

# Advanced Topics in Cryptography

## Lecture 9: Identity based encryption (IBE), Cocks' scheme.

Benny Pinkas

## Related papers

- Lecture notes from MIT  
<http://crypto.csail.mit.edu/classes/6.876/lecture-notes.html>
- Clifford Cocks , An Identity Based Encryption Scheme based on Quadratic Residues.  
<http://www.cesg.gov.uk/site/ast/idpkc/media/ciren.pdf>

## Identity based encryption (IBE)

- A public-key encryption scheme where the key can be an arbitrary string
  - In RSA, the public key must be of the form  $n=p \cdot q$
- Typical application:
  - The public key is the user's identity
  - If we want to send messages to Alice we don't need to know her public key
- The idea was suggested by Shamir in 1987
  - Only makes sense if there is an additional trusted entity which provides users with their private keys

## The setting

- Key generation center (KGC)
  - Holds the master private key
  - Generates public system parameters
- Key derivation: The KGC can provide each user with the private key corresponding to his/her name.
  - The private key is a function of the name (or an arbitrary string) and the master private key
- Encryption: everyone can encrypt messages to Alice. The ciphertext is a function of the plaintext, Alice's name, and the public parameters.
- Decryption: Alice uses her private key and the system parameters to decrypt messages sent to her

## Applications

- A public key infrastructure without certificates
  - To encrypt, you only need to get the system parameters from the KGC (once for all users)
  - Can encrypt messages to Alice even before she obtains her private key
- A solution to revocation of public keys
  - The public key can be of the form Alice@foo.com|date, and change every day.
  - Alice needs to obtain a new private key for every day. Can take with her only the keys which are currently needed.
  - Revocation is simple.
  - Adding credentials: alice@foo.com|date|cleanace.

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 5

## Applications

- Temporary keys
  - Alice could generate the keys by herself, and use it with her different devices.
- Delegation of duties
  - Encrypt messages to doctor-in-charge@foo.com|date, accounting@foo.com|date .
  - The public key is encoded as an XML schema, which defines the access policy. In order to decrypt, you must get the corresponding private key from the KGC, which checks whether you are entitled to get it.

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 6

## Identity based encryption

- Master Key Generation:
  - $\text{MKG}(1^k) \rightarrow (\text{PK}_{\text{master}}, \text{SK}_{\text{master}})$
- Key Generation:
  - $G(\text{ID}, \text{SK}_{\text{master}}) \rightarrow \text{SK}_{\text{ID}}$
- Encryption:
  - $E(m, \text{ID}, \text{PK}_{\text{master}}) \rightarrow c$
- Decryption
  - $D(c, \text{ID}, \text{SK}_{\text{ID}}) \rightarrow m$  such that  $c = E(m, \text{ID}, \text{PK}_{\text{master}})$

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 7

## IBE – security definitions

- Main challenge: adversary can get private keys of some identities, while attacking a different identity
- Adaptively-chosen-key semantic security
  1. The adversary obtains keys for a polynomial number of IDs, which it chooses adaptively
  2. It outputs a different  $\text{ID}^*$ , and two messages  $m_0, m_1$
  3. It receives  $E(m_b, \text{ID}^*)$ , for  $b \in_{\mathbb{R}} \{0, 1\}$
  4. The adversary tries to guess  $b$
- Variants:
  - Selective-ID: the adversary selects  $\text{ID}^*$  before receiving the IDs in Step 1 (i.e.,  $\text{ID}^*$  is not a function of Step 1).
  - Adaptively-chosen-key chosen-ciphertext security: the adversary can mount chosen-ciphertext attacks after Step 3.

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 8

## IBE – constructions

- Clifford Cocks
  - A construction based on Quadratic Residuosity
  - Encrypts one bit at a time
- Boneh-Franklin
  - A more efficient construction based on bilinear maps
  - (which is a slightly less accomplished assumption)

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 9

## Cocks' IBE scheme – Number theory background

- We work in  $Z_n^*$
- $x$  is a quadratic residue in  $Z_n^*$  ( $x \in QR_n$ ) if there exists  $y \in Z_n^*$  such that  $x = y^2 \pmod n$ .
- If  $p$  is prime, then the Legendre symbol  $\left(\frac{x}{p}\right)$  is 1 if  $x$  is a  $QR_p$ , and -1 otherwise.
- $x^{(p-1)/2} \pmod p = \left(\frac{x}{p}\right)$
  
- $\forall n, x \in QR_n$  iff  $\forall p|n, x \in QR_p$

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 10

## The Jacobi symbol

- The Jacobi symbol generalizes the Legendre symbol for non-primes
- For  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ , the Jacobi symbol is
$$\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)^{a_1} \dots \left(\frac{x}{p_k}\right)^{a_k}$$
- The Jacobi symbol can be efficiently computed, even without knowing the factorization of  $n$ . (Alg 1.4.10, "A course in computational algebraic number th.", H. Cohen)
- Suppose  $n$  is a Blum integer:  $n=p \cdot q$ , where  $p=q=3 \pmod 4$ .
  - If  $\left(\frac{y}{n}\right) = 1$  then either  $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = 1$  or  $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1$
  - $y \in QR_n$ , only if  $y \in QR_p$  and  $y \in QR_q$ . Namely, the first option above.
  - Given  $p, q$ , it is easy to compute  $y^{1/2}$ , and therefore  $\left(\frac{y}{n}\right)$

