Principe et Algorithme Cryptographiques : examen

première session / documents et calculatrice autorisés / durée 2h / 4 pages

22 mai 2018

Ce sujet est composé de 4 pages. Vos réponses doivent **absolument** être justifiées. Le sujet est constitué d'un seul problème et certaines questions s'enchainent, mais pas toutes. Les différentes sections contiennent des questions de difficultés variés (certaines sont de simples questions de cours). La plupart des questions admettent des réponses assez courtes, mais n'oubliez pas de les justifier — vous avez été prévenu(e). Le sujet est probablement trop long, mais ce n'est pas grave de ne pas aller jusqu'au bout.

Votre progression dans le TP sera relevée une dernière le vendredi 1er juin à 23 :59. Un rendu sur PROF sera demandé. Plus de précisions dans un email à venir.

On rappelle que la notation $\{m\}_k$ désigne (comme dans le cours) le chiffrement du message m avec la clef k. Ceci peut faire référence à un chiffrement symétrique (auquel cas k est la clef symétrique) ou bien à un chiffrement asymétrique (auquel cas k est la clef publique du destinataire).

Échange équitable et transfert inconscient de secrets

1 Introduction

On s'intéresse à un scénario ou Alice et Bob, deux journalistes d'investigation, possèdent des informations confidentielles et souhaitent se les échanger. Par exemple, Alice possède un secret s_a (révélation sur des comportement sexuellements déviants d'un certain chef d'État), tandis que Bob possède s_b (état d'avancement du programme extra-légal de développement de drones tueurs autonomes par un certain autre état). Bien sûr, ils aimeraient bien avoir le beurre et l'argent du beurre : obtenir le scoop de l'autre sans rien révéler en échange.

Du coup, on souhaite construire un protocole *équitable* : si Alice apprend bien le secret de Bob, alors Bob apprend bien le secret d'Alice (et vice-versa). Même si Alice et Bob se lancent dans l'exécution d'un tel protocole, aucun mécanisme cryptographique ne semble à même de garantir que les chaines de bits s_a et s_b qui vont être échangées possèdent vraiment une nature « sensible » (et intéressante d'un point de vue journalistique). On va donc supposer que c'est bien le cas, et que ni Alice ni Bob n'essayent directement de tricher en remplaçant leur secret par une chaine de bits aléatoire (on admettra que les conséquences, par exemple la ruine de sa réputation professionnelle, seraient trop grave pour tenter le coup).

Alice et Bob ne se sont jamais rencontrés et communiquent uniquement par internet. Pour commencer, on suppose qu'ils possèdent tous les deux la clef publique de l'autre. On considère dans un premier temps le protocole le plus simple possible pour qu'Alice et Bob échangent leur secret respectif.

Protocole E (*Échange de secrets*). Alice et Bob envoient simplement leur secret, chiffré, l'un après l'autre.

E1. [A révèle son secret.] Alice envoie $\{s_a\}_{pk_b}$ à Bob.

E2. [B révèle son secret.] Bob envoie $\{s_b\}_{pk_a}$ à Alice.

▷ **Question 1 :** Expliquer en une phrase quel genre de mécanisme Alice et Bob peuvent utiliser, préalablement à l'exécution du protocole, pour être sûrs d'avoir la bonne clef publique de l'autre.

▷ **Question 2 :** Dans le protocole E, si Alice entreprenait de tricher de manière grossière en envoyant du charabia pseudo-aléatoire à la place de son « vrai » secret, que se passerait-il ?

▷ **Question 3 :** Si jamais le lien réseau entre Alice est Bob était rompu après l'étape E1 mais avant l'étape E2, que se passerait-t-il ? Bob aurait-il intérêt à provoquer cet évènement ?

2 Échange équitable de secrets

Le problème du protocole E c'est qu'il n'est pas équitable : il favorise Bob. Un échange équitable de secret doit placer les deux participants à égalité : à n'importe quel moment du protocole, il faut que les deux participants aient appris autant d'information sur le secret de l'autre. Par conséquent, si l'un des deux est coupé d'internet,

décide de se retirer ou de se mettre à répondre n'importe quoi, alors il ne pourra pas en obtenir un avantage. Une approche naïve consiste à utiliser un protocole où les secrets sont transmis « progressivement ».

Protocole P (*Échange de secrets progressif*). Alice et Bob chiffrent leurs messages avec des clefs de session jetables de n bits, puis s'échangent les clefs un bit après l'autre.

P1. [A met son secret en gage.] Alice génère une clef de session K_a puis envoie $\{\{s_a\}_{pk_b}\}_{K_a}$ à Bob.

P2. [B met son secret en gage.] Bob génère une clef de session K_b puis envoie $\{\{s_b\}_{pk_a}\}_{K_b}$ à Alice.

