Sylvan LE DEUNFF, ENSSAT, IMR3

Canaux de diffusion anonymes

1. Un canal de diffusion anonyme est une primitive qui peut être utilisée comme brique de base pour réaliser de nombreuses tâches. Imaginer deux autres applications possibles du canal de diffusion anonyme et décrivez les chacune en quelques phrases.

Vote électronique: Ici c'est l'identité de l'émetteur qui est protégée. L'autorité qui est responsable de l'élection ne doit pas apprendre les votes individuels des électeurs.

Crypto-monnaie: La divulgation d'une transaction entre un acheteur et un vendeur est une violation de la vie privée de l'acheteur. Une blockchain anonymisée (comme celle utilisée par Monero) permet la protection de cette information.

2. Argumenter sur le fait que suite au protocole décrit dans la deuxième partie, Alice et Bob se retrouvent en possession d'un secret sur lequel l'adversaire n'a aucune information. Pourquoi est ce le cas ?

La primitive d'échange de clé repose sur le fait de pouvoir connaitre l'émetteur des bits échangés. Or dans ce protocole seul les 2 interlocuteurs ont cette capacité :

- l'émetteur d'un message sait qu'il l'a émis.
- le récepteur sait qu'il ne l'a pas émis.

Tous les autres observateurs (y compris l'espion) n'ont aucun moyen de déterminer la source du message. Et par conséquent ne peuvent déterminer quel bit (b) est associé au message i.

3. Expliquer en quelques mots pourquoi il est important d'avoir des primitives permettant à deux entités de générer un secret commun à travers un canal de communication qui est potentiellement surveillé par un espion.

Sur un canal de communication anonyme, il est intéressant de protéger ses communications en les chiffrant. Pour cela on peut choisir d'utiliser un chiffrement symétrique, 2 interlocuteurs doivent alors convenir d'un secret commun.

Problème: Si un espion est en mesure d'intercepter le secret commun, il pourra déchiffrer notre communication. Il est donc impératif de définir des primitives, qui permettent de générer un secret :

- qui sera connu des deux interlocuteurs.
- qu'aucun espion ne pourra reconstituer simplement en écoutant sur le canal.