q_\mathrm{P}},\mathbf{KG}}(St),\mathsf{V}\rangle((Y^*,\mathscr{RL}^*),\mathrm{PK})\\ &\text{If } b=1 \text{ then return WIN else return LOSE}\end{aligned}$$

Two restrictions are imposed: First, $\mathbf{A}$ is not allowed to relay the messages even in partial. Second, $\mathbf{A}$ is not allowed to issue a key-extraction query $(X_j,\mathtt{id}_j)$ s.t. $\bar{\mathsf{R}}^\kappa((X_j,\mathtt{id}_j),(Y^*,\mathscr{RL}^*))=1$.

The advantage $\mathbf{Adv}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ of $\mathbf{A}$ over rADPA is defined as the winning probability: $\mathbf{Adv}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)\stackrel{\text{def}}{=}\Pr[\mathsf{Expr}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\text{ returns WIN}]$. rADPA is said to be (adaptively) concurrently sound if, for any given PPT algorithm $\mathbf{A}$, $\mathbf{Adv}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ is negligible in λ.

The notion of *semi-adaptive* concurrent soundness is defined by imposing $\mathbf{A}$ to declare the target *after* seeing PK and public parameters but *before* issuing any queries.

$$\begin{aligned}
&\mathsf{Expr}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\\
&(\mathrm{PK},\mathrm{MSK})\leftarrow \mathsf{Setup}(1^\lambda,\kappa),\ ((Y^*,\mathscr{RL}^*),St)\leftarrow \mathbf{A}(\mathrm{PK},\kappa)\\
&b\leftarrow \langle \mathbf{A}^{\mathbf{P}_i(\mathrm{SK}^{X_i}_{\mathtt{id}_i})|^{q_\mathrm{P}}_{i=1},\mathbf{KG}}(St),\mathsf{V}\rangle((Y^*,\mathscr{RL}^*),\mathrm{PK})\\
&\text{If } b=1 \text{ then return } \textsc{Win} \text{ else return } \textsc{Lose}
\end{aligned}$$

The advantage $\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ is defined in the same way.

$$\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)\stackrel{\text{def}}{=}\Pr[\mathsf{Expr}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\text{ returns }\textsc{Win}].$$

3.2.2 Anonymity

Intuitively, anonymity means privacy which is indistinguishability between satisfying two patterns of key attributes. Formally a definition is given via the following experimental algorithm $\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}$.

$$\begin{aligned}
&\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\\
&(\mathrm{PK},\mathrm{MSK})\leftarrow \mathsf{Setup}(1^\lambda,\kappa)\\
&((X^*_0,\mathtt{id}^*_0),(X^*_1,\mathtt{id}^*_1),St)\leftarrow \mathbf{A}(\mathrm{PK},\mathrm{MSK})\\
&\mathrm{SK}^{X^*_0}_{\mathtt{id}^*_0}\leftarrow \mathsf{KeyGen}((X^*_0,\mathtt{id}^*_0),\mathrm{PK},\mathrm{MSK}),\mathrm{SK}^{X^*_1}_{\mathtt{id}^*_1}\leftarrow \mathsf{KeyGen}((X^*_1,\mathtt{id}^*_1),\mathrm{PK},\mathrm{MSK})\\
&((Y^*,\mathscr{RL}^*),St)\leftarrow \mathbf{A}(St,\mathrm{SK}^{X^*_0}_{\mathtt{id}^*_0},\mathrm{SK}^{X^*_1}_{\mathtt{id}^*_1})\text{ s.t.}\\
&\ \bar{\mathsf{R}}^\kappa((X^*_0,\mathtt{id}^*_0),(Y^*,\mathscr{RL}^*))=\bar{\mathsf{R}}^\kappa((X^*_1,\mathtt{id}^*_1),(Y^*,\mathscr{RL}^*))\\
&b\in_R\{0,1\},b^*\leftarrow \mathbf{A}^{\mathbf{P}(\mathrm{SK}^{X^*_b}_{\mathtt{id}^*_b})}(St)\\
&\text{If } b=b^* \text{ then return } \textsc{Win} \text{ else return } \textsc{Lose}
\end{aligned}$$

The advantage $\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ of $\mathbf{A}$ over rADPA is defined as the winning probability: $\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)\stackrel{\text{def}}{=}\left|\Pr[\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\text{ returns }\textsc{Win}]-\frac{1}{2}\right|$. rADPA is said to have anonymity if, for any given PPT algorithm $\mathbf{A}$, $\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ is negligible in λ.

