Hybrid Proxy Re-Encryption

Cloud storage. Cloud storage is a secure storage system which stores users' data in a "secure way", with as purpose those users to be able to access their data anywhere, at anytime, from any authorized devices, and only them. The most interesting case is when the cloud storage is dynamic since it permits to control the access to the data by adding/deleting devices/users. The idea behind cloud storage is that data are stored as if they were in a safe, where the cloud storage plays the role of an access control to this safe. In reality, the data are encrypted and, most of the time, the cloud server has the decryption key and manages the rights to each user to access or not the data.

Ateniese, Fu and Hohenberger proposed a privacy-preserving architecture for distributed storage which makes use of a so-called proxy re-encryption (PRE) scheme. A similar system have next been proposed in the case of cloud storage by Tysowski and Anwural Hasan. With such a system, where the cloud plays the role of the proxy, the access to a plaintext is only permitted to authorized users. For example, a data can be stored on a dedicated cloud storage using Alice's public key. If Bob can access this document, the proxy/cloud makes use of the re-encryption from Alice to Bob.

Proxy re-encryption schemes. PRE, invented in 1998 by Blaze, Bleumer and Strauss, allows a user A to delegate its decryption capability to a user B. To do so, this user A, computes a *re-encryption key* $R_{A\to B}$. This re-encryption key allows the proxy to transform a ciphertext originally intended to A into a ciphertext intended to B. While doing this transformation, the proxy cannot learn *any* information on the plaintexts nor the secret keys of both Alice and Bob.

The cloud storage of Ateniese *et al.* makes use of a *unidirectional* and *single-hop* scheme, which means (1) that with a re-encryption key $R_{A\to B}$, a proxy cannot translate a ciphertext intended to Bob, into a ciphertext intended to Alice and (2) that once a message has been moved into a ciphertext intended to Bob, no more transformation on the new ciphertext intended to Bob is possible. It also exists in the literature several PRE schemes which are *bidirectional*, meaning that they allow a symmetrical transformation, and *multi-hop*, meaning that several translations are possible.

Related work. It exists in the literature numerous papers on PRE schemes. Some of them are unidirectional and single-hop and some others are bidirectional and multi-hop. Thus, even if this is theoretically possible, both couples (unidirectional, single-hop) and (bidirectional, multi-hop) seem to be indissociable in practical constructions[1].

A matter of trust. In fact, using a bidirectional (and thus most of the time multi-hop) PRE in the case of cloud storage is not really a good thing regarding security. In fact, in the above example, Alice trusts Bob so that this latter can access Alice's confidential documents, but this does not necessarily mean that Bob trusts Alice. Similarly, if Alice trusts Bob and Bob trusts Carol, it does not necessarily mean that Alice trusts Carol: trust is thus not transitive and a multi-hop scheme is not necessarily a good choice for such system.

However, in some cases, a multi-hop (and thus most of the time bidirectional) scheme can be really useful, and in particular when *e.g.* Alice loses one of her device. In this case, the corresponding decryption secret key is compromised and cannot be used anymore. Thus, if a data is encrypted with the corresponding public key, this can be a problem. But the power of a (even unidirectional) PRE scheme is such that the proxy can re-encrypt the ciphertext - and next delete the old one - so that another key can be used to decrypt the ciphertext. However, the result could not be re-encrypted anymore if a single-hop PRE scheme is used. One possibility consists in asking the owner of the secret key related to the new encrypting public key to decrypt and then encrypt again the data, which leads to a very unpractical system. The second possibility is to make use of a bidirectional multi-hop scheme but this implies the above problem regarding trust between people. The last solution is to use a unidirectional multi-hop PRE scheme but, no practical construction exists.

Hybrid PRE. In this paper, we investigate a new approach which consists in designing a hybrid scheme which can be either unidirectional and single-hop *or* bidirectional and multi-hop. All the possibilities are sum up in Figure 1. Our idea is that if Alice owns several different devices, the trust she has in all her devices is similar and thus, in that particular case, we can use a bidirectional and multi-hop PRE: the trust is mutual. Regarding one Alice's device and one Bob's device, there is no mutual and transitive trust and we use in this case a unidirectional and single-hop PRE.

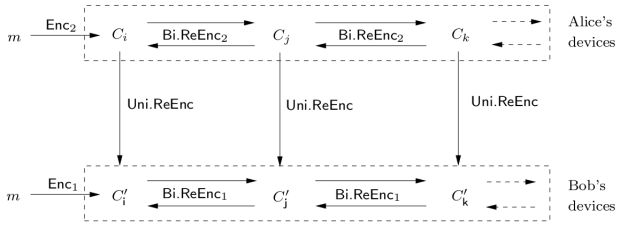

Fig. 1. General scheme for hybrid PRE

Organization. We formally introduce the concept of the hybrid PRE (HPRE), which notion is, to the best of our knowledge, new. We give several generic results regarding the link between HPRE, unidirectional single-hop PRE and bidirectional multi-hop PRE. We finally propose a practical construction of HPRE, based on the Libert-Vergnaud PRE scheme, which can directly be implemented to manage the lost of devices in a privacy-preserving cloud storage system.

[1] With one exception: Deng, Weng, Liu and Chen have proposed a secure bidirectional single-hop PRE scheme.