Towards Fine-Grained Secure Communications

Tatsuaki Okamoto
Fellow, Nippon Telegraph and Telephone Corporation, Japan

Abstract:

Although many encryption systems have been developed to make communications secure for several thousands of years (mainly for military and diplomatic applications before the 1960s), any traditional encryption system before the 1970s faced a great restriction in terms usage, i.e., a pair comprising a sender and receiver should be fixed before establishing secure communications. The innovative notion of public-key cryptosystems in the 1970s relaxed this restriction, where a sender of secure communications did not need to be fixed, i.e., anyone could send an encrypted message to a receiver who published a public key. However, public-key cryptosystems still have a restriction with respect to the receivers; a receiver should be fixed by a value (its public key) registered or certified before initiating secure Communications. Recently a new innovation has appeared.

In identity-based encryption (IBE), the receiver does not need to be fixed by a value that is registered or certified before initiating secure communications, but is only fixed by an arbitrary value (e.g., its identity). Attribute-based encryption (ABE) and predicate encryption (PE) have fewer restrictions or provide more flexibility to the receivers. A set of (possible) receivers is determined by the properties (requirements) that are set for each ciphertext and even a sender who sets the properties for the ciphertext has no idea who are the (possible) receivers. In other words, the relations between senders and receivers in traditional cryptosystems are coarse-grained, while those in ABE and PE are fine-grained. For example, a sender sets properties such as [Type = animation, and Restriction = NC-17, and Group = group 2] on a ciphertext regarding the plaintext (e.g., contents). A user is issued (or purchases) a secret key, on which a policy (predicate) is set for decryption such as [(Type = (drama or animation or news), and Age = over 20), or Group = group 1]. The ciphertext (the contents) can be decrypted (accessed) by the user using the secret key, but cannot be decrypted using another key such as [Type = drama or news, and Age = over 20, and Group = any]. Typical applications of this technology are broadcast or database services of contents, where the access control is executed by such fine-grained encryption in a distributed manner. Fine-grained authentication schemes such as attribute-based signatures have been also developed.