**Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption**

**Abstract:**

Attribute-based encryption (ABE) with outsourced decryption not only enables fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of cipher text size and decryption cost) of the standard ABE schemes. In particular, an ABE scheme with outsourced decryption allows a third party (e.g., a cloud server) to transform an ABE cipher text into a (short) El Gamal-type cipher text using a public transformation key provided by a user so that the latter can be decrypted much more efficiently than the former by the user. However, a shortcoming of the original outsourced ABE scheme is that the correctness of the ***cloud server’s transformation cannot be verified by the user. That is, an end user could be cheated into accepting a wrong or maliciously transformed output.*** **In this paper,** we first formalize a security model of ABE with verifiable outsourced decryption by introducing a ***verification key*** *in the output of the encryption algorithm*. Then, we present an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general, and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE **neither increases** the user’s and the cloud server’s **computation costs except some nondominant operations** (e.g., hash computations), nor expands the cipher text size except adding a hash value (which is <20 byte for 80-bit security level). We show a concrete construction based on **Green et al.’s cipher text-policy** ABE scheme with outsourced decryption, and provide a detailed performance evaluation to demonstrate the advantages of our approach.