3.2.3 Deniability

Intuitively, deniability means privacy which states anti-forensic property that a third party is not able to confirm whether a prover actually participate in the authentication protocol. Formally a definition is given via the indistinguishability of the following two probability distributions Real and Sim, where $\mathbf{A}$ is any given algorithm and S is an adaptively given algorithm to $\mathbf{A}$.

$$\begin{aligned}
\mathrm{Real}(\lambda,\kappa,(X,\mathtt{id}),(Y,\mathscr{RL}))&\stackrel{\text{def}}{=}\mathsf{View}\big(\langle \mathsf{P}(\mathrm{SK}^X_{\mathtt{id}}),\mathbf{A}\rangle((Y,\mathscr{RL}),\mathrm{PK})\\
&\qquad\big|\ \mathsf{Setup}(1^\lambda,\kappa)\to(\mathrm{PK},\mathrm{MSK});\mathsf{KeyGen}((X,\mathtt{id}),\mathrm{MSK})\to\mathrm{SK}^X_{\mathtt{id}}\big),\\
\mathrm{Sim}(\lambda,\kappa,(X,\mathtt{id}),(Y,\mathscr{RL}))&\stackrel{\text{def}}{=}\mathsf{View}\big(\langle \mathsf{S},\mathbf{A}\rangle((Y,\mathscr{RL}),\mathrm{PK})\\
&\qquad\big|\ \mathsf{Setup}(1^\lambda,\kappa)\to(\mathrm{PK},\mathrm{MSK});\mathsf{KeyGen}((X,\mathtt{id}),\mathrm{MSK})\to\mathrm{SK}^X_{\mathtt{id}}\big).
\end{aligned}$$

rADPA is said to have deniability if, for any given PPT algorithm $\mathbf{A}$, there exists a PPT algorithm S s.t. for any given PPT algorithm $\mathbf{D}$ it holds that

$$\begin{aligned}&\Pr[\mathbf{D}(\mathrm{Real}(\lambda,\kappa,(X,\mathtt{id}),(Y,\mathscr{RL})))=1]\\ \approx_{\mathrm{c}}&\Pr[\mathbf{D}(\mathrm{Sim}(\lambda,\kappa,(X,\mathtt{id}),(Y,\mathscr{RL})))=1].\end{aligned}$$

4 Generic Construction of Anonymous Deniable Predicate Authentication Scheme with Revocability

In this section, we give a generic construction of an rADPA scheme in Section 3 following the idea of previous work [24].

4.1 Construction

The idea in [24], which originates from the work of Naor [15], is to combine an IND-CCA secure verifiable predicate encryption scheme with a perfectly binding commitment scheme. In our case, we follow the above idea, but we employ a revocable attribute-based encryption scheme rABE as the predicate encryption scheme. That is, we substitute the original ciphertext attribute Y of the predicate encryption scheme with the pair of a ciphertext attribute and a revocation list $(Y,\mathscr{RL})$ of rABE.

Intuitively, the prototype of rADPA is a challenge-and-response protocol in which rABE is employed. Then we modify it by, for each $i=1$ to λ, dividing the "response" $\tilde{r}$ into two random strings r_{i0} and r_{i1} with a linear constraint $\tilde{r}=r_{i0}\oplus r_{i1}$. Then we execute "commit and open" protocol with randomly selected bits b_i for $i=1$ to λ.

Formally, the four PPT algorithms Setup, KeyGen, P and V of our scheme rADPA are generically constructed as follows.

• $\mathsf{Setup}(1^\lambda,\kappa)\to(\mathrm{PK},\mathrm{MSK})$. On input the security parameter 1^λ and the attribute index κ, the algorithm executes rABE.Setup with the same input to obtain a pair of a public key PK and a master secret keyMSK. It returns $(\mathrm{PK},\mathrm{MSK})$.

