AARHUS UNIVERSITY, COMPUTER SCIENCE

Crytography Handin 10

Peter Burgaard 201209175

December 8, 2016

PART 1

Using only the public key, one can transform an El Gamal ciphertext that encrypts message m efficiently into a different ciphertext that also encrypts m. Use this to show that the El Gamal cryptosystem is not CCA secure.

Adv is given a ciphertext c and a public key Pk, such that $c = E_{Pk}(m)$ for $m \in P$. To prove the El Gamal is not CCA secure *Adv* does the following:

Adv choses two new different plaint texts $m', m'' \in P$ and produces two ciphertexts $c' = E_{Pk}(m')$ and $c'' = E_{Pk}(m'')$. These are used to construct two new ciphertexts $c_1 = c \cdot c' = E_{Pk}(m) \cdot E_{Pk}(m') = E_{Pk}(m \cdot m')$ and $c_1 = c \cdot c'' = E_{Pk}(m) \cdot E_{Pk}(m'') = E_{Pk}(m \cdot m'')$.

Adv sends c_1 and c_2 to the oracle and receives m_1 and m_2, and can now check if $\frac{m_1}{m'} = m = \frac{m_2}{m''}$. If so, then we are in the real case, else we are in the ideal case.

PART 2

Suppose we change the cryptosysten as follows: say we are given an injective and easy invert function $f : \{0,1\}^t \to G$. To encrypt a bit string m, we encrypt $w = f(m)$ using El Gamal. The decryption first does El Gamal decryption to get w. If $w \in Im(f)$, outputs $f^{-1}(w)$, and outputs an error if $w \notin Im(f)$.

Show that this cryptosystem us not CCA secure either, regardless of which funcition f we use.

We are given a ciphertext c and a public keyPk, such that $c = E_{Pk}(w) = E_{Pk}(f(m))$ for $m \in P$ and $w \in Im(f)$.

The *Adv* starts out by finding the identity element for space G, which is easily done since the function f is easy to invert. Let this element be I and $f^{-1}(I) = I'$. We give the oracle message $m' = I'$ and receive c'. We see that if we give the oracle the ciphertext $c'' = c \cdot c' = E_{Pk}(f(m)) \cdot E_{Pk}(f(I')) = E_{Pk}(f(m) \cdot I) = E_{Pk}(f(m))$, we would get $f^{-1}(m)$ back, since $f(m) = w \in Im(f)$.

The *Adv* send c'' to the oracle an receives m''. The *Adv* can then gives m'' to the oracle an receives c'''. If $c = c'''$ then we are in the real case, and if not the we are in the ideal case.