Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption

Abstract

Attribute-based encryption (ABE) provides a mechanism for complex access control over encrypted data. However in most ABE systems, the ciphertext size and the decryption overhead, which grow with the complexity of the access policy, are becoming critical barriers in applications running on resource-limited devices. Outsourcing decryption of ABE ciphertexts to a powerful third party is a considerable manner to solve this problem. Since the third party is usually believed to be untrusted, the security requirements of ABE with outsourced decryption should include privacy and verifiability. Namely, any adversary including the third party should learn nothing about the encrypted message, and the correctness of the outsourced decryption is supposed to be verified efficiently. We propose generic constructions of CPA-secure and RCCA-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respectively. We also instantiate our CPA-secure construction in the standard model and then show an implementation of this instantiation. The experimental results show that, compared with the existing scheme, our CPA-secure construction has more compact ciphertext and less computational costs. Moreover, the techniques involved in the RCCA-secure construction can be applied in generally constructing CCA-secure ABE, which we believe to be of independent interest.
EXISTING SYSTEM

Outsourcing decryption of ABE ciphertexts to a powerful third party is a considerable manner. The third party is usually believed to be untrusted, the security requirements of ABE with outsourced decryption should include privacy and verifiability.

DRAWBACK OF EXISTING SYSTEM

- Complexity of access policy to the ciphertext and decryption overhead on computational cost.
- Applications running on resource-limited devices.

PROPOSED SYSTEM

Generic constructions of CPA-secure and RCCA-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respectively. We also instantiate our CPA-secure construction in the standard model and then show an implementation of this instantiation.

ADVANTAGE OF PROPOSED SYSTEM

- More compact ciphertext and less computational costs.
- RCCA-secure construction with CCA-secure ABE, which we believe to be of independent interest.
- Contributes to access control over encrypted data.
SYSTEM SPECIFICATION

Hardware Requirements

System : Pentium IV 2.4 GHz
Hard Disk : 40 GB
Floppy Drive : 1.44 Mb
Monitor : 15 VGA Colour
Mouse : Logitech
Ram : 512 Mb

Software Requirements

Operating system : Windows Family
Tools : eclipse
Technology Used : Java
Backend Used : SQLITE