

# TP 11: Cocks' Identity-Based Encryption

David Galindo

Université du Luxembourg  
www.dgalindo.es

## 1 Identity-Based Encryption based on Quadratic Residuosity

The goal is to implement an Identity-Based Encryption using the tools from previous assignments. In particular you can make use of the NTL library in [www.shoup.net](http://www.shoup.net).

1. Find a description of Cocks' IBE scheme in [http://www.csie.nctu.edu.tw/~pctsai/20070904\\_Cocks.pdf](http://www.csie.nctu.edu.tw/~pctsai/20070904_Cocks.pdf)
2. Implement the Jacobi symbol  $\left(\frac{a}{n}\right)$  for  $n$  a 1024-bit RSA modulus such that  $n = pq$  and  $p = q = 3 \pmod{4}$ . Such a modulus  $n$  is called a Blum integer.
3. Let  $a$  be a quadratic residue modulo a Blum integer  $n = pq$ . Implement a procedure that given  $a, n$  computes  $r$  a square root of  $a$  modulo  $n$ . An integer  $r$  such that  $r^2 = a \pmod{n}$  can be computed as

$$r = a^{\frac{n+5-(p+q)}{8}} \pmod{n}.$$

$r$  is precisely a square root of  $a$  modulo  $n$ .

4. Implement the Cocks' IBE scheme for a 1024-bit length Blum integer  $n$  and identities  $ID \in \mathbb{Z}_n$ . Notice that a hash function  $h : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  such that  $\left(\frac{h(ID)}{n}\right) = 1$  for every  $ID \in \mathbb{Z}_n$  can be obtained by successively applying a standard hash function  $g : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ . That is  $h(ID) = g(\dots g(g(ID)) \dots)$  until  $\left(\frac{g(\dots g(g(ID)) \dots)}{n}\right) = 1$ .