• $\mathsf{KeyGen}((X,\mathtt{id}),\mathrm{PK},\mathrm{MSK})\to \mathrm{SK}^X_{\mathtt{id}}$. On input a key attribute $(X,\mathtt{id})$, the public key PK and the master secret key MSK, the algorithm executes rABE.KeyGen with the same input to obtain a private secret key $\mathrm{SK}^X_{\mathtt{id}}$.

• $\langle \mathsf{P}(\mathrm{SK}^X_{\mathtt{id}}),\mathsf{V}\rangle((Y,\mathscr{RL}),\mathrm{PK})\to 1/0$. On common input a ciphertext attribute $(Y,\mathscr{RL})$ and the public key PK and private input a private secret key $\mathrm{SK}^X_{\mathtt{id}}$ to the prover P, first the verifier V chooses a random string $r\in_R\{0,1\}^\lambda$, and executes the encryption algorithm for the plaintext r with the randomness ρ $\mathsf{rABE.Enc}((Y,\mathscr{RL}),\mathrm{PK},r;\rho)$. Then V sends the ciphertext CT to P.

Second, receiving the ciphertext CT, the prover P executes the decryption algorithm $\mathsf{rABE.Dec}(\mathrm{SK}^X_{\mathtt{id}},(Y,\mathscr{RL}),\mathrm{PK},CT)$, and obtains the decryption result $\tilde{r}$. If $\tilde{r}=\perp$, then for $i=1$ to λ P chooses pairs of random strings $(r_{i0},r_{i1})\in_R\{0,1\}^\lambda\times\{0,1\}^\lambda$ to be committed. Otherwise, for $i=1$ to λ P chooses a random string $r_{i0}\in_R\{0,1\}^\lambda$ and computes $r_{i1}:=\tilde{r}\oplus r_{i0}$ (i.e. linear constraint). Then, for $i=1$ to λ and for $j=0,1$ P computes a commitment $C_{ij}\leftarrow\mathsf{Com}(r_{ij};\gamma_{ij})$ with a randomness $\gamma_{ij}\in_R\mathscr{R}$. P sends all the commitments $(C_{ij})^{1\le i\le\lambda}_{j=0,1}$ to the verifier V.

Third, receiving the commitments, the verifier V chooses for $i=1$ to λ the coins $b_i\in_R\{0,1\}$, and sends those coins to the prover P.

Fourth, receiving the coins, the prover P for $i=1$ to λ opens the commitment C_{ib_i} by using the randomness γ_{ib_i} as the opening key to get opened value $\hat{r}_{ib_i}$. P sends all the opened values together with the opening keys $(\hat{r}_{ib_i},\gamma_{ib_i})^{1\le i\le\lambda}$ to the verifier V.

Fifth, receiving the opened values together with the opening keys, the verifier V sends the random plaintext r and the randomness ρ for encryption to the prover P.

Sixth, receiving the random plaintext r and the randomness ρ, the prover P for $i = 1$ to λ opens the remaining commitment $C_{i\bar{b}_i}$ by using the randomness $\gamma_{i\bar{b}_i}$ as the opening key to get opened value $\hat{r}_{i\bar{b}_i}$. P sends all the opened values together with the opening keys $(\hat{r}_{i\bar{b}_i}, \gamma_{i\bar{b}_i})^{1\leq i\leq\lambda}$ to the verifier V.

Finally, receiving the opened values together with the opening keys, the verifier V for $i = 1$ to λ checks whether the following expected linear constraint holds or not: $r =_? r_{i0} \oplus r_{i1}$. If all the equations holds, then V returns 1 (accept), and otherwise, 0 (reject).

Fig.1 shows our construction of rADPA.

4.2 Security

The following three theorems are direct consequences of the corresponding theorems of Yamada et al. [24] because our rADPA is their anonymous deniable predicate authentication scheme because our attributes $(X, \mathtt{id})$ and $(Y, \mathscr{R}\mathscr{L})$ can be seen as a key attribute and a ciphertext attribute for our extended predicate function $\bar{\mathsf{R}}^{\kappa}$. Therefore, we give a proof only for the corollary that is for the case of semi-adaptive security.

