Identity Based Broadcast Encryption Based on One to Many Identity Based Proxy Re-encryption

Xu an Wang, Xiaoyuan Yang
Key Laboratory of Information and Network Security
Engneering College of Chinese Armed Police Force, 710086, P. R. China
E-mail:wangxahq@yahoo.com.cn

***Abstract*— Broadcast encryption schemes enable senders to efficiently broadcast ciphertexts to a large set of receivers in a way that only non-revoked receivers can decrypt them. Identity based broadcast encryption schemes are public key broadcast encryption using identity as the public key. In this paper, we show a novel way to construct identity based broadcast encryption. We introduce a new concept: one to many identity based proxy re-encryption. And we show how to construct efficient identity based broadcast encryption based on this primitive. Our scheme can achieve constant size public keys and private keys and linear size ciphertext. But our scheme no longer needs explicitly describing receiver set while all the other schemes need. Thus our scheme is an efficient broadcast encryption scheme compared with other schemes.**

I. Introduction

A. Broadcast encryption

The concept of broadcast encryption is introduced by Fiat and Naor in [7], which allows a broadcaster encrypts messages and transmits them to a group of users who are listening to a broadcast channel and use their private keys to decrypt transmissions. At encryption time, the broadcaster can choose the set S of identities that will be able to decrypt messages. A broadcast encryption is said to be fully collusion resistant when, even if all users are not in S collude, they can by no means infer information about the broadcast message.

Many BE systems have been proposed. The best known fully collusion systems are the schemes of Boneh, Gentry and Waters [4] which achieve $O(n)$-size public key, constant size ciphertext and constant size private keys. We denote it by BGW in the following.

B. Proxy re-encryption

The concept of proxy re-encryption is introduced by Blaze, Bleumer and Strauss in [2], which allows a proxy can transfer a ciphertext computed under Alice's public key into one that can be opened under Bob's decryption key. In ACNS'07, Green et al. proposed the first identity based proxy re-encryption scheme. Later in pairing'07, Matsuo proposed another few more proxy re-encryption schemes in identity based setting [15]. But unfortunately, in their identity based proxy re-encryption scheme, the proxy actually can transfer any other IBE users's ciphertext to be the delegatee's ciphertext.

978-1-4244-4520-2/09/$25.00 ©2009 IEEE

C. Our Contribution

In this paper, we introduce a new concept: one to many identity based proxy re-encryption scheme. And we show how to construct efficient identity based broadcast encryption based on this primitive. Our scheme can achieve constant size public keys and private keys and linear size ciphertext. But our scheme no longer needs explicitly describing receiver set while all the other schemes need. Thus our scheme is an efficient broadcast encryption scheme compared with other schemes.

D. Roadmap

We organize our paper as following. In section 2, we propose the concept of one to many proxy re-encryption and construct a concrete one to many proxy re-encryption scheme. In section 3, we show how to transfer this one to many proxy re-encryption scheme into a broadcast encryption scheme. In section 4, we give some comparison between our scheme and BGW scheme. We give our conclusion in section 5.

II. Identity Based One to Many Proxy Re-encryption Scheme

A. Concept of Identity Based One to Many Proxy Re-encryption Scheme

Definition 1: An identity based one to many proxy re-encryption scheme is tuple of algorithms (Setup, KeyGen, Encrypt, Decrypt, RKGen, Reencrypt):

- Setup(1^k). On input a security parameter, the algorithm outputs both the master public parameters which are distributed to users, and the master secret key (msk) which is kept private.
- KeyGen(params, msk, id). On input an identity $id \in \{0,1\}^*$ and the master secret key, outputs a decryption key sk_{id} corresponding to that identity.
- Encrypt(params, id, m). On input a set of public parameters, an identity $id \in \{0,1\}^*$ and a plaintext $m \in M$, output c_{id}, the encryption of m under the specified identity.
- RKGen(params, msk, sk_{id_1}, sk_{id}, id_1, id). On input secret keys msk, sk_{id_1}, PKG, the delegator generate the re-encryption key rk_{id_1}, the algorithm output it.
- Reencrypt(params, rk_{id_1}, c_{id_1}). On input a ciphertext c_{id_1} under identity id_1, and a re-encryption key rk_{id_1}, outputs a re-encrypted ciphertext c_{id} for any other id except id_1.

- Decrypt(params, sk_{id}, c_{id}). Any IBE user id can decrypt the ciphertext c_{id} using the secret key sk_{id}, and output m or $\perp$.

