Key-Policy ABE with Delegation of Rights

Lenaïck Gouriou

Leanear, DIENS, École normale supérieure, CNRS, PSL
University, INRIA, Paris, France

December 6, 2021

A Key-Policy Attribute-Based Encryption (KP-ABE) scheme is a public key scheme where a policy is embedded inside each user's private key, and the ciphertext is associated with attributes. Users can then decrypt a message if the policy in their keys is fulfilled by the attributes in the ciphertext.

We present a KP-ABE scheme which meet two requirements :

- It allows for fine-grained delegation without interacting with any authority, meaning that any user can create new keys with total autonomy, as long as their policy is more strict than the original.
- It allows for private blackbox traitor-tracing, meaning that under certain hypothesis, it is possible to identify which user's key was used to create a new key for an illegitimate third-party.

The scheme was designed to answer the following use case. Nowadays it's common that users possess multiple devices that comes in all forms and for all kinds of use : smartphone, laptop, desktop computer, for work and for personal use. Ideally, users want to manage these many devices in a way that is both ergonomic and secure. Thus, they must be in control of the decrypting permissions of each of their devices, while not depending on any authority to configure them. Fine-grained delegation perfectly answers these problematics. Tracing as an additional feature gives more agency to users by allowing them to know when one of their device has been compromised.

On a technical level, our scheme is constructed from pairings on elliptic curve under the Dual Pairing Vector Space framework developed by Okamoto and Takashima, under the SXDH assumption (ie. DDH in both groups as a source for the pairing). One of the main technical challenge was to overcome a natural friction between delegation and tracing : On the one hand, for delegation, users must be given enough information in the public key to be able to produce valid delegated keys. On the other hand, for the tracing process to be effective, users must not be able to detect it. Information required for delegation may help to detect tracing.