P3. [Échange des clefs.] Pour chaque $1 \leq j \leq n$:
Alice envoie à Bob le j-ème bit de K_a.
Bob envoie à Alice le j-ème bit de K_b.

▷ **Question 4 :** Le chiffrement « externe » (avec les clefs de session) est-il symétrique ou asymétrique ?

▷ **Question 5 :** En 2018, quelle taille de clefs de session (n) semble raisonnable ?

▷ **Question 6 :** Pourquoi a-t-on tenu à conserver le chiffrement asymétrique ?

▷ **Question 7 :** Que se passe-t-il si l'un des deux (disons Bob) décide d'interrompre le protocole au milieu de l'étape P3 ? Ceci entraine-t-il une rupture d'équité ?

▷ **Question 8 :** Que se passe-t-il si Alice décide de tricher en répondant n'importe quoi lors de l'étape P3 ? Bob, qui lui exécute le protocole honnêtement, peut-il le détecter avant la fin ?

La suite du sujet propose une manière de réparer ce protocole, ce qui n'est pas trivial.

3 Transfert inconscient

Le « (1-2) transfert inconscient » (*oblivious transfer*) est un mécanisme cryptographique où Alice possède deux secrets s_0, s_1, et où l'un de ces secrets est communiqué à Bob. Alice souhaite que Bob apprenne *un seul* de ses petits secrets. Bob lui ne souhaite pas qu'Alice sache *lequel* il souhaite recevoir. Cette section est consacrée à un protocole dû à Vanessa Vitse (*univ. Grenoble-Alpes*), mais non-publié à ce jour.

Protocole OT (*Transfert Inconscient*). Bob possède un bit secret i. Le but du protocole est qu'Alice « transfère » s_i à Bob, sans lui révéler l'autre secret s_{1-i} et sans qu'Alice apprenne i (c'est ça le côté « inconscient »). Le protocole fonctionne dans un groupe avec un générateur g modulo p. L'ordre du générateur est un nombre premier q. La description du groupe (p, g, q) est publique.

OT1. [Mise en gage.] Alice choisit aléatoirement deux nombres a_0 et a_1, puis transmet g^{a_0} et g^{a_1} à Bob.

OT2. [Masquage.] Bob pose $x \leftarrow g^{a_i}$, choisit un nombre aléatoire b, calcule $y \leftarrow x^b$ et enfin envoie y à Alice.

OT3. [Envoi chiffré.] Alice calcule $k_0 \leftarrow y^{(a_0^{-1})}$ et $k_1 \leftarrow y^{(a_1^{-1})}$ puis envoie $\{s_0\}_{k_0}$ et $\{s_1\}_{k_1}$ à Bob.

Préliminaires On se penche d'abord sur la tailles des données manipulées pendant le protocole.

▷ **Question 9 :** La sécurité de ce protocole repose implicitement sur le fait qu'un problème calculatoire classique de la cryptographie à clef publique est difficile. Lequel ?

▷ **Question 10 :** Quelle taille (en bits) doit avoir p pour offrir une bonne sécurité, en 2018 ?

▷ **Question 11 :** Quelle devrait, idéalement, être la taille de q ?

Annotations implicites Comme dans le cours, la description du protocole omet de signaler les opérations « modulo » qui ont pourtant lieu dans chacune des trois étapes. Il s'agit ici de préciser les choses.

▷ **Question 12 :** Dans l'étape OT1, Alice effectue deux exponentiations modulaires. Quel est le modulus [1] ?

▷ **Question 13 :** Dans l'étape OT3, indiquer le modulus utilisé : a) pour les deux inversions modulaires et b) pour les deux exponentiations.

▷ **Question 14 :** Dans quel intervalle est-ce qu'Alice et Bob doivent choisir les nombres a_0, a_1 et b ?

1. Rappel : quand on fait des calculs « modulo n », le modulus est n.

Un détail manquant Dans l'étape OT3, Alice calcule des clefs puis effectue un chiffrement. Le texte ne dit pas s'il s'agit-il d'un mécanisme de chiffrement symétrique ou asymétrique... mais on peut, par le raisonnement, s'y retrouver quand même.

▷ **Question 15 :** Expliquer pourquoi, dans une exécution honnête du protocole, les deux clefs k_0, k_1 sont des nombres aléatoires.

▷ **Question 16 :** Dans les mécanismes de chiffrement à clef publique vus en cours, la clef publique est calculée à partir de la clef privée. Pourrait-il être possible de faire l'inverse, c'est-à-dire de calculer la clef privée à partir de la clef publique ?

▷ **Question 17 :** Expliquer pourquoi (vu la réponse à la question précédente) le mécanisme de chiffrement utilisé à l'étape OT3 est forcément un mécanisme de chiffrement *symétrique*.

Sécurité et correction du protocole On se penche maintenant sur les caractéristiques fonctionnelles du protocole.

