Sécurité prouvable
TD LoR, RoR, malleability

Exercice I

Une forme très utilisée de la sécurité IND-CPA figure un jeu légèrement modifié par rapport à la définition que nous avons utilisé en cours (la notion qu'on avait vue s'appelle Left-or-Right (LoR) Indistinguishability, car l'adversaire doit distinguer entre un chiffrement du message à gauche ou le message à droite).

Nous allons à présent voir une autre notion, notamment Real-or-Random Indistinguishability (RoR), qui est identique au jeu LoR, sauf que, au lieu d'envoyer deux messages d'une taille pareille au challenger, l'attaquant n'envoie qu'un. Si le bit secret du challenger est 0, alors ce dernier chiffre le message envoyé par l'attaquant. Si le bit secret est 1, alors le challenger choisit un message aléatoire de l'espace de messages possibles M, et le chiffre. Le texte chiffré obtenu (soit du vrai message, soit du message aléatoire) est envoyé à l'attaquant (comme dans le jeu LoR).

1. Ecrivez en forme de jeu de sécurité la notion RoR IND-CPA.
2. Comment va-t-on définir l'avantage de l'adversaire dans ce cas-ci ?
3. Pouvez-vous définir quand un schéma est RoR-IND-CPA secure ?

Maintenant nous allons trouver les relations entre la sécurité LoR IND-CPA et celle RoR IND-CPA.

4. Supposez qu'il existe un adversaire A qui a un avantage non-négligeable de gagner le jeu RoR IND-CPA. Montrez comment une réduction R (prenant en entrée l'adversaire A à boîte noire) peut alors gagner le jeu LoR IND-CPA avec un avantage non-négligeable.
5. Qu'avez-vous prouvé sur les notions RoR et LoR IND-CPA avec la preuve de la question 4 ?
6. Maintenant supposez qu'il existe un adversaire A qui a un avantage non-négligeable de gagner le jeu LoR IND-CPA. Pouvez-vous trouver une réduction R qui gagne au jeu RoR IND-CPA avec une probabilité non-négligeable ? (suivez les étapes ci-dessous)
    a. Quelle est la différence principale entre les deux jeux ? Quelle est la difficulté qu'elle produit pour la réduction ?
    b. Rappelez-vous de votre preuve pour le chiffrement ElGamal. Comment avez-vous résolu la difficulté similaire ?
    c. Faites la réduction et calculez la probabilité de gagner de la réduction en fonction de la probabilité de gagner de l'adversaire A.

Exercice II

Faites une réduction qui montre que le chiffrement ElGamal est RoR IND-CPA si l'hypothèse DDH est difficile.

Exercice III

Imaginez-vous un protocole d'authentification pour un serveur, qui est en possession d'une paire de clés (sk, pk) pour le chiffrement ElGamal (ces clés sont certifiées !).

Le client veut authentifier le serveur. Il commence le protocole en choisissant un nombre aléatoire r, tiré uniformément et indépendamment d'un espace très large (disons $\{0,1\}^{512}$). Le client chiffre r avec la clé publique du serveur et lui envoie le texte chiffré obtenu.

Le serveur doit déchiffrer le texte chiffré obtenu et ensuite envoyer au client la valeur r.

1. Faites un schéma de ce protocole
2. Qu'est-ce qui se passe lorsqu'un attaquant envoie des valeurs arbitraires au serveur ?
3. ElGamal est sécurisé contre les attaques IND-CPA. Quelles informations un attaquant a-t-il dans un jeu IND-CPA ? Est-ce qu'un attaquant contre notre protocole d'authentification a plus, moins ou autant d'informations sur le chiffrement ElGamal que l'adversaire IND-CPA ?
4. Disons qu'on a un texte chiffré ElGamal : $(C_1 = g^r, C_2 = M \cdot pk^r)$. Comment un adversaire ne connaissant pas le message M peut-il obtenir un texte chiffré $(\widetilde{C_1}, \widetilde{C_2})$ qui rendra (en le déchiffrant) le même message M ?
5. Utilisez cette attaque de rerandomisation pour obtenir une attaque contre le protocole d'authentification.
6. Quelle propriété serait nécessaire pour obtenir la sécurité du schéma ?