Sécurité des communications informatiques
TD#4

2024–02–16

Exercice 1 (Preuve à divulgation nulle de connaissance & spéléologie) :

Q.1 : Soit le dessin au tableau, expliquez :

1. Comment $\mathscr{A}$ peut convaincre $\mathscr{B}$ de la connaissance de la phrase magique.
2. Comment $\mathscr{B}$ ne peut pas convaincre $\mathscr{C}$ que $\mathscr{A}$ connaît la phrase magique.
3. Pourquoi on peut déduire de cela que $\mathscr{A}$ n'a révélé aucune « information » à $\mathscr{B}$ sur la phrase magique elle-même.

Référence : https://doi.org/10.1007/0-387-34805-0_60

Exercice 2 : Protocole de preuve d'identité

On considère un groupe cyclique $\mathbb{G} = \langle g \rangle$ d'ordre premier p. Un prouveur $\mathscr{A}$ souhaite montrer à un vérifieur $\mathscr{B}$ qu'il connaît un entier x tel que $g^x =: X \in \mathbb{G}$. Il utilise pour cela le protocole suivant :

1. $\mathscr{A}$ choisit $r \twoheadleftarrow [\![0, p-1]\!]$ et envoie $R := g^r$ à $\mathscr{B}$
2. $\mathscr{B}$ choisit un *challenge* $c \twoheadleftarrow [\![0, p-1]\!]$ et l'envoie à $\mathscr{A}$
3. $\mathscr{A}$ calcule $a := r + cx \ \% \ p$ et l'envoie à $\mathscr{B}$
4. $\mathscr{B}$ calcule g^a et accepte la preuve ssi. $g^a = RX^c$

Q.1 :

1. Montrer que si $\mathscr{A}$ connaît x, il peut toujours construire une preuve acceptée par $\mathscr{B}$.

Q.2 :

1. Pourquoi est-ce important pour un prouveur honnête de choisir r uniformément ? (Et quelle attaque (permettant par exemple d'apprendre de l'information sur x) pourrait-on réaliser si ce n'était pas le cas (par exemple si l'adversaire peut deviner la valeur de r avec une forte probabilité) ?)

Q.3 :

1. Pourquoi est-ce important d'utiliser des valeurs distinctes de r pour chaque exécution du protocole ? (Et quelle attaque pourrait-on réaliser dans le cas contraire ?)

Q.4 :

1. Montrez qu'en choisissant R et c lui-même, $\mathscr{B}$ peut créer un transcript du protocole indistinguable (c-à-d suivant la même distribution) qu'un transcript produit grâce à une interaction avec $\mathscr{A}$.

   INDICE : Faites d'abord choisir c et a par $\mathscr{B}$, puis calculez R.

2. Déduisez-en qu'*un* transcript du protocole n'apporte aucune information sur x.

3. Y a-t'il néanmoins une limite sur le nombre de transcripts pouvant être produits sans donner d'information sur x (avec forte probabilité) ?