▷ **Question 18 :** Que se passerait-il si Alice choisissait $a_i = 0$ dans l'étape OT1 ? Quel intérêt Alice aurait-elle à vouloir faire ceci ? Bob peut-il le détecter et l'empêcher efficacement ?

▷ **Question 19 :** Même question avec $b = 0$.

▷ **Question 20 :** Expliquer pourquoi est-ce qu'Alice n'apprend pas i (le choix de Bob) à l'issue de l'étape OT2, et ceci quelle que soit la puissance de calcul dont elle dispose.

▷ **Question 21 :** Expliquer ce que Bob doit faire pour récupérer s_i (et donc réaliser concrètement le « transfert »).

▷ **Question 22 :** Expliquer informellement pourquoi Bob n'apprend pas s_{1-i}.

▷ **Question 23 :** Indiquer de quelle(s) manière(s) le protocole échouerait si jamais un algorithme très efficace pour résoudre le problème calculatoire difficile sous-jascent venait à être découvert.

4 Échange équitable de paires de secrets

Armés d'un protocole de transfert inconscient, on av pouvoir résoudre le problème de l'échange équitabel de secrets, mais avant cela, il nous faut passer par une étape intermédiaire : l'échange de *paires secrètes*. On va noter $\texttt{OT}(A, B, x, y)$ pour dénoter un protocole de transfert inconscient (par exemple celui de la section précédente), où A transfère à B l'un de ses deux secrets x et y. Cette section est consacrée au protocole suivant :

Protocole PE (*Échange équitable de paires*). Alice et Bob possèdent tous les deux n *paires* de chaines de bits secrètes, toutes de la même taille ℓ. Alice possède $(u_i, v_i)_{1 \leq i \leq n}$ tandis que Bob possède $(x_i, y_i)_{1 \leq i \leq n}$. Le but du protocole est de s'échanger les paires équitablement.

PE1. [Transfert inconscient.] Alice effectue le transfert inconscient $\texttt{OT}(A, B, u_i, v_i)$ pour $1 \leq i \leq n$.
Bob effectue le transfert inconscient $\texttt{OT}(B, A, x_i, y_i)$ pour $1 \leq i \leq n$.
Dans les deux cas, le « receveur » choisit aléatoirement s'il veut recevoir le premier ou le deuxième élément de la paire.

PE2. [Transmission progressive.] Pour chaque $1 \leq j \leq \ell$:
Alice envoie à Bob le j-ème bit de u_i et v_i (pour tout $1 \leq i \leq n$).
Bob envoie à Alice le j-ème bit de x_i et y_i (pour tout $1 \leq i \leq n$).

▷ **Question 24 :** Justifier qu'à la fin d'une exécution (honnête) du protocole, les paires ont bien été échangées (Alice connaît les paires de Bob et réciproquement).

▷ **Question 25 :** Que va-t-il se passer si Alice ou Bob répond n'importe quoi à un moment dans l'étape PE2 ? L'autre peut-il le détecter ? Quel rôle joue le nombre n de paires dans le processus ?

5 Un protocole d'échange de secrets équitable

On est finalement en mesure de réparer le protocole PE de l'introduction.

Protocole P' (*Échange de secrets équitable*). Alice et Bob chiffrent leurs messages avec des clefs de session de n bits, puis s'échangent les clefs de manière équitable grace au protcole d'échange équitable de paires.

P'1.[A met son secret en gage.] Alice génère une clef de session aléatoire K_a puis envoie $\{\{s_a\}_{pk_b}\}_{K_a}$ à Bob.

P'2.[B met son secret en gage.] Bob génère une clef de session aléatoire K_b puis envoie $\{\{s_b\}_{pk_a}\}_{K_b}$ à Alice.

P'3.[Échange équitable des clefs.] Alice génère n paires (u_i, v_i) en choisissant u_i aléatoirement et en posant $v_i \leftarrow K_a \oplus u_i$.
Bob génère également n paires (x_i, y_i), où x_i est aléatoire et $y_i \leftarrow K_b \oplus x_i$.
Finalement, Alice et Bob exécutent le protocole PE de la section précédente pour s'échanger équitablement leurs paires respectives.

▷ **Question 26 :** En supposant que les participants exécutent le protocole honnêtement, comment font-ils pour obtenir leurs secrets respectifs ?

▷ **Question 27 :** Si le protocole est interrompu avant le début de l'étape P'3, un des deux participants est-il avantagé ?

▷ **Question 28 :** Supposons que l'un des deux participants décide de tout arrêter après l'étape PE1 du sous-protocole d'échange équitable des paires. Peut-il récupérer le secret de l'autre ?

▷ **Question 29 :** Alice peut toujours décider d'interrompre le protocole au milieu de l'étape PE2 de l'échange de paires. Si elle dispose d'une grande puissance de calcul, comment peut-elle essayer d'apprendre le secret de Bob malgré tout ?

Ceci, par contre, est quasiment inévitable.