Theorem 1 (Concurrent Soundness [24])**.** *If rABE is IND-CCA secure and verifiable, and if Com is perfectly binding, then our rADPA is concurrently sound. More precisely, for any given* PPT *algorithm* $\mathbf{A}$ *which is in accordance with* $\mathsf{Expr}^{c\text{-}sound}_{rADPA,\mathbf{A}}(\lambda,\kappa)$*, there exists a* PPT *algorithm* $\mathbf{B}$ *such that the following inequality holds.*

$$\mathbf{Adv}^{c\text{-}sound}_{rADPA,\mathbf{A}}(\lambda,\kappa) < \mathbf{Adv}^{ind\text{-}cca}_{rABE,\mathbf{B}}(\lambda,\kappa) \tag{2}$$

Corollary 1 (Semi-adaptive Concurrent Soundness)**.** *If rABE is semi-adaptively IND-CCA secure and verifiable, and if Com is perfectly binding, then our rADPA is semi-adaptively and concurrently sound. More precisely, for any given* PPT *algorithm* $\mathbf{A}$ *which is in accordance with* $\mathsf{Expr}^{semiad\text{-}c\text{-}sound}_{rADPA,\mathbf{A}}(\lambda,\kappa)$*, there exists a* PPT *algorithm* $\mathbf{B}$ *such that the following inequality holds.*

$$\mathbf{Adv}^{semiad\text{-}c\text{-}sound}_{rADPA,\mathbf{A}}(\lambda,\kappa) < \mathbf{Adv}^{ind\text{-}semiad\text{-}cca}_{rABE,\mathbf{B}}(\lambda,\kappa) \tag{3}$$

Proof. This is straightforward because the discussion of semi-adaptiveness is independently applied to the proof of Theorem 1. □

Theorem 2 (Anonymity [24])**.** *If rABE is IND-CCA secure and verifiable, then our rADPA has anonymity. More precisely, for any given unbounded algorithm* $\mathbf{A}$ *the following equality holds.*

$$\mathbf{Adv}^{anonym}_{rADPA,\mathbf{A}}(\lambda,\kappa) = 0 \tag{4}$$

Theorem 3 (Deniability [24])**.** *If rABE is correct, and if Com is computationally hiding, then our rADPA has deniability. More precisely, for any given* PPT *algorithm* $\mathbf{D}$ *the following inequality holds.*

$$\Pr[\mathbf{D}(\mathit{Real}(\lambda,\kappa,(X,\mathtt{id}),(Y,\mathscr{R}\mathscr{L}))) = 1] \tag{5}$$

$$\approx_c \Pr[\mathbf{D}(\mathit{Sim}(\lambda,\kappa,(X,\mathtt{id}),(Y,\mathscr{R}\mathscr{L}))) = 1]. \tag{6}$$

