Identity-based multi-condition proxy re-encryption

Pingshu Wang

School of Mathematics Qinghai University for Nationalities, Xining, 810007, China

email: wangpingshu@sina.com

Keywords: Identity based encryption; Identity-based Multi-condition Proxy Re-encryption; Bilinear maps

Abstract. In a proxy re-encryption system, a semi-trusted proxy can convert a ciphertext originally intended for Alice into one encrypting the same plaintext for Bob without seeing the underlying plaintext. However, a fine-grained delegation is demanded in some scenarios. For this, Weng *et al*. introduce the notion of conditional proxy re-encryption (CPRE), and formalize its security model and propose an efficient CPRE scheme. This paper presents the notion of identity-based multi-condition proxy re-encryption, which is a variant of identity-based condition proxy re-encryption. In such system, ciphertexts are generated under specified conditions by Alice, and the proxy can translate the ciphertext if the relevant conditions are satisfied. We formalize its security model and construct a concrete multi-condition proxy re-encryption scheme, and prove its security in the standard model.

Introduction

In 1998, Blaze, Bleumer and Strauss introduced concept of proxy re-encryption [1]. A semi-trusted proxy converts any ciphertext under Alice's public key into ciphertext under Bob's public key without being able to infer any information on the corresponding plaintext. A number of proxy re-encryption systems have been proposed in the context of public-key encryption [2, 3, 5, 6, 8, 9].

Green and Ateniese extended the notion of proxy re-encryption to the area of Identity Based, so called Identity-Based Proxy Re-Encryption (IBPRE). Senders encrypt messages using the recipient's identity (a string) as the public key and the proxy uses proxy keys, or re-encryption keys to transform ciphertext from one identity to another without being able to learn the plaintext and to deduce secret keys of Alice or Bob from the proxy keys in the IBPRE system. Then many of the IBPRE schemes have been proposed in identity-based setting [4, 7, 10, 14, 17].

In actual application, there exist scenarios which ciphertext under Alice's public key is not completely translated into ciphertext with Bob's private key to decrypt it, for example, Alice wants only to convert this type emails which subject contain urgent keyword. However, traditional PRE system enables the proxy to transform all of email which is encrypted by Alice without any discrimination. To meet the issue, notion of type-based proxy re-encryption (TBPRE) [11] and concept of conditional proxy re-encryption (CPRE) [12] were introduced by Tang and Weng, respectively. In CPRE systems, delegator can implement fine-grained delegation of decryption rights by additional condition.

In this paper, we introduce the notion of Identity-based multi-condition proxy re-encryption (IBMCPRE), in which delegator will augment number of condition to effectively control proxy powers to convert one ciphertext into another. And then we formalize the definition and security notions for IBMCPRE, and further propose a concrete IBMCPRE scheme, and prove its security in the standard model.

Related Work

Blaze, Bleumer and Strauss [1] formalized the concept of proxy re-encryption, and proposed the first bidirectional PRE scheme, in which the delegation from Alice to Bob also allows re-encryption

from Bob to Alice. In 2006, Ateniese *et al*. [2] presented unidirectional PRE schemes based on bilinear pairings. In ACM CCS'07, Canetti and Hohenberger[5] presented a CCA-secure bidirectional PRE scheme from bilinear pairings. Later, Libert and Vergnaud [3] proposed the first unidirectional proxy re-encryption schemes with chosen-ciphertext security in the standard model. In CANS'08, Deng *et al*. [6] constructed a CCA-secure bidirectional PRE scheme without pairings. In PKC'09, Shao and Cao [8] proposed a unidirectional PRE scheme without pairings; Weng *et al*. [9] presented an efficient CCA-secure unidirectional PRE scheme without pairings.

Green and Ateniese [4] extended the notion of proxy re-encryption to the area of Identity-Based Encryption (IBE), in which senders encrypt messages using the recipient's identity (a string) as the public key, and presented tow non-interactive, unidirectional proxy re-encryption schemes in the IBE setting. Similarly, Matsuo [7], Chu and Tzeng [10] also studied proxy re-encryption in identity-based setting, respectively.

Traceable proxy re-encryption, introduced by Libert and Vergnaud [13], attempts to solve the problem of disclosing re-encryption keys, by tracing the proxies who have done so. To more effectively control rights of proxy re-encryption, in [12], Weng and others introduced the notion of conditional proxy re-encryption (CPRE) with bilinear pairings and gave a new scheme for CPRE [16]. Later, Vivek and others [15] proposed a CPRE scheme to use substantially less number of bilinear pairings. In[14], Zhou and others introduced the notion of identity-based conditional proxy re-encryption (IBCPRE), and presented a concrete IBCPRE scheme.