Definition 2: Intuitively, a one to many IB-PRE is correct if the Decrypt algorithm always outputs the expected decryption of a properly generated ciphertext. Slightly more formally, let $c_{id_1} \leftarrow Encrypt(params, id_1, m)$ be a properly generated ciphertext, Then $\forall m \in \mathcal{M}, \forall id_1 \in \{0,1\}^*$, where $sk_{id_1} = KeyGen(msk, id_1)$, $rk_{id_1} \leftarrow RKGen(params, sk_{id_1}, msk, id_1)$, the following propositions hold: Decrypt(params, sk_{id_1}, c_{id_1})= m; Decrypt(params, sk_{id}, Reencrypt(params, rk_{id_1}, c_{id_1}))=m

B. Our Proposed Scheme

- The underlying IBE scheme:
  1) $\mathbf{SetUp_{IBE}(k)}$.Given a security parameter k, select a random generator $g \in G$, choose randomly $t_1, t_2 \in Z_p^*$ and computes elements $g_2 = g^{t_1}, h = g^{t_2} \in G$. Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^\alpha$,$mk = (g_2^\alpha, t_1, t_2)$, and $parms = (g, g_1, g_2, h)$. Let mk be the master- secret key and let $parms$ be the public parameters.
  2) $\mathbf{KeyGen_{IBE}(mk, parms, ID)}$. Given $mk = g_2^\alpha$ and ID with $parms$, pick a random $u, x \in Z_p^*$. Set $sk_{ID} = (d_0, d_1, d_2) = (g_2^\alpha (g_1^{ID} h)^u, g^u, g^{\frac{u}{\alpha}})$.
  3) $\mathbf{Enc_{IBE}(ID, parms, M)}$. To encrypt a message $M \in G_1$ under the public key $ID \in Z_p^*$, pick a random $r \in Z_p^*$ and compute $C_{ID} = (g^r, (g_1^{ID} h)^r, Me(g_1, g_2)^r)$.
  4) $\mathbf{Dec1_{IBE}(sk_{ID}, parms, C_{ID})}$. Given a normal ciphertext $C_{ID} = (C_1, C_2, C_3)$ and the secret key $sk_{ID} = (d_0, d_1, d_2)$ with $prams$, compute $M = \frac{C_3 e(d_1, C_2)}{e(d_0, C_1)}$.
  5) $\mathbf{Dec2_{IBE}(sk_{ID'}, parms, ID, C_{ID'})}$. Given a re-encrypted ciphertext $C_{ID'} = (C_1, C_2, C_3, C_4, C_5)$ and the secret key $sk_{ID} = (d_0, d_1, d_2)$ with $prams$, compute $M = \frac{C_4 e(d_1, C_3^{(ID'-ID)} C_2)}{e(d_0, C_1) e(d_2, C_5^{(ID'-ID)})}$.
- The delegation scheme:
  1) $\mathbf{KeyGen_{PRO}(mk, parms, ID)}$. The KGC randomly choose $x \in Z_p^*$ sets $rk_{ID} = (rk_1, rk_2) = (\frac{\alpha+x}{\alpha ID+t_2}, \frac{x\alpha}{\alpha ID+t_2})$ and sends it to the proxy via secure channel. We must note that the KGC computes a different x for every different ID.
  2) $\mathbf{ReEnc(rk_{ID}, parms, C_{ID}, ID')}$. Given the delegator's identity ID, the delegatee's identity ID', $rk_{ID} = (rk_1, rk_2) = (\frac{\alpha+x}{\alpha ID+t_2}, \frac{x\alpha}{\alpha ID+t_2})$,$C_{ID} = (C_1, C_2, C_3)$ with $parms$, re-encrypt the ciphertext C_{ID} into $C_{ID'}$ as follows. First it runs "Check", if output 0, then return "Reject". Else computes $C_{ID'} = (C_1', C_2', C_3', C_4', C_5') = (C_1, C_2, C_2^{rk_1}, C_3, C_2^{rk_2})$.
  3) $\mathbf{Check(parms, C_{ID}, ID)}$. Given the delegator's identity ID and $C_{ID} = (C_1, C_2, C_3)$ with $parms$, compute $v_0 = e(C_1, g_1^{ID} h)$ and $v_1 = (C_2, g)$. If $v_0 = v_1$ then output 1. Otherwise output 0.