$\mathsf{Setup}(1^\lambda, \kappa)$		$\mathsf{KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK})$
$\mathsf{rABE.Setup}(1^\lambda, \kappa)$		$\mathsf{rABE.KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK})$
$\to (\mathrm{PK}, \mathrm{MSK})$		$\to \mathrm{SK}^X_{\mathtt{id}}$
return $(\mathrm{PK}, \mathrm{MSK})$		return $\mathrm{SK}^X_{\mathtt{id}}$
$\mathsf{P}(\mathrm{SK}^X_{\mathtt{id}}, (Y, \mathscr{RL}), \mathrm{PK})$		$\mathsf{V}((Y, \mathscr{RL}), \mathrm{PK})$
		$r \in_R \{0,1\}^\lambda$
		$\mathsf{rABE.Enc}((Y, \mathscr{RL}), \mathrm{PK}, r; \rho)$
		$\to CT$
	CT	
$\mathsf{rABE.Dec}(\mathrm{SK}^X_{\mathtt{id}}, (Y, \mathscr{RL}), \mathrm{PK}, CT)$	$\leftarrow$	
$\to \tilde{r}$		
If $\tilde{r} = \perp$ then		
For $i = 1$ to λ:		
$(r_{i0}, r_{i1}) \in_R \{0,1\}^\lambda \times \{0,1\}^\lambda$		
else		
For $i = 1$ to λ:		
$r_{i0} \in_R \{0,1\}^\lambda, r_{i1} := \tilde{r} \oplus r_{i0}$		
For $i = 1$ to λ:		
For $j = 0, 1$:		
$\gamma_{ij} \in_R \mathscr{R}, \mathsf{Com}(r_{ij}; \gamma_{ij}) \to C_{ij}$		
	$(C_{ij})^{1 \le i \le \lambda}_{j=0,1}$	
	$\to$	For $i = 1$ to λ:
		$b_i \in_R \{0,1\}$
	$(b_i)^{1 \le i \le \lambda}$	
For $i = 1$ to λ:	$\leftarrow$	
$\mathsf{Open}(C_{ib_i}, \gamma_{ib_i}) \to \hat{r}_{ib_i}$		
	$(\hat{r}_{ib_i}, \gamma_{ib_i})^{1 \le i \le \lambda}$	
	$\to$	
	(r, ρ)	
For $i = 1$ to λ:	$\leftarrow$	
$\mathsf{Open}(C_{i\bar{b}_i}, \gamma_{i\bar{b}_i}) \to \hat{r}_{i\bar{b}_i}$		
	$(\hat{r}_{i\bar{b}_i}, \gamma_{i\bar{b}_i})^{1 \le i \le \lambda}$	
	$\to$	For $i = 1$ to λ:
		$r =_? r_{i0} \oplus r_{i1}$
		If all eqs. hold then return 1
		else return 0

Figure 1: Our generic construction of anonymous deniable predicate authentication scheme with revocability, rADPA.

Table 1: Instantiations

IND-CCA Secure rABE ABE (Flavor), IBR	CmtSch	Verifiability	Message Len.	Security	Assumptions
[3, 24] (KP-ABE), [3]	EG [11]	via [24]	const.	adap.	mat-DH, EDHE
[3, 24] (KP-ABE), [6]	EG [11]	via [24]	const.	adap.	mat-DH, EDHE
[19, 24] (KP-ABE), [3]	EG [11]	via [24]	const.	semi-adap.	DLIN
[19, 24] (KP-ABE), [6]	EG [11]	via [24]	const.	semi-adap.	DLIN
[1, 24](CP-ABE), [3]	EG [11]	via [24]	const.	semi-adap.	SXDH, EDHE
[1, 24](CP-ABE), [6]	EG [11]	via [24]	const.	semi-adap.	SXDH, EDHE
[19, 5, 24] (CP-ABE), [3]	EG [11]	via [24]	const.	semi-adap.	DLIN
[19, 5, 24] (CP-ABE), [6]	EG [11]	via [24]	const.	semi-adap.	DLIN

5 Discussion on Instantiations

In this section, we discuss how our generic construction of rADPA in Section 4 is instantiated in the setting of bilinear groups (see, for example, [20]).

Our rADPA consists of the two building blocks: rABE and CmtSch. According to Theorem 1, 2 and 3 in Section 4, we need the correctness, IND-CCA security and verifiability for rABE and the perfectly binding and computationally hiding properties for CmtSch. Further, according to the first construction of rABE proposed in [22, 23], we are able to construct rABE from an attribute-based encryption scheme (ABE) and an identity-based revocation scheme (IBR) in the pair encoding framework [3], which combines ABE and IBR via the generic conjunctive conversion [7]. Note here that we have to apply the CPA-to-CCA technique [24] to the component ABE scheme if it is needed. Thanks to the functionality-preserving property [22, 23], if ABE is correct and IND-CCA secure, then so is the converted rABE.

As for verifiability, the adaptively or semi-adaptively secure ABE schemes which depend on the dual-system encryption technique [20, 4] are not verifiable in their proposed forms. However, they can be modified into verifiable schemes (as is mentioned in [24]). That is, a prover P is given *two* private secret keys $\mathrm{SK}_{\mathrm{id}}^{X}$ and $\mathrm{SK}_{\mathrm{id}}^{\prime X}$ with *different* randomness in the key generation phase. In the decryption phase, the two keys are used independently for a single ciphertext; if the result is the same, then the verification output is 1 (legitimate), and otherwise, 0 (illegitimate). Hence we obtain verifiable adaptively or semi-adaptively IND-CCA secure rABE, respectively.