Contributions and Paper Organization

We formalize identity-based multi-condition proxy re-encryption system model and construct a concrete multi-condition proxy re-encryption scheme in the standard model.

The rest of the paper is organized as follows. In Preliminaries section, we review some properties of bilinear pairing and complexity assumptions, we formalize the definition and security notions of identity-based multi-condition proxy re-encryption (IBMCPRE), and propose a concrete IBMCPRE scheme form pairings and give security proof of scheme, in Model of IBMCPRE Systems section and IBMCPRE Scheme section, respectively. Finally, we conclude the paper in Conclusion section.

Preliminaries

In this section, we review definition of bilinear pairing and a complex assumption on which our scheme is based.

Bilinear Groups and Bilinear Pairings

Let G and G_T be two cyclic multiplicative groups with the same prime order q. A bilinear pairing is a map $e: G \times G \to G_T$ with the following properties.

Bilinearity: We have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$, for $\forall g_1, g_2 \in G$ and $\forall a, b \in Z_q^*$;

Non-degeneracy: There exist $g_1, g_2 \in G$ such that $e(g_1, g_2) \neq 1$;

Computability: There exists an efficient algorithm to compute $e(g_1, g_2)$ for $\forall g_1, g_2 \in G$.

Complexity Assumptions

The Bilinear Diffie-Hellman (BDH) problem in (G, G_T) is as follows: given a tuple $g, g^a, g^b, g^c \in G$ as input, output $e(g,g)^{abc} \in G_T$. An algorithm has advantage ε in solving BDH in (G, G_T) if

$$\Pr\left[\mathcal{A}(g, g^a, g^b, g^c) = e(g,g)^{abc} \right] \geq \varepsilon ,$$

where the probability is over the random choice of generator g in G, the random choice of a, b, c in Z_q, and the random bits consumed by $\mathcal{A}$.

Similarly, we say that an algorithm that outputs $b \in \{0, 1\}$ has advantage ε in solving the decisional bilinear Diffie-Hellman (DBDH) problem in (G,G_T) if

$$\left|\Pr\left[\mathcal{A}(g,g^a,g^b,g^c,e(g,g)^{abc}=0\right]-\Pr\left[\mathcal{A}(g,g^a,g^b,g^c,Q)=0\right]\right|\geq\varepsilon,$$

where the probability is over the random choice of generator g in G, the random choice of a, b, c in Z_q, and the random choice of $Q\in G_T$.

Definition 1. We say that the (t, ε)-DBDH assumption holds in (G, G_T) if no t-time algorithm has advantage at least ε in solving the DBDH problem in (G, G_T).

Model of IBMCPRE System

We give the definitions and security notions for IBMCPRE systems in this section.

Definition of IBMCPRE systems

Formally, an IBMCPRE scheme consists of the following algorithms:

Setup (1^κ): The key generation algorithm takes as input a security parameter 1^κ. It generates the global parameters *param*. The parameters in *param* are implicitly given as input to the following algorithms.

KeyGen(*msk*, ID): On input an identity $ID\in\{0,1\}^n$ and the master secret key *msk*, it generates a decryption key sk_{ID} corresponding to that identity.

ReEnKeyGen($sk_{ID_1}, C(\omega_1,\omega_2), ID_1, ID_2$): The re-encryption key generation algorithm, run by user ID_1, takes as input a secret key sk_{ID_1}, compound condition $C(\omega_1,\omega_2)$ and identities ID_1, ID_2. It outputs a re-encryption key $sk_{ID_1}^{C(\omega1,\omega2)}{}_{ID_2}$, where ω_1, ω_2 are two independent conditions.

Enc (ID, *m*, $C(\omega_1,\omega_2)$): The encryption algorithm takes as input an identity ID, a plaintext $m\in\mathcal{M}$ and a compound condition $C(\omega_1,\omega_2)$. It outputs ciphertext CT associated with condition $C(\omega_1,\omega_2)$ under the specified identity. Here M denotes the message space.

ReEnc($CT_{ID_1}, sk_{ID_1}^{C(\omega1,\omega2)}{}_{ID_2}$): The re-encryption algorithm takes as input a ciphertext CT_{ID_1} associated with $C(\omega_1,\omega_2)$ under identity ID_1, and a re-encryption key $sk_{ID_1}^{C(\omega1,\omega2)}{}_{ID_2}$, this re-encryption algorithm, run by the proxy, outputs a re-encrypted ciphertext CT_{ID_2} under identity ID_2.

