AARHUS UNIVERSITY - COMPUTER SCIENCE DEPARTMENT

Cryptology - Handin 9

Peter Burgaard - 201209175

November 23, 2016

IF THE DDH PROBLEM IS HARD (W.R.T. GGEN), THEN THE EL GAMAL CRYPTOSYSTEM IS CPA SECURE

Proof. We will prove this by proof of contradiction. Assume the existence of an adversary Adv with advantage greater than ϵ against the El Gamal cryptosystem. We will make a polynomial time reduction DDH≤El Gamal.

The reduction is as follows;
The DDH is built on a group G, generator α and constants a and b which are used to generate α^a, α^b and $\alpha^{a\cdot b}$. Given a DDH cryptosystem we built our El gamal cryptosystem as such:

1. Base the system on the same group as DDH, lets name it G'
2. Base the system on the same generator as DDH, lets name it α'
3. Set $\beta := \alpha'^a$, note that DDH's $\alpha^a = \alpha'^a$ in our El Gamal cryptosystem
4. Encoding a messages is then based on the pair $(\alpha^b,\ \alpha'^{a\cdot b}\cdot m)$

It is easily varified that none of these steps takes more than polynomial time.

By construction Adv would take $(\alpha^b,\ \alpha'^{a\cdot b}\cdot m)$ and be able to decide whether he received the encrypted chosen message back from the oracle. Since this El gamal message is build on a reduction of DDH, the adversary can decide DDH with advantage greater than ϵ ↯.

No such adversary Adv can exist, and El Gamal must be CPA secure. □