We can verify its correctness as the following

$$\begin{aligned}
&\frac{C_4 e(d_1, C_3^{(ID'-ID)} C_2)}{e(d_0, C_1) e(d_2, C_5^{(ID'-ID)})} = \\
&\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID} h)^{r \cdot \frac{\alpha+x}{\alpha ID+t_2} \cdot (ID'-ID)} (g_1^{ID} h)^r)}{e(g_2^\alpha (g_1^{ID'} h)^u, g^r) e(g^{u/\alpha}, (g_1^{ID} h)^{r \cdot \frac{x\alpha}{\alpha ID+t_2} \cdot (ID'-ID)})} = \\
&\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID'} h)^r) e(g^u, g^{xr(ID'-ID)})}{e(g_2^\alpha (g_1^{ID'} h)^u, g^r) e(g^{u/\alpha}, g^{x\alpha r(ID'-ID)})} = \\
&\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID'} h)^r))}{e(g_2^\alpha (g_1^{ID'} h)^u, g^r)} = \\
&M =
\end{aligned}$$

Remark 1: In the scheme, we can see that the proxy can re-encrypt ciphertext for ID into ciphertext for ID'(any IBE user except ID).

III. How to Transfer the Above Scheme to a Broadcast Encryption Scheme

In the basic IBE scheme, assume the users are $(ID, ID_1, ID_2, ID_3, \cdots ID_n)$. Assume the valid receiver set is S. Now we require the proxy can transfer ID's ciphertext to be ciphertext of any user in S while cannot transfer ID's ciphertext to be be ciphertext of any user not in S. We can design our scheme as following:

1) $\mathbf{SetUp_{IBE}(k)}$.Given a security parameter k, select a random generator $g \in G$, choose randomly $t_1, t_2 \in Z_p^*$ and computes elements $g_2 = g^{t_1}, h = g^{t_2} \in G$. Choose a hash function $H : G \rightarrow Z_p^*$, Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^\alpha$,$mk = (g_2^\alpha, t_1, t_2)$, and $parms = (g, g_1, g_2, h, H)$. Let mk be the master-secret key and let $parms$ be the public parameters.
2) $\mathbf{KeyGen_{IBE}(mk, parms, ID)}$. Given $mk = g_2^\alpha$ and ID with $params$, pick a random $u \in Z_p^*$. Set $sk_{ID} = (d_0, d_1, d_1', d_2) = (g_2^\alpha (g_1^{ID} h)^u, g^{\frac{u}{\alpha+ID}}, g^{\frac{u}{a(\alpha+ID)}}, g^{\frac{u}{\alpha}})$. The KGC preserves a User-Key-list of the form (ID, u).
3) $\mathbf{KeyGen_{PRO}(mk, parms, ID)}$. The KGC randomly choose $x, t \in Z_p^*$searches in the User-Key-list and computes $rk = (rk_1, rk_2, rk_3, rk_4, rk_5, rk_6) = (\frac{t}{\alpha ID+t_2}, x + \alpha + t\prod_{i \in S} ID_i, \frac{a\alpha t}{\alpha ID+t_2}, a\alpha(x + \alpha + t\prod_{i \in S} ID_i), x\alpha + t\prod_{i \in S} ID_i, \alpha^2 ID + t_2\alpha)$. He sends rk to the proxy as the re-encryption key. We must note that the KGC computes a different (x, t) for every different ID.
4) $\mathbf{Enc_{IBE}(ID, parms, M)}$. To encrypt a message $M \in G_1$ under the public key $ID \in Z_p^*$, pick a random $r \in Z_p^*$ and compute $C_{ID} = (g^r, (g_1^{ID} h)^r, Me(g_1, g_2)^r)$.
5) $\mathbf{Check(parms, C_{ID}, ID)}$. Given the delegator's identity ID and $C_{ID} = (C_1, C_2, C_3)$ with $parms$, compute $v_0 = e(C_1, g_1^{ID} h)$ and $v_1 = e(C_2, g)$. If $v_0 = v_1$ then output 1. Otherwise output 0.
6) $\mathbf{ReEnc(rk_{ID}, parms, C_{ID}, ID')}$. Given the delegator's identity ID, the receiver set S, rk =

	BGW **Scheme [4]**	**Our Scheme**
private key length	$O(1)$	$O(1)$
ciphertext length(excluding S)	$O(1)$	$O(1)$
public key length	$O(n)$	$O(1)$

Fig. 1. Comparision with BGW Scheme

$(rk_1, rk_2, rk_3, rk_4, rk_5, rk_6) = (\frac{t}{\alpha ID+t_2}, x+\alpha+t\prod_{i\in S} ID_i, \frac{a\alpha t}{\alpha ID+t_2}, a\alpha(x+\alpha+t\prod_{i\in S} ID_i), x\alpha + t\prod_{i\in S} ID_i, \alpha^2 ID + t_2\alpha)$. $C_{ID} = (C_1, C_2, C_3)$ with $params$, re-encrypt the ciphertext C_{ID} into ciphertext of any user in S as follows. First it runs "Check", if output 0, then return "Reject". Else computes $C = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6, C'_7, C'_8, C'_9) = (C_1, C_1^{rk_2}, C_1^{rk_4}, C_1^{rk_5}, C_2, C_2^{rk_1}, C_2^{rk_3}, C_3, C_1^{rk_6})$.