Dec(CT, sk_{ID}): The decryption algorithm takes as input a secret key sk_{ID} and a cipertext CT. It outputs a message $m\in\mathcal{M}$ or the error symbol $\perp$.

Security Notions of IBMCPRE systems

In this subsection, we will define the security notions for IBMCPRE systems following definition in [14]. The semantic security under adaptive-ID and chosen plaintext attacks for an IBMCPRE scheme is defined according to the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$:

Setup. Challenger $\mathcal{C}$ runs algorithm Setup (1^κ) and gives the global parameters *param* to $\mathcal{A}$.

Phase 1. The adversary A adaptively issues queries $q_1, \cdots, q_m$, where query q_i is one of the following:

Extract query: challenger $\mathcal{C}$ runs algorithm KeyGen(*msk*, ID) to obtain the sk_{ID}, and then gives it to $\mathcal{A}$.

ReEnKeyGen query: challenger $\mathcal{C}$ first runs algorithm KeyGen(*msk*, ID_1) to obtain the sk_{ID}, and then runs re-encryption key generation algorithm ReEnKeyGen $(sk_{ID_1}, C(\omega_1,\omega_2), ID_1, ID_2)$, and returns $sk_{ID_1}^{C(\omega1,\omega2)}{}_{ID_2}$ to $\mathcal{A}$.

Challenge. Once $\mathcal{A}$ decides Phase 1 is over, it outputs a target identity ID^* and two equal-length plaintexts m_0, $m_1 \in \mathcal{M}$. Challenger $\mathcal{C}$ tosses a random coin $\delta \in \{0, 1\}$ and runs the re-encryption algorithm to set the challenge ciphertext to be $CT^* = \text{Enc}(ID^*, m, C(\omega_1,\omega_2)^*)$, which is sent to $\mathcal{A}$.

Phase 2. Adversary $\mathcal{A}$ adaptively issues query as in Phase 1, and challenger $\mathcal{C}$ answers them as before.

Guess. Finally, adversary $\mathcal{A}$.outputs a guess $\delta' \in \{0,1\}$ and wins the game if $\delta' = \delta$. Adversary $\mathcal{A}$ is subject to the following restrictions during the above game.

(1) Adversary $\mathcal{A}$ can not issue the extraction query on ID^* to obtain the target secret key sk_{ID*}.

(2) Adversary $\mathcal{A}$ can not issue the ReEnKeyGen query on $C(\omega_1,\omega_2)^*, ID^*, ID'$, If ID' appears in a previous extraction query.

We refer to the above adversary $\mathcal{A}$ as an IND-IBMCPRE-CPA adversary. $\mathcal{A}$'s advantage in attacking our IBMCPRE scheme is defined as

$$\text{Adv}_{\mathcal{A}}^{\text{IND-IBMCPRE-CPA}} = \left|\Pr[\delta'=\delta]-\frac{1}{2}\right|,$$

where the probability is taken over the random coins consumed by the adversary and the challenger.

Definition 2 An IBMCPRE scheme Ψ is said to be (t, q_e, q_{rk}, ε)-IND-IBMCPRE-CPA secure, if for any t-time IND-IBMCPRE-CPA adversary $\mathcal{A}$ that makes at most q_e times KeyGen queries, at most q_{rk} times ReEnKeyGen queries, we have

$$\text{Adv}_{\Psi,\mathcal{A}}^{\text{IND-IBMCPRE-CPA}} \le \varepsilon .$$

IBMCPRE Scheme

Based on Waters's identity-based encryption scheme [17] and Zhou's identity-based conditional proxy re-encryption scheme [14], we propose an IBMCPRE scheme, and prove the security under the DBDH assumption.

The IBMCPRE scheme consists of the following algorithms:

Setup (1^κ): The setup algorithm takes as input a security parameter κ. It first generates (q, G, G_T,e), where q is a κ-bit prime, G and G_T are two cyclic multiplicative groups with prime order q, e is the bilinear pairing $e: G \times G \to G_T$, and g be a random generator of G. Next it picks $\alpha \in Z_q^*$ and computes $g_1 = g^\alpha$, $Z = e(g_1, g_2)$ (where $g_2 \in G$), and two hash functions H_1, H_2, H_3 such that $H_1 : \{0,1\}^n \to G$, $H_2 : \{0,1\}^n \times \{0,1\}^n \to G$, here n is determined by the security parameter. Finally, it outputs the master secret key $msk = g_2^\alpha$ and the global parameters $param$ = (g, g_1, g_2, Z, H_1, H_2).