Among possible instantiations, we are interested in semi-adaptively secure rABE with constant size ciphertexts. This is because, in the semi-adaptive security model, adversaries choose the target (in our case $(Y^*, \mathscr{RL}^*)$) after seeing a public key PK and before issuing any queries. This model is natural and sufficient in the case of *authentication* (see Section 2.2.2), which makes a contrast to the case of encryption. As for constant-size property of ciphertexts, when an authentication scheme is applied in a real network protocol, the message length should preferably be constant. There are adaptively or semi-adaptively secure ABE schemes with constant size ciphertexts in the flavor of key-policy (KP) and ciphertext-policy, such as KP-ABE schemes of Attrapadung [3] and Takashima [19] and CP-ABE schemes of Agrawal and Chase [1] and Takashima [19] with the KP-to-CP transform of Attrapadung et al. [5]. Also, there are IBR schemes with constant size ciphertexts [3, 6]. Hence we can actually instantiate our rADPA with constant message length. In that cases the IND-CCA securities of ABE and IBR are under the matrix Diffie-Hellman assumption (mat-DH) or the symmetric external Diffie-Hellman (SXDH) and the extended DH exponent assumption (EDHE), or, the decisional linear assumption (DLIN), respectively (see Table 1).

As for a commitment scheme CmtSch with the perfectly binding and computationally hiding properties, we can employ the ElGamal encryption scheme (EG) [11]. The computationally hiding prop-

$\mathsf{Setup}(1^\lambda, \kappa)$		$\mathsf{KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK})$
$\mathsf{ABE.Setup}(1^\lambda, \kappa)$		$\mathsf{ABE.KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK})$
$\to (\mathrm{PK}, \mathrm{MSK})$		$\to \mathrm{SK}_{X,\mathtt{id}}$
return $(\mathrm{PK}, \mathrm{MSK})$		return $\mathrm{SK}_{X,\mathtt{id}}$
$\mathsf{P}(\mathrm{SK}_{X,\mathtt{id}}, (Y, \mathscr{RL}), \mathrm{PK})$		$\mathsf{V}((Y, \mathscr{RL}), \mathrm{PK})$
		$r \in_R \mathbb{G}_T$
		$\mathsf{ABE.Enc}((Y, \mathscr{RL}), \mathrm{PK}, r; \rho)$
		$\to CT$
	CT	
$\mathsf{ABE.Dec}(\mathrm{SK}_{X,\mathtt{id}}, (Y, \mathscr{RL}), \mathrm{PK}, CT)$	$\leftarrow$	
$\to \tilde{r}$		
If $\tilde{r} = \perp$ then		
For $i = 1$ to λ:		
$(r_{i0}, r_{i1}) \in_R \mathbb{G}_T \times \mathbb{G}_T$		
else		
For $i = 1$ to λ:		
$r_{i0} \in_R \mathbb{G}_T, r_{i1} := \tilde{r} \cdot r_{i0}^{-1}$		
For $i = 1$ to λ:		
For $j = 0, 1$:		
$\gamma_{ij} \in_R \mathbb{G}_T, \mathsf{Com}(r_{ij}; \gamma_{ij}) \to C_{ij}$		
	$(C_{ij})_{j=0,1}^{1 \le i \le \lambda}$	
	$\to$	For $i = 1$ to λ:
		$b_i \in_R \{0, 1\}$
	$(b_i)^{1 \le i \le \lambda}$	
For $i = 1$ to λ:	$\leftarrow$	
$\mathsf{Open}(C_{ib_i}, \gamma_{ib_i}) \to \hat{r}_{ib_i}$		
	$(\hat{r}_{ib_i}, \gamma_{ib_i})^{1 \le i \le \lambda}$	
	$\to$	
	(r, ρ)	
For $i = 1$ to λ:	$\leftarrow$	
$\mathsf{Open}(C_{i\bar{b}_i}, \gamma_{i\bar{b}_i}) \to \hat{r}_{i\bar{b}_i}$		
	$(\hat{r}_{i\bar{b}_i}, \gamma_{i\bar{b}_i})^{1 \le i \le \lambda}$	
	$\to$	For $i = 1$ to λ:
		$r =_? r_{i0} \cdot r_{i1}$
		If all eqs. hold then return 1
		else return 0

Figure 2: Instantiation of our generic rADPA in the setting of bilinear groups.

erty is obtained from the indistinguishability against chosen-plaintext attacks, which is under the Diffie-Hellman assumption (DH). Note that the DH assumption is implied from the mat-DH assumption.

