THEOREM

SUPPOSE THE DDH ASSUMPTION HOLDS WITH RESPECT TO GenCG. THEN, THE ELGAMAL ENCRYPTION SCHEME IS SECURE

PROOF.

LET US CONSIDER, JUST FOR THE SAKE OF PROVING THIS RESULT, A VARIATION $\tilde{\Pi}$ OF THE ELGAMAL ENCRIPTION SCHEME, IN WHICH Gen IS KEPT LIKE IN ELGAMAL, WHILE Enc IS REPLACED BY THE FOLLOWING ALGORITHM:

$$\tilde{Enc}((\mathbb{G}, q, g, h), m):$$
$$y \leftarrow \mathbb{Z}_q; \quad z \leftarrow \mathbb{Z}_q; \quad \text{return } (g^y, g^z \cdot m)$$

ALTHOUGH BEING COMPLETELY USELESS IN PRACTICE, $\tilde{\Pi}$ SATISFIES THE FOLLOWING PROPERTY:

$$Pr\left[PubK^{eav}_{\tilde{\Pi},A}(n) = 1\right] - 1/2$$

THIS IS BECAUSE THE CHALLENGE CIPHERTEXT CONTAINS NO INFORMATION ALLOWING THE ADVERSARY TO DISCRIMINATE BETWEEN m_0 AND m_1, SIMPLY BECAUSE m IS MULTIPLIED BY g^z, AND THE FIRST COMPONENT g^y IS INDIPENDENT FROM g^z.

- NOW THE REAL PROOF BY REDUCTION CAN START. WE BUILD AN ADVERSARY B AGAINST DDH FROM AN ADVERSARY A AGAINST ELGAMAL IN SUCH A WAY THAT IF A IS SUCCESSFUL, THEN B IS SUCCESSFUL:

Adversary $B(\mathbb{G}, q, g, g^x, g^y, h)$:

- WE INVOKE A ON INPUT $1^{|q|}$ AND $(\mathbb{G}, q, g, g^x)$, AND A RETURNS m_0, m_1
- $b \leftarrow \{0, 1\}$
- WE BUILD C AS $\langle g^y, m_b \cdot h\rangle$
- WE PASS C TO A, WHICH RETURNS b^*
- WE RETURN $\neg(b^* \oplus b)$

WHAT CAN WE SAY? AT LEAST, WE KNOW THAT

$$Pr(PubK^{eav}_{A,\tilde{\Pi}}(n) = 1) = Pr(B(\mathbb{G}, q, g, g^x, g^y, g^z) = 1)$$
$$Pr(PubK^{eav}_{A,\Pi}(n) = 1) = Pr(B(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1)$$

ELGAMAL

NOW: IF A BREAKS Π, THEN $Pr(PubK^{eav}_{A,\Pi}(n) = 1)$ IS IN THE FORM $1/2 + \eta(n)$ WHERE η IS NOT NEGLIGIBLE. BUT SINCE WE KNOW THAT $Pr(PubK^{eav}_{A,\tilde{\Pi}}(n) = 1) = 1/2$, THEN WE CAN CONCLUDE THAT

$$\left|Pr(B(\mathbb{G}, q, g, g^x, g^y, g^z) = 1) - Pr(B(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1)\right|$$
$$= \eta(n)$$

WHICH IS THE THESIS: B IS SUCCESSFUL!