KeyGen(*msk*, ID): On input an identity $ID \in \{0,1\}^n$, this algorithm randomly chooses $r \in Z_q^*$, and then defines the secret key for ID as

$$sk_{ID} = (d_1, d_2) = (msk \cdot H_1^{\,r}(ID), g^r).$$

ReEnKeyGen($sk_{ID_1}, C(\omega_1,\omega_2), ID_1, ID_2$): On input a secret key $sk_{ID} = (d_1, d_2)$, another identity ID_2 and a compound condition $C(\omega_1,\omega_2) \in \{0,1\}^n \times \{0,1\}^n$, this algorithm randomly chooses $r_1, r_2 \in Z_q^*$, and then outputs the re-encryption key from identity ID_1 to ID_2 associated with condition $C(\omega_1,\omega_2)$ as

$$sk_{ID_1 \xrightarrow{C(\omega_1,\omega_2)} ID_2} = (s_1, s_2, s_3, s_4, s_5) = (d_1 \cdot H_{2^n}(c(\omega_1,\omega_2)), d_2, g^n, g^{r_2}, H_{1^{r_2}}(ID_2)).$$

Enc (ID, *m*, $C(\omega_1,\omega_2)$): This algorithm takes as input an identity $ID \in \{0,1\}^n$, a plaintext $m \in G_T$, a compound condition $C(\omega_1,\omega_2) \in \{0,1\}^n \times \{0,1\}^n$, and the sender picks $s \in Z_q^*$. It outputs ciphertext $CT_{ID} = (c_1, c_2, c_3, c_4)$ as $c_1 = H_1^s(ID)$, $c_2 = H_2^s(c(\omega_1,\omega_2))$, $c_3 = g^s$, $c_4 = m \cdot H^s{}_2(c(\omega_1,\omega_2) \cdot Z^s$.

ReEnc($CT_{ID_1}, sk_{ID_1}^{C(\omega 1,\omega 2)}{}_{ID_2}$ **):** The re-encryption algorithm takes as input a ciphertext $CT_{ID} = (c_1, c_2, c_3, c_4)$, and a re-encryption key

$sk_{ID_1}^{C(\omega 1,\omega 2),}{}_{ID_2} = (s_1, s_2, s_3, s_4, s_5)$.

This algorithm outputs a re-encrypted ciphertext CT_{ID_2} under identity ID_2. It first computes:

$c_1' = e(s_1, c_3), c_2' = e(s_2, H_1^s(ID_1)) \cdot e(s_2, H_2^s(c(\omega_1, \omega_2)))$, $c_3' = c_2' / c_1'$, $c_4' = c_4$, $c_5' = s_5$ then

$CT_{ID_2} = (c_1', c_2', c_3', c_4', c_5')$.

Dec (CT, sk_{ID}): This decryption algorithm takes as input a secret key sk_{ID} and a cipertext CT_{ID}.

If $sk_{ID} = (d_1, d_2)$ and $CT_{ID} = (c_1, c_2, c_3, c_4)$, it outputs a message

$m = \dfrac{c_4 \cdot e(c_1, d_2)}{c_2 \cdot e(c_3, d_1)}$, or if $sk_{ID_1}^{C(\omega 1,\omega 2),}{}_{ID_2} = (s_1, s_2, s_3, s_4, s_5)$ and

$CT_{ID_2} = (c_1', c_2', c_3', c_4', c_5')$, it outputs a message

$m = \dfrac{c_4' \cdot e(s_2, c_2)}{c_2 \cdot e(s_3, c_2)}$.

Analysis

Our proposed scheme only achieves the chosen-plaintext security, and there some are properties in this scheme also, proxy can check whether validity of re-encryption key from delegator to send it in phase of re-encryption key generation by verifying following equations hold or not. If all equations hold following, then proxy re-encryption keys are valid.

$e(s_1, g) = Z \cdot e(s_4, H_1(ID_2)) \cdot e(s_2, H_1(ID_1)) \cdot e(s_3, H_2(c(\omega_1, \omega_2)))$, $e(s_5, g) = e(s_4, H_1(ID_2))$.

In the next section, we can use re-encryption technique in [14] to provide chosen-plaintext security.

Security Proof

The proposed IBMCPRE scheme is IND-CPRE-CPA secure in standard model. The scheme is a variant identity-based condition proxy re-encryption system, which is added combinational conditions to reduce capacity of decryption for proxy. Our proof idea essentially follows that of [14], we omit the details of following proof of theorem here due to the page limit.