Table 1 summarizes the above discussion, and Figure 2 shows the instantiation in the setting of bilinear groups.

6 Conclusion

We proposed an anonymous deniable predicate authentication scheme with revocability, rADPA, which has strong privacy protection properties. We gave the syntax and formal security definitions of rADPA; concurrent soundness, anonymity and deniability. Then we showed a generic construction of rADPA, whose building blocks are a revocable attribute-based encryption scheme, rABE, and a commitment scheme, CmtSch. We stated that, when rABE and CmtSch have suitable properties, then our rADPA

attains the security properties. Finally, we discussed how our generic construction of rADPA is instantiated. Our future work would be a feasibility study of our rADPA by implementation. Also, we have to examine how the six-round authentication protocol of our rADPA is feasible in real scenarios in the internet.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP18K11297. We would like to express our sincere thanks to Keita Emura for his suggestions on the semi-adaptive security. We would also like to express our sincere thanks to Nuttapong Attrapadung for his comments on the instantiations.

References

[1] S. Agrawal and M. Chase. A study of pair encodings: Predicate encryption in prime order groups. In *Proc. of the 13th International Conference on Theory of Cryptography (TCC'16-A), Tel Aviv, Israel*, volume 9563 of *Lecture Notes in Computer Science*, pages 259–288. Springer-Verlag, January 2016.

[2] H. Anada and Y. Ueshige. Generic construction of anonymous deniable predicate authentication scheme with revocability. In *Proc. of the 12th International Conference on Innovative Security Solutions for Information Technology and Communications (SecITC'19), Bucharest, Romania*, volume 12001 of *Lecture Notes in Computer Science*, pages 142–155. Springer-Verlag, February 2020.

[3] N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In *Proc. of the 33rd International Conference on Advances in Cryptology (EUROCRYPT'14), Copenhagen, Denmark*, volume 8441 of *Lecture Notes in Computer Science*, pages 557–577. Springer-Verlag, May 2014.

[4] N. Attrapadung. Dual system encryption framework in prime-order groups via computational pair encodings. In *Proc. of 22nd International Conference on Advances in Cryptology (ASIACRYPT'16), Hanoi, Vietnam*, volume 10032 of *Lecture Notes in Computer Science*, pages 591–623. Springer-Verlag, December 2016.

[5] N. Attrapadung, G. Hanaoka, and S. Yamada. Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs. In *Proc. of the 21st International Conference on Advances in Cryptology (ASIACRYPT'15), Auckland, New Zealand*, volume 9452 of *Lecture Notes in Computer Science*, pages 575–601. Springer-Verlag, November 2015.

[6] N. Attrapadung, B. Libert, and E. de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC'11), Taormina, Italy*, volume 6571 of *Lecture Notes in Computer Science*, pages 90–108. Springer-Verlag, March 2011.

[7] N. Attrapadung and S. Yamada. Duality in ABE: converting attribute based encryption for dual predicate and dual policy via computational encodings. In *Proc. of The Cryptographer's Track at the RSA Conference 2015, (CT-RSA'15), San Francisco, California, USA*, volume 9048 of *Lecture Notes in Computer Science*, pages 87–105. Springer-Verlag, April 2015.

[8] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, October 1988.

[9] J. Chen and H. Wee. Semi-adaptive attribute-based encryption and improved delegation for boolean formula. In *Proc. of the 9th International Conference on Security and Cryptography for Networks (SCN'14), Amalfi, Italy*, volume 8642 of *Lecture Notes in Computer Science*, pages 277–297. Springer-Verlag, September 2014.