7) $\mathbf{Dec_{IBE}}(\mathbf{sk_{ID_i}}, \mathbf{parms}, \mathbf{ID}, \mathbf{C_{ID}})$. Given a re-encrypted ciphertext $C = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6)$ and the secret key $sk_{ID_i} = (d_0, d_1, d_2)$ with $params$, let $f(y) = \prod_{i\in S}(y - ID_i) - \prod_{i\in S} ID_i$, the algorithm decrypt as following:

$$M = \frac{C'_8 e(d_1, C'_9 {C'_5}^{ID_i}) e(d'_1, ({C'_7}^{f(ID_i)} c'_3)^{(ID_i - ID)})}{e(d_0, C'_1)} \cdot \frac{e(d_1, ({C'_6}^{f(ID_i)} C'_2)^{ID_i(ID_i-ID)})}{e(d_2, ({C'_6}^{f(ID_i)} C'_4)^{(ID_i-ID)})}$$

We can verify its correctness as the following:

- If $ID_i \in S$, then

$$\frac{e(d_1, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots} C_3)^{(ID_i-ID)})}{e(d_2, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots})^{(ID_i-ID)})} \cdot \frac{C_4 e(d_1, C_2)}{e(d_0, C_1) e(d_2, C_5^{(ID_i-ID)})} =$$
$$\frac{e(d_1, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots+a_0})^{(ID_i-ID)})}{e(d_2, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots+a'_0})^{(ID_i-ID)})} \cdot \frac{C_4 e(d_1, C_2)}{e(d_0, C_1)} =$$
$$\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID} h)^{r\cdot\frac{\alpha+x}{\alpha ID+t_2}\cdot(ID_i-ID)} (g_1^{ID} h)^r)}{e(g_2^\alpha (g_1^{ID_i} h)^u, g^r) e(g^{u/\alpha}, (g_1^{ID} h)^{r\cdot\frac{x\alpha}{\alpha ID+t_2}\cdot(ID_i-ID)})} =$$
$$\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID_i} h)^r) e(g^u, g^{xr(ID_i-ID)})}{e(g_2^\alpha (g_1^{ID_i} h)^u, g^r) e(g^{u/\alpha}, g^{x\alpha r(ID_i-ID)})} =$$
$$\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID_i} h)^r))}{e(g_2^\alpha (g_1^{ID_i} h)^u, g^r)} = M$$

- If $ID_i \notin S$, then

$$\frac{e(d_1, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots} C_3)^{(ID_i-ID)})}{e(d_2, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots})^{(ID_i-ID)})} \cdot \frac{C_4 e(d_1, C_2)}{e(d_0, C_1) e(d_2, C_5^{(ID_i-ID)})} =$$
$$\frac{e(d_1, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots+a_0})^{(ID_i-ID)})}{e(d_2, (C_2^{H(d_1)^n + a_{n-2}H(d_1)^{n-2}+\cdots+a'_0})^{(ID_i-ID)})} \cdot \frac{C_4 e(d_1, C_2)}{e(d_0, C_1)} =$$
$$\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID} h)^{r\cdot\frac{\alpha+x}{\alpha ID+t_2}\cdot(ID_i-ID)} (g_1^{ID} h)^r)}{e(g_2^\alpha (g_1^{ID_i} h)^u, g^r) e(g^{u/\alpha}, (g_1^{ID} h)^{r\cdot\frac{x\alpha}{\alpha ID+t_2}\cdot(ID_i-ID)})} \neq$$
$$\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID_i} h)^r) e(g^u, g^{xr(ID_i-ID)})}{e(g_2^\alpha (g_1^{ID_i} h)^u, g^r) e(g^{u/\alpha}, g^{x\alpha r(ID_i-ID)})} \neq$$
$$\frac{Me(g_1, g_2)^r e(g^u, (g_1^{ID_i} h)^r))}{e(g_2^\alpha (g_1^{ID_i} h)^u, g^r)} \neq M$$

Remark 2: In the scheme, we can see that the proxy can re-encrypt ciphertext which for ID into valid ciphertext for authorized ID', but can not re-encrypt ciphertext which for ID into valid ciphertext for non authorized ID'.

