Notes on threshold Diffie-Hellman cryptosystem

Ganyu Xu[1]

University of Waterloo, Ontario, Canada
g66xu@uwaterloo.ca

1 TDH0a: naive threshold Diffie-Hellman cryptosystem

1.1 Review: a hybrid ElGamal cryptosystem

Let (G, g) be a cyclic group of prime order q. Let (E, D) be a symmetric cipher with key space $\mathcal{K}$. Let $H_{\mathcal{K}} : G \to \mathcal{K}$ be a hash function. Consider the following ElGamal-like hybrid public-key encryption scheme, which we denote by `ElGamal`:

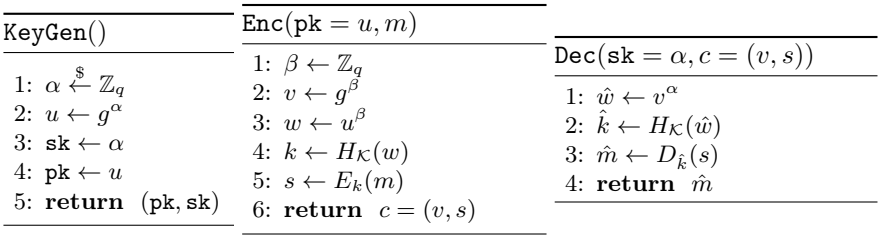

Fig. 1: ElGamal hybrid public-key encryption scheme

Under the random oracle model (ROM), if the interactive computational Diffie-Hellman (ICDH) problem is intractable for the cyclic group G, then this hybrid ElGamal cryptosystem is secure against chosen ciphertext attacks. For a sketch of proof, we try to construct an ICDH adversary $\mathcal{B}$ using a CCA adversary $\mathcal{A}$. From the definition of ICDH problem, we know $\mathcal{B}$ is given an instance of a CDH problem $(u^*, v^*) \in G \times G$ and access to a DDH oracle $\mathcal{O}^{\mathsf{DDH}} : (u, v, w) \mapsto \{\mathtt{accept}, \mathtt{reject}\}$ where the oracle outputs `accept` if and only if (u, v, w) is a Diffie-Hellman triple. $\mathcal{B}$ needs to simulate the CCA game for $\mathcal{A}$ using the following strategy:

- $\mathcal{B}$ gives u^* to $\mathcal{A}$ as the public key
- $\mathcal{B}$ needs to answer an encryption query from $\mathcal{A}$. When $\mathcal{A}$ outputs the pair of plaintext (m_0, m_1) to $\mathcal{B}$, $\mathcal{B}$ flips a coin $b \xleftarrow{\$} \{0, 1\}$ to pick the plaintext m_b to encrypt. However, instead of running the encryption routine, $\mathcal{B}$ directly uses v^* from the CDH problem and uses a randomly sampled symmetric key k^* to encrypt m_b: $s^* \xleftarrow{\$} E(k^*, m_b)$. $\mathcal{B}$ gives $c^* = (v^*, s^*)$ to $\mathcal{A}$ as the challenge ciphertext.

- $\mathcal{B}$ simulates the random oracle $H_{\mathcal{K}}$ for $\mathcal{A}$
- $\mathcal{B}$ simulates the decryption oracle $\mathcal{O}^{\mathsf{Dec}}$ for $\mathcal{A}$. On decryption query $\tilde{c} = (\tilde{v}, \tilde{s})$, $\mathcal{B}$ searches through the tape of $H_{\mathcal{K}}$ for $(\tilde{w}, \tilde{k}) \in \mathcal{L}^{H_{\mathcal{K}}}$ such that $\mathcal{O}^{\mathsf{DDH}}(u^*, \tilde{v}, \tilde{w}) = \texttt{accept}$. If true, then $\mathcal{B}$ decrypts $\tilde{s}$ using $\tilde{k}$, otherwise $\mathcal{B}$ decrypts $\tilde{s}$ using a randomly sampled key $\tilde{k} \xleftarrow{\$} \mathcal{K}$ and patch $H_{\mathcal{K}}$ with input-output pair $(\tilde{w}, \tilde{k})$

We can argue that the simulated game is indistinguishable to $\mathcal{A}$, except for when $\mathcal{A}$ queries $H_{\mathcal{K}}$ with w^* where (u^*, v^*, w^*) is a Diffie-Hellman triple. Because $\mathcal{B}$ has access to a DDH oracle, when this event happens, $\mathcal{B}$ wins its CDH game immediately. All of above is captured in the theorem below:

Theorem 1. *Under ROM, if ICDH is intractable for the group G and if the symmetric cipher is semantically secure, then hybrid ElGamal is CCA secure.*

1.2 Shamir's secret sharing

We can apply Shamir's secret sharing scheme to convert this into a threshold scheme, which we will denote by `TDH0a`. t, n are the threshold parameters: there are n decryption servers and t or more are needed to decrypt a ciphertext.

Algorithm 1 `TDH0a.KeyGen`(t, n)

1: $\alpha_0, \ldots, \alpha_{t-1} \leftarrow \mathbb{Z}_q$
2: $f(x) \leftarrow \alpha_{t-1} x^{t-1} + \ldots + \alpha_1 x + \alpha_0$
3: **for** $i \in \{1, 2, \ldots, n\}$ **do**
4: $\quad \mathtt{sk}_i \leftarrow f(i)$
5: **end for**
6: $\mathtt{pk} \leftarrow g^{f(0)}$ (equal to g^{α_0})
7: **return** $(\mathtt{pk}, \{\mathtt{sk}_i\}_{i=1}^n)$

1.3 The TDH0a cryptosystem

1.4 The TDH0b cryptosystem

2 TDH1

3 TDH2

3.1 Pedersen-Chaum ZKP

3.2 TDH2