CSC 591 Cryptography 10/10/2018

Lecture 10 – ElGamal Encryption Scheme

Lecturer: Alessandra Scafuro *Scribe: Vibhav N.A. Srivaths*

ElGamal Encryption

In the previous lectures, we discussed the Diffie-Hellman Assumptions, Key Agreement, and the construction of pseudo random generators from the DDH assumption. We also discussed using the RSA Algorithm for the construction of a Public Key Encryption scheme.

In this lecture, we introduced the concept of the ElGamal Encryption Scheme and discussed its CPA security.

Definition

The ElGamal Encryption Scheme adapts the Diffie-Hellman key exchange protocol to give a CPA-secure public key encryption scheme. In the Diffie-Hellman key exchange protocol, we consider two entities Alice and Bob. Alice sends a message to Bob and Bob responds with a message to Alice. Both of them must be able to derive a shared key k from the transcripts that is indistinguishable from a uniformly random element from some group $\mathbb{G}$. Bob can use the shared value k to encrypt and send a message $m \in \mathbb{G}$ by sending $k \cdot m$ to Alice, and Alice can decrypt to m without any eavesdropper that is able to learn anything about m.

In the ElGamal Encryption scheme, we view Alice's first message as her public key and Bob's reply as a ciphertext. In order to prove the security of this scheme let us first state the following assumption that must hold true.

Assumption

To prove the security of ElGamal encryption scheme, we need the DDH assumption. Besides the DDH assumption, we need to introduce the following claim and prove it. Let $\mathbb{G}$ be a finite group, and $m \in \mathbb{G}$ be some arbitrary element of $\mathbb{G}$. Then, choosing a uniform $k \in \mathbb{G}$ and $c := k \cdot m$ gives the same distribution for c as choosing c uniformly random from $\mathbb{G}$. This can be represented for any $\hat{g} \in \mathbb{G}$ we have:

$$Pr[k \cdot m = \hat{g}] = \frac{1}{|\mathbb{G}|}$$

Proof: We consider $\hat{g} \in \mathbb{G}$ to be arbitrary. Then, we get:

$$Pr[k \cdot m = \hat{g}] = Pr[k = \hat{g} \cdot m^{-1}]$$

As k is uniform over $\mathbb{G}$, the probability that k is equal to the fixed element $\hat{g} \cdot m^{-1}$ is $1/|\mathbb{G}|$. Thus it is proved.

With the above proved, for the scheme let us consider $\mathcal{G}$ to be a polynomial time algorithm that takes input 1^n and outputs a tuple of a cyclic group $\mathbb{G}$, order q, and a group generator g. With these assumptions, we can construct the scheme as follows:

Scheme

Consider the following algorithms Π = (GEN, ENC, DEC) and define the public key encryption scheme as follows:

1. GEN: On input 1^n run $\mathcal{G}(1^n)$ and get $(\mathbb{G}, q, g)$. Choose a uniform element $x \in \mathbb{Z}_q$ and compute $h := g^x$. The public key is then $(\mathbb{G}, q, g, h)$, while the private key is $(\mathbb{G}, q, g, x)$ and the message space is $\mathbb{G}$.
2. ENC: On input of the public key $pk = (\mathbb{G}, q, g, h)$ and a message $m \in \mathbb{G}$, choose a uniformly random $y \in \mathbb{Z}_q$ and output the ciphertext $c = (g^y, h^y \cdot m)$.
3. DEC: On input of the private key $k = (\mathbb{G}, q, g, x)$ and the ciphertext (c_1, c_2), output: $\hat{m} := c_2/c_1^x$

Security Proof

Since we defined ElGamal encryption scheme on the DDH problem, for the scheme to be CPA secure, the DDH problem must be a mathematically hard problem to solve relative to the algorithm $\mathcal{G}$ considered. Let Π denote the ElGamal encryption scheme. To prove that Π is CPA secure, i.e., the encrypted messages are indistinguishable even with an eavesdropping PPT Adversary A, then we must show that there exists a negligible function $negl(n)$ such that:

$$Pr[PubK^{eav}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$

where $PubK^{eav}_{A,\Pi}(n)$ is the indistinguishability experiment under eavsdropper.

Proof: Let us consider a modified encryption scheme $\hat{\Pi}$ which has the same GEN algorithm as in Π, and differs in terms of ENC of a message m with respect to the public key $pk = (\mathbb{G}, q, g, h)$. Encryption is done by selecting uniformly random $y, z \in \mathbb{Z}_q$, and outputting the ciphertext:

$$(g^y, g^z \cdot m)$$

Now, in the above ciphertext, the second part in scheme $\hat{\Pi}$ is a uniformly distributed group element and is independent of the message being encrypted. The first component of ciphertext is trivially independent of the message as well. Considering the whole ciphertext, no part of it contains any information on the message m. Thus:

$$Pr[PubK^{eav}_{A,\hat{\Pi}}(n) = 1] = \frac{1}{2}$$

Consider a PPT algorithm D that tries to distinguish and solve the DDH problem relative to $\mathcal{G}$. Algorithm D receives $(\mathbb{G}, q, g, h_1, h_2, h_3)$, where $h_1 = g^x, h_2 = g^y, h_3 =$ either g^{xy} or g^z. D must distinguish h_3 to be either g^z or g^{xy} for uniformly random x, y, z.

Algorithm D:

1. Set the public key $pk = (\mathbb{G}, q, g, h)$ and give it to the adversary A to obtain two messages $m_0, m_1 \in \mathbb{G}$.
2. Choose uniform bit b, and set $c_1 = h_2, c_2 = h_3 \cdot m_b$.
3. Give the ciphertext (c_1, c_2) to A and obtain output bit b'. If $b' = b$, output 1; else output 0.

Analysis: There are now two cases to be considered:

Case 1: Suppose the input to D is given as $h_1 = g^x, h_2 = g^y, h_3 = g^z$. then D uses a public key that is constructed as follows

$$pk = (\mathbb{G}, q, g, g^x)$$

The resultant ciphertext is

$$(c_1, c_2) = (g^y, g^z \cdot m_b)$$

This is distributed identically to the adversary's view in $PubK^{eav}_{A,\hat{\Pi}}(n)$. Since D outputs 1 when $b' = b$, we get

$$Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] = Pr[PubK^{eav}_{A,\hat{\Pi}}(n) = 1] = \frac{1}{2}$$

Case 2: Suppose the input to D is given as $h_1 = g^x, h_2 = g^y, h_3 = g^{xy}$. then D uses a public key that is constructed as follows

$$pk = (\mathbb{G}, q, g, g^{xy}) = (\mathbb{G}, q, g, h^y)$$

The resultant ciphertext is

$$(c_1, c_2) = (g^y, g^{xy} \cdot m_b)$$

This is distributed identically to the adversary's view in $PubK^{eav}_{A,\Pi}(n)$. Since D outputs 1 when $b' = b$, we get

$$Pr[D(G, q, g, g^x, g^y, g^{xy}) = 1] = Pr[PubK^{eav}_{A,\Pi}(n) = 1]$$

Now assuming that the DDH problem is hard relative to $\mathcal{G}$, consider a negligible function $negl(n)$ such that

$$\begin{aligned} negl(n) &\geq |Pr[D(G, q, g, g^x, g^y, g^z) = 1] - Pr[D(G, q, g, g^x, g^y, g^{xy}) = 1]| \\ &= |\frac{1}{2} - Pr[PubK^{eav}_{A,\Pi}(n) = 1]| \end{aligned}$$

Hence this proves the security of this scheme with the resulting:

$$Pr[PubK^{eav}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$