Courbes elliptiques — 4TMA902U

Responsables : G. Castagnos, D. Robert

Identity Based Encryption

Boneh and Franklin have proposed in 2001 an identity based encryption (IBE) scheme using pairing friendly elliptic curves. Let $e : \mathrm{G} \times \mathrm{G} \to \mathrm{G}_t$ be a type I (symmetric) cryptographic pairing. Let ℓ be the prime order of G and G_t and P a generator of G.

Disclaimer : we will use a type I pairing for simplicity, but in practice this means that we will use a supersingular curve that must be defined over a large prime field for security. This is inefficient compared with using a type III pairing.

1 Alice has a public key $\mathrm{A} := a\mathrm{P}$ and a secret key $a \in \mathbf{Z}/\ell\mathbf{Z}$. Bob has a public key $\mathrm{B} := b\mathrm{P}$ and a secret key $b \in \mathbf{Z}/\ell\mathbf{Z}$. Let $m \in \mathrm{G}_t$ be a plaintext. Show how Carl can create a ciphertext C of m that Alice and Bob can both decrypt (hint : get inspired by the Tripartite Diffie-Hellman key exchange).

2 Oscar intercepts C. What problem must he solve in order to decrypt C and retrieve m ?

3 From this protocol, we want to devise an identity based encryption (IBE) scheme. To simplify, suppose that the set of identities are the elements of G. Suppose Carl wants to encrypt $m \in \mathrm{G}_t$ for Bob using B as the identity of Bob (and assuming that Bob does not know the secret b anymore). From the protocol of question 1 show how to build this IBE scheme (hint : view Alice has the public key generator that provides a secret key to Bob in order to decrypt).

4 Now suppose that identities can be arbitrary bit-strings, $\mathsf{ID} \in \{0,1\}^*$. How can we get a full IBE scheme from the scheme of the previous question (this should give you the Boneh and Franklin IBE scheme) ?

5 Implement this scheme using a supersingular curve.

6 Show how to simplify the generic construction from an IBE scheme to a digital signature scheme in order to retrieve the BLS scheme of last week from the Boneh and Franklin IBE scheme.