[10] Y. Dodis, J. Katz, A. D. Smith, and S. Walfish. Composability and on-line deniability of authentication. In *Proc. of the 6th International Conference on Theory of Cryptography (TCC'09), San Francisco, California, USA*, volume 5444 of *Lecture Notes in Computer Science*, pages 146–162. Springer-Verlag, March 2009.

[11] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proc. of the 4th International Conference on Advances in Cryptology (CRYPTO'84), Santa Barbara, California, USA*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer-Verlag, August 1985.

[12] O. Goldreich. *Foundations of Cryptography - Volume 1, Basic Techniques*. Cambridge University Press, 2001.

[13] R. Goyal, V. Koppula, and B. Waters. Semi-adaptive security and bundling functionalities made generic and easy. In *Proc. of the 14th International Conference on Theory of Cryptography (TCC'16-B), Beijing, China*, volume 9986 of *Lecture Notes in Computer Science*, pages 361–388. Springer-Verlag, October 2016.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM Conference on Computer and Communications Security (CCS'06), Alexandria, Virginia, USA*, pages 89–98. ACM, October-November 2006.

[15] M. Naor. Deniable ring authentication. In *Proc. of the 22nd International Conference on Advances in Cryptology (CRYPTO'02), Santa Barbara, California, USA*, volume 2442 of *Lecture Notes in Computer Science*, pages 481–498. Springer, Berlin, Heidelberg, August 2002.

[16] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *Proc. of the 14th ACM Conference on Computer and Communications Security (CCS'07), Alexandria, Virginia, USA*, pages 195–203. ACM, October-November 2007.

[17] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Proc. of the 24th International Conference on Advances in Cryptology (EUROCRYPT'05), Aarhus, Denmark*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer-Verlag, May 2005.

[18] K. Takashima. Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In *Proc. of the 9th International Conference on Security and Cryptography for Networks (SCN'14), Amalfi, Italy*, volume 8642 of *Lecture Notes in Computer Science*, pages 298–317, September 2014.

[19] K. Takashima. Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 103-A(1):74–106, 2020.

[20] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *Proc. of the 29th Annual International Conference on Advances in Cryptology (CRYPTO'09), Santa Barbara, California, USA*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer-Verlag, August 2009.

[21] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC'11), Taormina, Italy*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70. Springer-Verlag, March 2011.

[22] K. Yamada, N. Attrapadung, K. Emura, G. Hanaoka, and K. Tanaka. Generic constructions for fully secure revocable attribute-based encryption. In *Proc. of the 22nd European Symposium on Research in Computer Security (ESORICS'17), Oslo, Norway*, volume 10492 of *Lecture Notes in Computer Science*, pages 532–551. Springer-Verlag, August 2017.

[23] K. Yamada, N. Attrapadung, K. Emura, G. Hanaoka, and K. Tanaka. Generic constructions for fully secure revocable attribute-based encryption. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 101-A(9):1456–1472, September 2018.

[24] S. Yamada, N. Attrapadung, B. Santoso, J. C. N. Schuldt, G. Hanaoka, and N. Kunihiro. Verifiable predicate encryption and applications to CCA security and anonymous predicate authentication. In *Proc. of the 15th International Conference on Practice and Theory in Public Key Cryptography (PKC'12), Darmstadt, Germany*, volume 7293 of *Lecture Notes in Computer Science*, pages 243–261. Springer-Verlag, May 2012.

Author Biography

Hiroaki Anada received the B.S. degree in science from Waseda University in 1996, M.S. degree in science from the same university in 1998, and Ph.D. degree from Institute of Information Security in 2012. Currently he is a professor in University of Nagasaki. His research interests include Cryptography, Statistics and Applied Mathematics. He is a member of IEEE, ACM, IACR, IEICE, IPSJ and JSIAM.

Yoshifumi Ueshige received the B.S. degree in science from Kyushu Institute of Technology in 1992, M.S. degree in science from the same university in 1994, and Ph.D. degree from the same university in 1997. Currently he is an associate professor in Nagasaki University. His research interests include authentication protocols, electronic voting and their deniability. He is a member of IPSJ.