

TP 05: Identity-Based Encryption

David Galindo

Université du Luxembourg
www.dgalindo.es

1 Three-Party Diffie-Hellman Key Exchange

Assuming the BDDH problem is hard to solve (i.e. determining β when given (g, g^a, g^b, g^c, Z) where $Z = e(g, g)^{abc}$ if $\beta = 1$ and $z \leftarrow \mathbb{G}_1$ otherwise), describe how Alice, Bob and Charlie can non-interactively build a common secret key K_{ABC} such that they are sure this key is only known to them. That is, define

- their respective public/secret keys $(pk_A, sk_A), (pk_B, sk_B), (pk_C, sk_C)$
- How Alice on inputs $(pk_A, sk_A), pk_B, pk_C$ computes K_{ABC}
- How Bob on inputs $(pk_B, sk_B), pk_A, pk_C$ computes K_{ABC}
- How Charlie on inputs $(pk_C, sk_C), pk_B, pk_A$ computes K_{ABC}

2 Digital signatures from Identity-Based Encryption

[Extracted from *SIAM J. of Computing*, Vol. 32, No. 3, pp. 586-615, 2003. An extended abstract of this paper appears in the *Proceedings of Crypto 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229, Springer-Verlag, 2001.]

IBE implies signatures. Moni Naor has observed that an IBE scheme can be immediately converted into a public key signature scheme. The intuition is as follows. The private key for the signature scheme is the master key for the IBE scheme. The public key for the signature scheme is the global system parameters for the IBE scheme. The signature on a message M is the IBE decryption key for $ID = M$. To verify a signature, choose a random message M_0 , encrypt M_0 using the public key $ID = M$, and then attempt to decrypt using the given signature on M as the decryption key. If the IBE scheme is IND-ID-CPA, then the signature scheme is existentially unforgeable against a chosen message attack. Note that, unlike most signature schemes, the signature verification algorithm here is randomized. This shows that secure IBE schemes incorporate both public key encryption and digital signatures.

1. Describe the digital signature scheme obtained from applying the generic transformation sketched above to the Boneh-Franklin IBE scheme.
2. Describe your intuition on why an attacker against this digital signature scheme implies an attacker against the indistinguishability of encryptions of the Boneh-Franklin IBE scheme.