**Revisiting Attribute-Based Encryption With**

**Verifiable Outsourced Decryption**

Abstract:

Attribute-based encryption (ABE) is a promising technique for fine-grained access control of encrypted data in a cloud storage, however, decryption involved in the ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity. In order to reduce the decryption overhead for a user to recover the plaintext, Green *et al.* suggested to outsource the majority of the decryption work without revealing actually data or private keys. To ensure the third-party service honestly computes the outsourced work, Lai *et al.* provided a requirement of verifiability to the decryption of ABE, but their scheme doubled the size of the underlying ABE ciphertext and the computation costs. Roughly speaking, their main idea is to use a parallel encryption technique, while one of the encryption components is used for the verification purpose. Hence, the bandwidth and the computation cost are doubled In this paper, we investigate the same problem. In particular, we propose a more efficient and generic construction of ABE with verifiable outsourced decryption based on an attributebased key encapsulation mechanism, a symmetric-key encryption scheme and a commitment scheme. Then, we prove the security and the verification soundness of our constructed ABE scheme in the standard model. Finally, we instantiate our scheme with concrete building blocks. Compared with Lai *et al.*’s scheme, our scheme reduces the bandwidth and the computation costs almost by half.

**EXISTING SYSTEMS:**

* the existing pairing-based ABE schemes (see [6], [8]), the number of pairing operations to decrypt a ciphertext is linear to the complexity of the access

policy.

* It would be a significant challenge for users to complete the decryption independently on resource-constrained devices, e.g., mobile phones.
* In order to reduce the number of pairing operations for users when executing the decryption algorithm, considered outsourcing the heavy computation of decryption to a third-party service, which helps to implement “thin clients.”
* existing pairing-based AB-KEMs (KP or CP) satisfy the property of multiplicative homomorphism. Thus, our technique can be applied to most existing AB-KEMs in both KP and CP settings.
* Therefore, we conclude that our instantiation of ABE with verifiable outsourced decryption is more efficient than the existing scheme.

**ADVANTAGES:**

 **We** have flexible access control of encrypted data utilizing access policies and described attributes associated with private keys and ciphertexts respectively.

 the ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity.

 To keep the data security and privacy for data owners, the sharing data needs to be encrypted before being uploaded and fine-grained access control is required.

**DISADVANTAGE:**

Itprovided a requirement of verifiability to the decryption of ABE, but their scheme doubled the size of the underlying ABE ciphertext and the computation costs.

**PROPOSED SYSTEMS**

* + A more efficient and generic construction of ABE with verifiable outsourced decryption based on an attribute based key encapsulation mechanism, a symmetric-key encryption scheme and a commitment scheme.
	+ Then, we prove the security and the verification soundness of our constructed ABE scheme in the standard model
	+ According to the cipher text associated with an access policy or containing a set of attributes, ABE schemes are divided into two kinds: ciphertextpolicy (CP) ABE and key-policy.
	+ We revisit ABE with verifiable outsourced decryption (VO-ABE), and try to solve these problems. We first present a generic construction of VO-ABE, based on an attribute-based key encapsulation mechanism.
	+ An appropriate transform for the actual secret key to achieve outsourcing the decryption. In fact, the transform we used here may be thought as a subclass of all-or-nothing transforms (AONTs).

**ADVANTAGE:**

Instantiation of ABE with verifiable outsourced decryption is more efficient than the existing scheme.

 Attribute based encryption (ABE) have flexible access control of encrypted data utilizing access policies and ascribed attributes associated with private keys and cipher texts respectively.

A key blind

ing technique to outsource the decryption without leaking data or secret keys as a precaution against maliciously detecting from the third-party service.

**IMPLEMENTATION**

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

 The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**MODULE DESCRIPTION**:

 The system is proposed to have the following modules along with functional requirements.

* Attribute-Based Encryption
* Verifiability
* Access Control
* Reencryption
* Outsourced Decryption

**Attribute-Based Encryption:**

Attribute-BasedEncryption (ABE) was thus proposed to have flexible access control of encrypted data utilizing access policies and ascribed attributes associated with private keys and ciphertexts respectively. attribute-based encryption, most of ABE systems are constructed with pairings while the computation cost in the decryption phase grows along with the size of the access policy. ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity. encryption requires the data sender to encrypt an extra random message and compute a checksum value related to two messages; decryption requires the third-party service to execute the underlying decryption algorithm twice and the data receiver to verify the outsourced computation with respect to the encrypted messages.

**Verifiability:**

No challenged file blocks should be retrieved by the verifier (*e.g.*, cloud,admin) during verification process for efficiency concern.

 **Access Control:**

To keep the data security and privacy for data owners, the sharing data needs to be encrypted before being uploaded and fine-grained access control is required. encryption (ABE) was thus proposed to have flexible access control of encrypted data utilizing access policies and ascribed attributes associated with private keys and ciphertexts respectively. The functionality of access control is very powerful, however, expensive. We generate the pulic key and privatekey to provide dataowner ,and datauser.

**Outsourced Decryption:**

decryption involved in the ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity. In order to reduce the decryption overhead for a user to recover the plaintext, Green et al. suggested to outsource the majority of the decryption work without revealing actually data or private keys. It would be a significant challenge for users to complete the decryption independently on resource-constrained devices.

They proposed a key blinding technique to outsource the decryption without leaking data or secret keys as a precaution against maliciously detecting from the user service.

**Reencryption:**

Attribute-based encryption is a promising technique for fine-grained access control of encrypted data in a cloud storage. The sharing data needs to be encrypted before being uploaded and fine-grained access control is required.the data will be more secured in cloud storage. To perform the fine grain access control to be generate secretkey in dataowner.

 **CONCLUSION**

We evaluate the performance of our instantiation of CP-ABE scheme with verifiable outsourced decryption. For comparing the efficiency of our scheme to the LDGW-scheme , we tabulate the exponential and pairing operations . As show our scheme only requires nearly half of the modular exponentiations used in the

LDGW-scheme during the encryption phase and needs one less modular exponentiation in G*T* than during the final decryption phase. The computation cost for the third-party service to transform a standard ABE ciphertext in our scheme is half of that in. For further comparison of the efficiency, we implement the schemes the encryption time and the size of a standard ABE ciphertext of our scheme are far less than . Specifically, a message encrypted under a policy with 100 attributes needs around 1 second and the size of the generated ciphertext is around 16.68 KB, which are both nearly half of the counterparts illustrates that the third-party service for our scheme just needs half of the time used in to transform a standard ABE ciphertext. The final decryption time is slightly more than half of that in .

All our experimental results are coincident with the theoretic analysis presented above. Therefore, we conclude that our instantiation of ABE with verifiable outsourced decryption is more efficient than the existing scheme.