Ciphertext-Policy Attribute-Based Broadcast Encryption Scheme

Muhammad Asim, Luan Ibraimi, Milan Petković

Ciphertext-Policy Attribute-Based Broadcast Encryption Scheme

Muhammad Asim[1],Luan Ibraimi[2], Milan Petković[1,3]

[1] Philips Research Eindhoven, The Netherlands
[2] Faculty of EWI, University of Twente, The Netherlands
[3] Faculty of Mathematics and Computer Science,
Eindhoven University of Technology, The Netherlands
{muhammad.asim,milan.petkovic}@philips.com,ibraimi@utwente.nl

Abstract In this work, we design a new attribute-based encryption scheme with the revocation capability. In the proposed schemes, the user (broadcaster) encrypts the data according to an access policy over the set of attributes, and a list of the identities of revoked users. Only recipients who have attributes which satisfy the access policy and whose identity is not in the list of revoked users will be able to decrypt the message.The proposed scheme can be used for revocation of up to t users. The complexity of proposed schemes is dependent on the number of revoked users r, rather than on the total number n of users in the system. The security of the scheme has been proved under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Keywords: Attribute-Based Encryption, Revocation

1 Introduction

In a broadcast encryption scheme with revocation capability, the sender (broadcaster) sends a ciphertext to a group of recipients such that only non-revoked users inside the group can decrypt the broadcasted content. Such a scheme allows the broadcaster to specify the list of revoked users who are not allowed to decrypt the digital content that is either broadcasted or placed in the organization's or public databases.

Efficient revocation of users in broadcast encryption schemes have achieved significant attention over the years as the revocation of the user is necessary and inevitable in numerous use cases. For example, in the domain of healthcare, privacy regulations such as healthcare insurance portability and accountability act (HIPAA)[1] give rights to patients to specify their consent policy. More specifically, individuals can request restrictions on the use and disclosure of health information. As a consequence, a doctor, who may be able to view the patient's data according to these regulations, may not be able to view the data. The revocation of a user also becomes important when an employee leaves the organization. Ideally the system should be able to revoke a user without (or minimally) affecting the non-revoked users.

*Our Contributions.*In this paper we propose a new ciphertext-policy attribute-based broadcast encryption scheme. In our proposed scheme the encryptor encrypts the data according to the access policy τ and the list of the identities of revoked users. Only the users with the attribute set that satisfy the access policy τ and their identities are not in the list of revoked users would be able to decrypt the ciphertext. The proposed scheme is inspired by the Naor and Pinkas [2] scheme, which in turn uses a secret sharing technique to revoke users. We use this idea in the context of CP-ABE where only non-revoked users who satisfy the access policy will be capable to reconstruct the secret in the exponent and be able decrypt the ciphertext.

2 The Construction

1. **Setup**($\mathbf{k}$). The setup algorithm selects a bilinear group $\mathbb{G}_0$ of prime order p and generator g. It also chooses a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ and hash function $H_1 : G_1 \rightarrow \{0,1\}^l$. Next to this, the setup picks $\alpha, \beta, x_1, x_2, \cdots, x_k \in \mathbb{Z}_p$. For a set of attributes $\Omega = \{a_1, a_2, ..., a_k\}$, it sets $T_j = g^{x_j}$ $(1 \leq j \leq k)$. For the purpose of revocation, picks $R \in \mathbb{Z}_p$ and generates a random polynomial $P(z) = \tilde{a}_0 + \tilde{a}_1 z + \tilde{a}_1 z^2 + ... + \tilde{a}_t z^t$ of degree t over $\mathbb{Z}_p$ such that $P(0) = R$. Next, the setup algorithm generates N identifiers $\{I_{u_1}, I_{u_2}, \cdots, I_{u_N}\}$ and a share $P(i)$ where $1 \leq i \leq N$. In this paper, $P(i)$ will be alternatively denoted by $P(I_{u_i})$. The setup algorithm also computes t extra dummy shares which will be used when the number of revoked users is less than t. The public key-**PK** and master secret key-**MK** consist of the following components:

$$\mathbf{PK} = \left(\hat{e}(g,g)^{\alpha}, \hat{e}(g,g)^{\beta}, \{T_j\}_{j=1}^{k}, \{g^{P(I_{ui})}\}_{i=1}^{N}, \{g^{P(I_{dq})}\}_{q=1}^{t}\right)$$
$$\mathbf{MK} = \left(\alpha, \beta, R = P(0), \{x_j\}_{j=1}^{k}\right)$$

