AICA2013
Faculty of Informatics, UCM
Madrid (Spain), November 7-8th 2013.

Asymmetric group key agreement and contributory broadcast encryption

Josep Domingo-Ferrer [1]

In this talk, we review our notions of asymmetric group key agreement and contributory broadcast encryption. Both are intended to implement asymmetric secure group communications over open networks. We introduced asymmetric group key agreement in Eurocrypt 2009 and contributory broadcast encryption in Asiacrypt 2011.

First, the concept of asymmetric group key agreement is presented. A group key agreement (GKA) protocol allows a set of users to establish a common secret via open networks. Observing that a major goal of GKAs for most applications is to establish a confidential channel among group members, we revisit the group key agreement definition and distinguish the conventional (symmetric) group key agreement from asymmetric group key agreement (ASGKA) protocols. Instead of a common secret key, only a shared encryption key is negotiated in an ASGKA protocol. This encryption key is accessible to attackers and corresponds to different decryption keys, each of which is only computable by one group member.

Then we present contributory broadcast encryption. Broadcast encryption (BE) schemes allow a sender to securely broadcast to any subset of members but requires a trusted party to distribute decryption keys. Asymmetric group key agreement (ASGKA) protocols enable a group of members to negotiate a common encryption key via open networks so that only the members can decrypt the ciphertexts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the ciphertexts. We bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (CBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice.

[1] Universitat Rovira i Virgili
Departament d'Enginyeria Informática i Matemátiques
Av. Països Catalans, 26.
43007 Tarragona-Spain
josep.domingo(at)urv.cat