Sécurité des communications informatiques
TD#3

2024–02–09

Exercice 1 (tentatives de chiffrement authentifié) :

On considère un système de chiffrement symétrique Enc et un MAC *déterministe* M (qui à une clef et un message (k, m) fixés associe toujours le même tag t).

Q.1 :

1. Montrez que $\mathsf{Enc} + \mathsf{M} : (k', k, m) \mapsto \mathsf{Enc}(k', m) \| \mathsf{M}(k, m)$ est vulnérable à une attaque IND-CPA, *quelque soit* la sécurité IND-CPA de Enc.
2. Proposez une façon alternative de combiner Enc avec un MAC afin d'obtenir un chiffrement IND-CPA « authentifié », et justifiez informellement sa sécurité IND-CPA et sa résistance aux forgeries.

Exercice 2 (définitions de sécurité pour MACs) :

On considère à nouveau un MAC déterministe M.

Q.1 : Supposez que vous connaissez un algorithme A^{u}_{M} permettant de gagner le jeu de forgerie universelle pour M avec probabilité p^{u}_{M} ; on note t^{u}_{M} son temps de calcul et q^{u}_{M} le nombre requêtes qu'il fait à son oracle.

1. Spécifiez un algorithme A^E_M de forgerie existentielle pour M, qui utilise A^U_M en boîte noire.
2. Donnez le coût t^E_M et q^E_M de A^E_M ainsi que sa probabilité de succès p^E_M.

Q.2 : On suppose l'existence de A^E_M comme ci-dessus.

1. Spécifiez un adversaire PRF pour M qui utilise A^E_M en boîte noire, tourne en temps $t^F_M \approx t^E_M$ et fait $q^F_M \approx q^E_M$ requêtes à son oracle.
2. Déduisez-en un minorant pour $\mathbf{Adv}^{\mathrm{PRF}}_M(q^F, t^F)$.
3. Le scénario informel suivant est-il possible : « M est vulnérable à une attaque en forgerie existentielle, mais est difficile à distinguer d'une fonction aléatoire » ?

Q.3 :

1. Supposez qu'on puisse magiquement vous fournir un MAC M avec la garantie qu'il satisfasse l'*une* des trois hypothèses (informelles) suivantes :
   — M est une bonne PRF
   — M est résistant aux forgeries existentielles
   — M est résistant aux forgeries universelles
   Laquelle choisiriez-vous, et pourquoi ?

Exercice 3 (anniversaires et suite aléatoire) :

Soit $\mathcal{S}$ un ensemble arbitraire[1] de taille N et $(u_n)_{n\in\mathbb{N}}$ une suite dont les éléments sont tirés uniformément et indépendamment dans $\mathcal{S}$ (autrement dit pour tout i, $u_i \twoheadleftarrow \mathcal{S}$). Supposez que $\mathcal{S}$ et N sont initialement inconnus.

1. Donnez un algorithme qui examine $\Theta(\sqrt{N})$ termes de (u_n) et renvoie une approximation de N (on ne demande pas de quantifier la qualité de cette approximation).
2. Évaluez le coût en temps et en mémoire de votre algorithme (prenez garde à bien spécifier les éventuelles structures de données que celui-ci utilise).

1. En particulier, les éléments de $\mathcal{S}$ ne sont pas forcément des nombres. Par exemple, $\mathcal{S}$ pourrait être égal à $\{$*martes martes*, *martes foina*, *martes zibellina*$\}$.