2. **KeyGeneration**($\mathbf{MK}, \omega, I_{ui}$). The key generation algorithm takes as input the attribute set ω the user has, and the identifier I_{u_i} assigned to the user. The key generation algorithm first picks at random x,$y \in \mathbb{Z}_p$, and then computes the private key $SK_{I_{ui},\omega}$ that consists of the following components:

$$\mathbf{SK}_{I_{ui},\omega} = \begin{pmatrix} D^{(1)} = g^{\alpha - x - yP(0)}, & \{D_j^{(2)} = g^{\frac{x-\beta}{x_j}}\}_{a_j \in \omega}, \\ D^{(3)} = g^{yP(I_{ui})}, & D^{(4)} = g^{y} \end{pmatrix}$$

3. **Encryption**($m, \tau, \Re, \mathbf{PK}$). To encrypt a message $m \in \{0,1\}^l$, under the access policy τ over a set of attributes, and the set of revoked users $\Re = \{I_{u_1}, I_{u_2}, \cdots, I_{u_t}\}$ the encryption algorithm picks at random $s \in \mathbb{Z}_p$, and assigns $s_{\hat{i}}$ values (which are shares of s) to attributes in τ. For example the attributes are transformed into an access tree where the inner nodes represent an **AND** or **OR** boolean operators, and the leaf nodes are attributes. It assigns the value s to the root node. For **AND** node, it assigns a share

to each child node, such as the sum of all shares is s. If the node is **OR**, it assigns the same value s to its child nodes. For the sake of simplicity, we mentioned only access policies which consist of **AND** and **OR** nodes, however, our scheme could also support threshold nodes or **Out Of** nodes. The resulted ciphertext consists of the following components:

$$\mathbf{CT}_{\tau,\Re} = \begin{pmatrix} C^{(1)} = m \oplus H_1(\hat{e}(g,g)^{\alpha s}), & C^{(2)} = \hat{e}(g,g)^{\beta s}, & C^{(3)} = g^s, \\ \{C^{(4)}_{j,\hat{i}} = g^{x_j s_{\hat{i}}}\}_{a_{j,\hat{i}} \in \tau}, & \{C^{(5)}_i = g^{sP(I_{ui})}\}_{I_{ui} \in \Re} & \end{pmatrix}$$

4. **Decryption**$(\mathbf{CT}_{\tau,\Re}, \mathbf{SK}_{I_{u_i},\omega})$. The decryption algorithm takes as input the ciphertext $CT_{\tau,\Re}$ and the decryption key $SK_{I_{u_i},\omega}$. It checks if the secret key $SK_{I_{u_i},\omega}$ related to the attribute set ω satisfies the access policy τ. If yes, then the algorithm chooses the smallest subset ω' that satisfies τ and proceeds as follows:

$$Z^{(1)} = C^{(2)} \prod_{a_j \in \omega'} \hat{e}(D^{(2)}_j, C^{(4)}_{j,\hat{i}}) = \hat{e}(g,g)^{\beta s} \prod_{a_j \in \omega'} \hat{e}(g^{\frac{x-\beta}{x_j}}, g^{x_j s_{\hat{i}}}) = \hat{e}(g,g)^{xs}$$

$$Z^{(2)} = \hat{e}(C^{(3)}, D^{(3)})^{\lambda_u} \cdot \prod_{I_{u_j} \in \Re} \hat{e}(C^{(5)}_i, D^{(4)})^{\lambda_{u_j}} = \hat{e}(g^s, g^{yP(0)})$$

$$Z^{(3)} = \hat{e}(D^{(1)}, C^{(3)}) \cdot Z^{(1)} \cdot Z^{(2)} = \hat{e}(g,g)^{\alpha s}$$

The decryption algorithm recovers the message m as: $m = \left(C^{(1)} \oplus H_1(Z^{(3)})\right)$. *Note:*$\lambda_i$'s in $Z^{(2)}$ are Lagrange coefficients $\lambda_i = \prod_{j \neq i} \frac{-j}{i-j}$. A revoked user will not be capable to compute $Z^{(2)}$, hence it cannot recover the message m.

2.1 Security Proof

Theorem 1. Suppose the DBDH assumption holds. Then no polynomial adversary can break the CP-ABBE scheme with non-negligible advantage.
The complete security proof will be provided in the full version of this paper.

3 Conclusions

In this work, we present a ciphertext-policy attribute-based broadcast encryption scheme. The proposed scheme has the capability to revoke users from a broadcasted message. The scheme could be used to revoke a limited number of users with fixed and small ciphertext size. The security has been proved under DBDH assumption.

References

[1] The US Department of Health and Human Services. Summary of the HIPAA Privacy Rule, 2003.

[2] M. Naor and B. Pinkas. Efficient trace and revoke schemes. In *Proceedings of the 4th International Conference on Financial Cryptography*, pages 1–20. Springer, 2000.