Formal Grammar Identity-based Cryptography

Ádám Vécsi[1] and Attila Pethő[2]
Department of Computer Science, Faculty of Informatics, University of Debrecen
Kassai út 26, 4028 Debrecen, Hungary
[1]vecsi.adam@inf.unideb.hu
[2]petho.attila@inf.unideb.hu

Identity-based Cryptography (IBC) is an important branch of public-key cryptography. The original concept behind IBC was coined by Adi Shamir in 1984, who managed to build an identity-based signature scheme. However, identity-based encryption remained an unsolved problem until Dan Boneh and Matthew Franklin created their pairing-based scheme in 2001, providing feasible performance for practical use.

The uniqueness of IBC lies in the fact that its public key is a string which clearly identifies an individual in a certain domain. One may think about an email address or a username. This is in direct connection with the core idea of the IBC, which was to simplify the certificate management and eliminate the need for certification authorities. Assuming the use of the public key infrastructure, usually, a key is bound to its user's identity with a public key certificate, while with IBC the user's identity is the public key, so there is no need for the certificate.

Furthermore, the public key may contain more information, than just the identity of the user. It is possible to extend it with domain-specific data, this way the public key itself could carry useful information, which enables a wide spectrum of interesting use cases. Although there is a disadvantage of the IBC, the public key of the receiver must be bit-accurate to the encryption key, to access the belonging private key.

One possible solution to this problem is Attribute-based Cryptography (ABC). This type of cryptosystem uses an access structure to determine which cyphertexts a user can decrypt. This way it is possible to use logical operators between attributes and values, so the public key is more flexible and allows to target a group of receivers too. The drawback of the ABC schemes is that they require more and more computation on the user-side (encryption and decryption functions), with the growth of the access structure, which affects the usability of these protocols.

Our solution to the above problems is called Formal Grammar Identity-based Cryptography. The idea was to separate the public key, which is used for the encryption, and the access structure, that way we can use existing IBC schemes and extend it. In the protocol, the access structure is provided by the sender via authorization grammar, which generates those user public keys, which are permitted to access the decryption key and the private key generator is responsible to check if a user is permitted or not. It provides a more flexible access control than the ABC scheme, without affecting the user-side computation cost with the growth of the access structure.