Université Paris 8 — Année 2023–24 — J. Lavauzelle

Master 1 Mathématiques et applications

Cryptographie à clé publique – Solutions feuille de TD 7

11/03/2024

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`https://lvzl.fr/teaching/2023-24/cp.html`

($\star$) exercice fondamental ($\star\star$) pour s'entraîner ($\star\star\star$) pour aller plus loin 💻 sur machine

---

Exercice 1. ($\star$) Un nouveau protocole d'identification ?.

Alice souhaite s'identifier auprès de Bob. On suppose qu'Alice et Bob détiennent un secret commun $x \in \{0,1\}^t$, pour $t \geq 1$, qui doit servir à plusieurs identifications. Le protocole suivant est proposé :

1. Bob choisit une chaîne aléatoire $r \in \{0,1\}^t$ et l'envoie à Alice
2. Alice calcule $y = r \oplus x$ et renvoie y à Bob.
3. Bob vérifie que $x = r \oplus y$.

Question 1.– Pourquoi ce protocole ne peut pas être utilisé pour plusieurs identifications ?

Question 2.– Quelle étape d'un protocole d'identification à trois passes manque t-il dans ce protocole ?

Solutions de l'Exercice 1.

Solution Q1. En observant les valeurs transmises entre Alice et Bob, un attaquant peut retrouver le secret x en effectuant le `xor` du défi r et de $y = r \oplus x$.

Solution Q2. Il manque l'étape d'engagement, dans laquelle Alice publie une valeur v liée à son secret, mais qui ne le révèle pas. Du fait de l'absence de cette étape, Alice est forcée de retourner une valeur y, qui couplée avec le défi r, révèle le secret r.

Exercice 2. ($\star\star$) Schéma d'identification de Feige–Fiat–Shamir.

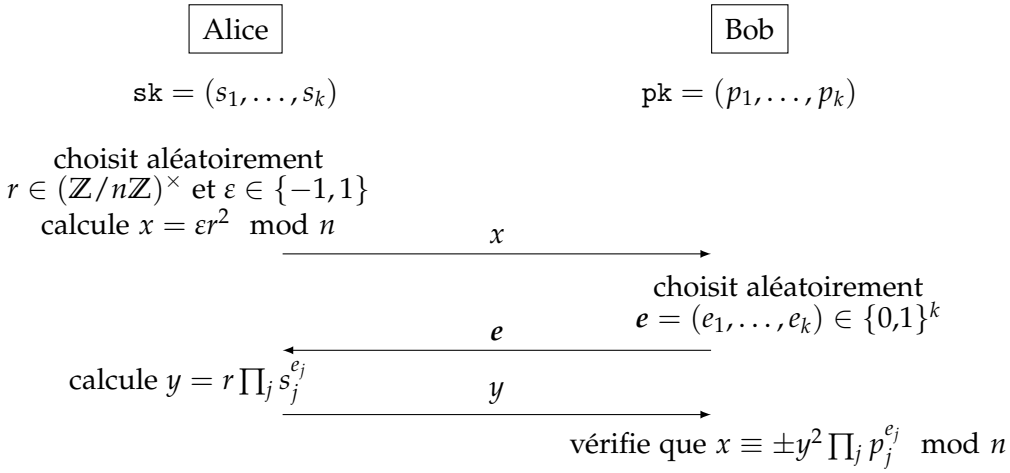
Dans cet exercice, on s'intéresse au schéma d'identification de Feige-Fiat-Shamir.

Dans le réseau de participants, une autorité de confiance choisit secrètement p et q deux grands nombres premiers, puis calcule et publie $n = pq$. On fixe ensuite k un entier, typiquement de taille $\log_2 \log_2 n$.

Alice, une utilisatrice du réseau, procède comme suit pour engendrer une paire de clefs :

1. Alice choisit aléatoirement $s_1, \ldots, s_k \in (\mathbb{Z}/n\mathbb{Z})^\times$.
2. Pour tout $j = 1, \ldots, k$, Alice choisit $\varepsilon_j \in \{-1, 1\}$ aléatoirement, puis calcule $p_j = \varepsilon_j / s_j^2$.
3. La clé publique d'Alice est $\mathtt{pk} = (p_1, \ldots, p_k)$, la clé privée d'Alice est $\mathtt{sk} = (s_1, \ldots, s_k)$.

Le protocole d'identification se déroule ainsi :



Question 1.– Démontrer que le protocole d'identification est valide.

Question 2.– Démontrer que, si un attaquant connaît le défi $\boldsymbol{e}$ de Bob **avant** de réaliser son engagement x, alors il peut monter une imposture. En déduire qu'il existe une attaque sur le système qui réussit avec probabilité 2^{-k}.