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 11

## The Quadratic Residuosity assumption

- The Quadratic Residuosity assumption
  - Given a Blum integer  $n=pq$ , and a random  $y \in Z_n^*$ , such that  $\left(\frac{y}{n}\right) = 1$ , the probability of deciding whether  $y \in QR_n$  is negligibly close to  $1/2$ .
- If factoring is easy then so is deciding QR
- It is not known whether the converse is true or not

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 12

## Cocks' IBE scheme

- Master key generation:
  - The master private key is  $p, q$  (both large primes)
  - The public master key is  $n=pq$ .
- Key generation:
  - $H(\text{ID}) \rightarrow a_{\text{ID}}$ , such that  $\left(\frac{a_{\text{ID}}}{n}\right) = 1$  (therefore either  $a_{\text{ID}}$  or  $-a_{\text{ID}}$  has a square root modulo  $n$ )
  - Assume that  $\text{SK}_{\text{ID}}=(a_{\text{ID}})^{1/2}$  (otherwise the decryption fails)
- Encryption of a bit  $m \in \{-1, 1\}$ :
  - Choose  $t \in_{\mathcal{R}} \mathbb{Z}_n^*$  such that  $\left(\frac{t}{n}\right) = m$
  - $c_1 = t + H(\text{ID})/t \pmod n$
- Decryption:
  - Output  $\left(\frac{2\text{SK}_{\text{ID}}c_1}{n}\right) = 1$

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 13

## Correctness

- $\text{SK}_{\text{ID}}=(a_{\text{ID}})^{1/2}$
- $c_1 = t + H(\text{ID})/t = t + a_{\text{ID}}/t \pmod n$
- $c_1 + 2\text{SK}_{\text{ID}} = t + a_{\text{ID}}/t + 2(a_{\text{ID}})^{1/2} = (t^2 + a_{\text{ID}} + 2t(a_{\text{ID}})^{1/2})/t = (t + a_{\text{ID}})^2 / t$
- Therefore the Jacobi symbol of  $c_1 + 2\text{SK}_{\text{ID}}$  is the same as that of  $1/t$ , which is the same as  $\left(\frac{t}{n}\right) = m$
- If  $\text{SK}_{\text{ID}}=(-a_{\text{ID}})^{1/2}$  then decryption fails with probability  $1/2$
- To overcome this the encryption must be repeated, sending  $c_2 = t - H(\text{ID})/t = t - a_{\text{ID}}/t \pmod n$

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 14

## Proof of Security

- Suppose that  $H()$  is a random oracle.
- Suppose that there is an adversary  $A$  which breaks Cocks' scheme with probability  $1/2 + \epsilon$ , then we can compute quadratic residuosity with the same probability
- We build  $A'(n, a)$ , which decides whether  $a \in \text{QR}_n$ :
  - When  $A$  asks for  $\text{SK}_{\text{ID}}$ , we choose  $\text{SK}_{\text{ID}}$  at random. Then with probability  $1/2$  we define  $H(\text{ID})=(\text{SK}_{\text{ID}})^2$ , and with probability  $1/2$  we define  $H(\text{ID})=-(\text{SK}_{\text{ID}})^2$ , subject to  $\left(\frac{H(\text{ID})}{n}\right) = 1$
  - This is exactly the same distribution as in the original execution, since  $H()$  is modeled as a random function.

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 15

## Proof, contd.

- $A$  sends  $\text{ID}$ ,  $m_0, m_1$  (which are  $m_0=0, m_1=1$ ).
- $A'$  defines  $H(\text{ID})=a$
- $A'$  sends to  $A$  an encryption of  $m_b$ ,  $b \in_{\mathcal{R}} \{0, 1\}$ , where  $a$  replaces  $H(\text{ID})$ :  $c_1 = t + a/t \pmod n$
- If  $A$  finds  $b$ ,  $A'$  answers "QR", otherwise answers "not QR"
- Claim: If  $a \in \text{QR}_n$  then  $A$  sees the same distribution as in a real run
  - $A$  decrypts correctly (namely, finds  $\left(\frac{t}{n}\right)$ ) with probability  $1/2 + \epsilon$

May 14, 2006

Advanced Topics in Cryptography, Benny Pinkas

page 16

## Proof, contd.

- Claim: If  $a$  is not in  $QR_n$  then  $A$  learns nothing about  $a$ .
- Proof:
  - $A$  computes  $\left(\frac{t}{n}\right)$  from  $n, a$ , and  $s = (t+a/t) \bmod n$ .
  - If  $\left(\frac{a}{n}\right) = 1$  but  $a$  is not a QR, then  $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$
  - $s = (t+a/t) \bmod n$ , but consider also  $t_1, t_2, t_3$ 
    - $t_1 = t \bmod p, \quad t_1 = a/t \bmod q$
    - $t_2 = a/t \bmod p, \quad t_2 = t \bmod q$
    - $t_3 = a/t \bmod p, \quad t_3 = a/t \bmod q$
  - $s = (t+a/t) = (t_1+a/t_1) = (t_2+a/t_2) = (t_3+a/t_3)$ , and therefore from  $A$ 's point of view,  $t, t_1, t_2, t_3$  are all equally likely.
  - But  $\left(\frac{t}{n}\right) = \left(\frac{t_3}{n}\right) \neq \left(\frac{t_1}{n}\right) = \left(\frac{t_2}{n}\right)$
  - Therefore,  $A$  has probability  $1/2$  of outputting  $\left(\frac{t}{n}\right)$