IV. Comparison

Now we analyze the performance of our scheme. Many efficiency benchmarks for broadcast encryption schemes exist. They are, length of ciphertext, length of private key, length of public key, computational cost for encryption and decryption etc. Those values vary according to the size of receiver set, the number of potential users, and how much its receiver set has changed. We compare these efficiency with the BGW scheme [4]. We can see the results in Fig. 1.

As we can see in this figure, our scheme has most of nice features of Bonehs scheme. Our scheme is the most advantageous over the previous scheme, such as BGW scheme in [4], when the number of potential receivers is huge but the maximum size of its receiver set is rather small and receivers set does not change drastically on an average day.

V. Conclusion

In this paper, we show a novel way to construct identity based broadcast encryption. We introduce a new concept: one to many identity based proxy re-encryption. And we show how to construct efficient identity based broadcast encryption based on this primitive. Our scheme can achieve constant size public keys and private keys and linear size ciphertext. But our

scheme no longer needs explicitly describing receiver set while all the other schemes need. Thus our scheme is an efficient broadcast encryption scheme compared with other schemes.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under contract no. 60842006.

REFERENCES

[1] G.Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage.In *ACM Trans. Inf. Syst. Secur. 9 (2006), no. 1, pages 1–30.*

[2] M. Blaze, G. Bleumer, and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography.In *Advances in Cryptology - Eurocrypt'98,* LNCS 1403, pp. 127–144.Springer–Verlag,1998.

[3] D. Boneh, E. Goh and T. Matsuo. Proposal for P1363.3 Proxy Re-encryption. http://grouper.ieee.org/groups/1363/IBC/submissions/NTTDataProposal-for-P1363.3-2006-09-01.pdf.

[4] Dan Boneh, Craig Gentry, BrentWaters. Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. In *CRYPTO 2005.* pp. 258-275. Springer–Verlag, 2005.

[5] R. Canetti and S. Hohenberger, Chosen Ciphertext Secure Proxy Re-encryption.In *In Proceedings of the 14th ACM conference on Computer and Communications Security(CCS 2007),*pp. 185–194.2007. Also available at Cryptology ePrint Archive: http://eprint.iacr.org/2007/171.pdf.

[6] C.Chu and W.Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007,*LNCS 4779, pp. 189–202.Springer–Verlag,2007.

[7] Amos Fiat, Moni Naor. Broadcast Encryption. In *CRYPTO 1993*, 480-491. Springer–Verlag, 1993.

[8] E. Goh and T. Matsuo.Proposal for P1363.3 Proxy Re-encryption. http://grouper.ieee.org/groups/1363/IBC/submissions/NTTDataProposal-for-P1363.3-2006-08-14.pdf.

[9] M. Green and G. Ateniese, Identity-Based Proxy Re-encryption. In *Applied Cryptography and Network Security'07,*LNCS 4521, pp. 288–306.Springer–Verlag,2007.

[10] S. Hohenberger. Advances in Signatures, Encryption, and E-Cash from Bilinear Groups. Ph.D. Thesis, MIT, May 2006.

[11] S. Hohenberger, G. N. Rothblum, a. shelat, V. Vaikuntanathan. Securely Obfuscating Re-encryption.In *TCC'07,*LNCS 4392, pp. 233–252.Springer–Verlag,2007.

[12] B. Libert and D. Vergnaud, Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption.In *11th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2008,*LNCS 4939, pp. 360–379.Springer–Verlag,2008.

[13] B. Libert and D. Vergnaud, Tracing Malicious Proxies in Proxy Re-Encryption.In *Secon bnbbd International Conference on Pairing-Based Cryptography - Pairing 2008*,Springer–Verlag,2008.

[14] L.Martin(editor). P1363.3(TM)/D1, Draft Standard for Identity-based Public Cryptography Using Pairings, May 2008.

[15] T. Matsuo, Proxy Re-encryption Systems for Identity-Based Encryption.In *First International Conference on Pairing-Based Cryptography - Pairing 2007,*LNCS 4575, pp. 247–267.Springer–Verlag,2007.

[16] J.Shao,D.Xing and Z.Cao, Identity-Based Proxy Rencryption Schemes with Multiuse, Unidirection, and CCA Security.Cryptology ePrint Archive: http://eprint.iacr.org/2008/103.pdf,2008.

[17] Q. Tang, P. Hartel, W. Jonker. Inter-domain Identity-based Proxy Re-encryption. To appear in Inscrypt'08, also available at http://eprints.eemcs.utwente.nl/12259/01/.