Question 3.– Selon vous, sur quel problème (difficile) repose la sécurité du schéma ? Donner une justification succincte.

Dans les questions suivantes, on cherche à démontrer que le protocole d'identification de Feige-Fiat-Shamir est une **preuve de connaissance à divulgation nulle**. Autrement dit, les itérations du protocole ne révèlent aucune information sur le secret $\mathtt{sk}$ d'Alice.

Pour obtenir cette propriété, l'idée est de démontrer que l'on peut simuler la distribution du transcript $(x, \boldsymbol{e}, y)$ sans la connaissance de $\mathtt{sk}$.

Question 4.– On suppose que tous les tirages sont uniformes. Quelle loi suit la variable aléatoire y ?

On définit le **simulateur** de transcript suivant :

1. choisir uniformément $\boldsymbol{e}' = (e'_1, \ldots, e'_k) \in \{0,1\}^k$,
2. choisir uniformément $r' \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $\epsilon' \in \{-1, 1\}$, puis calculer $x = \epsilon'(r')^2 \prod p_j^{e'_j} \mod n$,
3. définir $y' = r'$.

Question 5.– Démontrer que la loi de $(x', \boldsymbol{e}', y')$ induite par le simulateur est la même que celle de $(x, \boldsymbol{e}, y)$ issue du protocole d'identification. En déduire que le protocole est à divulgation nulle.

Solutions de l'Exercice 2.

Solution Q1. On doit vérifier que, modulo n, on a $y^2 \prod_{j=1}^k p_j^{e_j} \in \{-x, x\}$. Calculons :

$$y^2 \prod_{j=1}^k p_j^{e_j} = r^2 \prod_{j=1}^k s_j^{2e_j} (\varepsilon_j s_j^{-2})^{e_j} = r^2 \prod_{j=1}^k \varepsilon_j^{e_j}$$

Notons que ε et les ε_j sont dans $\{-1,1\}$, donc $y^2 \prod_{j=1}^k p_j^{e_j} \equiv \pm r^2 \equiv \pm \varepsilon r^2 \equiv \pm x \mod n$.

Solution Q2. Si un attaquant connaît le défi $\boldsymbol{e}$ avant son engagement, alors il peut :

— d'abord engendrer y aléatoirement,

— puis, calculer $x = y^2 \prod_j p_j^{e_j}$ (les p_j sont publics).

Lors d'une itération du protocole avec ces valeurs, Bob sera convaincu d'interagir avec Alice, car on aura (par construction) $x = y^2 \prod_j p_j^{e_j}$.

En toute généralité, l'attaquant peut donc essayer de deviner le vecteur $\boldsymbol{e}$. Si le tirage est uniforme, il obtient le bon vecteur avec probabilité 2^{-k}.

Solution Q3. Le problème repose sur la difficulté d'extraire une racine carrée modulo $n = pq$, lorsque la factorisation de n est inconnue. En effet, on observe que si l'on sait factoriser n, alors lors de la phase de réponse, il suffit de calculer une racine carrée de $x \prod_j p_j^{-e_j}$ modulo n pour convaincre Bob.

Solution Q4. La variable y suit une loi uniforme sur $(\mathbb{Z}/n\mathbb{Z})^\times$. En effet, y est construit come un produit d'éléments inversibles modulo n, tous tirés uniformément.

Solution Q5. On observe d'abord que le vecteur $\boldsymbol{e}'$ est tiré de la même manière que $\boldsymbol{e}$. Ensuite, on note que y' est tiré uniformément dans $(\mathbb{Z}/n\mathbb{Z})^\times$. D'après la question précédente, il suit la même loi que y. Enfin, la variable x' vaut

$$x' = \varepsilon'(r')^2 \prod_j \varepsilon_j^{e'_j} (s_j^{-e'_j})^2$$

Elle peut donc être décrire comme le produit d'un élément de $\{-1,1\}$ tiré uniformément (l'élément $\varepsilon' \prod_j \varepsilon_j^{e'_j}$), et d'un carré inversible (l'élément $r'^2 \prod_j (s_j^{-e'_j})^2$). La variable x' suit donc la même loi que x.

Enfin, ces trois variables sont liées par la même contrainte : $x = \alpha y^2 \prod_j p_j^{e_j}$, avec α uniforme dans $\{-1,1\}$. Les lois conjointes de $(x', \boldsymbol{e}', y')$ et $(x, \boldsymbol{e}, y)$ sont donc identiques.

Le protocole est donc à divulgation nulle (de connaissance du secret `sk`). En effet, on vient de démontrer que l'on peut simuler tout échange entre Alice et Bob sans la connaissance de ce secret.