Theorem 1. Our IBMCPRE scheme is IND-IBMCPRE-CPA secure in the standard model, assuming the DBDH assumption holds in groups (G, G_T).

Conclusion

In this paper we add to conditions in processing re-encryption ciphertexts so that delegator enables to control the proxy's rights in PRE systems in the IBE setting. Our work comparing with existed schemes are properly adding multiple conditions, and we introduce the concept of identity-based multi-condition proxy re-encryption, formalize its definition and its security notions, and propose a secure IBMCPRE scheme in the standard model.

Acknowledgement

In this paper, the research was sponsored by the Natural Science Foundation of Qinghai Province (Project No.2011-Z-906) and the Chunhui Project of Ministry of Education of China (Project No. Z2012113).

References

[1]Matt Blaze, Gerrit Bleumer and Martin Strauss. Divertible protocols and atomic proxy cryptography [C]. Proc. of Eurocrypt'98, Springer-Verlag, LNCS 1403, Espoo, Finland, 1998. 127–144.

[2]Giuseppe Ateniese, Kevin Fu, Matthew Green and Susan Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage [J]. ACM Transactions on Information and System Security (TISSEC), 2006(9)1-30.

[3]Benoit Libert, Damien Vergnaud. Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption [C]. In Proc. of PKC'08, LNCS 4929, Springer-Verlag, 2008. 360-379.

[4]Matthew Green, Giuseppe Ateniese. Identity-based proxy re-encryption [C]. In ACNS 2007, volume 4521 of LNCS, 2007. 288–306.

[5]Ran Canetti, Susan Hohenberger. Chosen-Ciphertext Secure Proxy Re-Encryption [C]. In Proceeding of ACM CCS 2007. 185-194.

[6]Robert H. Deng, Jian Weng, Shengli Liu, Kefei Chen. Chosen-cipertext secure proxy re-encryption without pairings [C]. In Proc. of CANS'08, Springer-Verlag, LNCS 5339, Hong Kong, China, 2008.1–17.

[7]Toshihiko Matsuo. Proxy re-encryption systems for identity-based encryption[C]. Proc.of Paring'07, LNCS 4575.247–267.

[8]Jun Shao, Zhenfu Cao. CCA-Secure Proxy Re-encryption without Pairings [C]. In: Public Key Cryptography. LNCS 5443. 357–376.

[9]Sherman S. M. Chow, Jian Weng, Yanjiang Yang, Robert H. Deng. Efficient unidirectional proxy re-encryption [C]. In Proc. of Cryptology–AFRICACRYPT 2010. 316-332.

[10] Cheng-Kang Chu, Wen-Guey Tzeng. Identity-based proxy re-encryption without random oracles[C]. In Proc. of ISC'07. LNCS 4779.189–202.

[11] Qiang Tang. Type-based proxy re-encryption and its construction [C]. In: Proc. of INDOCRYPT 2008. LNCS 5365. 130-144.

[12] Jian Weng, Robert H. Deng, Xuhua Ding, Cheng-Kang Chu, and Junzuo Lai. Conditional proxy re-encryption secure against chosen-ciphertext attack[C]. In ACM ASIACCS 2009, 322-332.

[13]Benoît Libert, Damien Vergnaud. Tracing malicious proxies in proxy re-encryption [C]. In Galbraith S D, Paterson K G, eds. Pairing. LNCS 5209. Berlin: Springer-Verlag, 2008.332-353.

[14] Dehua Zhou, Kefei Chen, Shengli Liu and Dong Zheng. Identity-Based Conditional Proxy Re-Encryption[J]. Chinese Journal of Electronics 2013(1): 61-66.

[15] S.Sree Vivek, S.Sharmila Deva Seli, V. Radhakishan, C. Pandu Rangan. Efficient conditional proxy re-encryption with chosen ciphertext security [J]. International Journal of Network Security & Its Applications (IJNSA), 2012(14):179-199.

[16] Jian Weng, Yanjiang Yang, Qiang Tang, Robert H. Deng, Feng Bao. Efficient conditional proxy re-encryption with chosen-ciphertext security [C]. In Proc. of ISC'09, Springer-Verlag, LNCS 5735.151–166.

[17] Brent Waters. Efficient Identity-based Encryption Without Rrandom Oracles [C]. Proc. of Eurocrypt'05, Springer-Verlag, LNCS 3494.114–127.