# 2. Quelques réductions

## 2.1 Problèmes aléatoirement auto-réductibles

Considérons le problème RSA, pour un module $n = pq$ et un exposant $e$ premier avec $\varphi(n)$. On dit qu'un algorithme $\mathcal{A}$ est un $(\varepsilon, t)$-adversaire contre le problème RSA $(n, e)$ si, en temps $t$, sa probabilité de résoudre une instance aléatoire est supérieure à $\varepsilon$ :

$$\mathsf{Succ}^{\mathsf{rsa}} n, e(\mathcal{A}) = \Pr_{x \in \mathbb{Z}_n^\star}[\mathcal{A}(n, e, x^e \bmod n) = x] \geq \varepsilon.$$

**Q-1.** Montrer que s'il existe un $(\varepsilon, t)$-adversaire contre le problème RSA $(n, e)$, alors il existe un algorithme qui résoud toute instance (avec probabilité proche de 1) en temps "raisonnable".

Décrire cet algorithme, et estimer ce temps "raisonnable".

## 2.2 Algorithme avec erreur contre le problème Diffie-Hellman

Dans la réduction ci-dessus, l'algorithme de départ résoud une instance RSA avec probabilité $\varepsilon$. Dans les autres cas, une réponse erronée ou un constat d'échec de la part de l'algorithme, sont équivalents puisque l'erreur est facilement détectée.

Considérons désormais le problème Diffie-Hellman sur un groupe cyclique $\mathcal{G}$ (noté multiplicativement) d'ordre premier $q$ (dont on désignera un générateur $g$). Le problème Diffie-Hellman dans $\mathcal{G}$, en la base $g$, consiste à calculer, sur les entrées $X = g^x$ et $Y = g^y$, la valeur $Z = g^{xy}$. On dit qu'un algorithme $\mathcal{A}$ est un $(\varepsilon, t)$-adversaire contre le problème Diffie-Hellman $(\mathcal{G}, g)$ si, en temps $t$, sa probabilité de résoudre une instance aléatoire est supérieure à $\varepsilon$ :

$$\mathsf{Succ}^{\mathsf{cdh}} \mathcal{G}, g(\mathcal{A}) = \Pr_{x,y \in \mathbb{Z}_q^\star}[\mathcal{A}(\mathcal{G}, g, g^x, g^y) = g^{xy}] \geq \varepsilon.$$

**Q-2.** Peut-on utiliser la même méthode que pour RSA ?

On veut cependant utiliser $\mathcal{A}$ pour résoudre l'instance fixée $(A = g^a, B = g^b)$, avec une bonne garantie du résultat. On dérive alors de cette instance une série d'instances $(X_i = A^{\alpha_i} g^{u_i}, Y_i = B^{\beta_i} g^{v_i})$, avec des exposants $\alpha_i, \beta_i, u_i, v_i$ aléatoires dans $\mathbb{Z}_q^\star$.

**Q-3.** Montrer qu'en cas de succès sur une instance $(X_i, Y_i)$, on en déduit la solution pour $(A, B)$. Montrer qu'en cas d'échec, cette même opération conduit à un élément parfaitement aléatoire dans $\mathcal{G}$.

Une méthode naturelle est donc de retourner la première collision, comme étant la solution. Il est en effet clair que deux succès conduisent tous deux à la solution, donc constituent une collision.

**Q-4.** Estimer la probabilité d'erreur, ainsi que le temps moyen d'exécution.

Il aurait été plus simple et plus rapide d'utiliser une séquence $(X_i = A^{\alpha_i}, Y_i = B^{\beta_i})$, avec des exposants $\alpha_i, \beta_i$ aléatoires dans $\mathbb{Z}_q^\star$.

**Q-5.** Montrer qu'un attaquant (tout puissant) pourrait nous induire en erreur, alors qu'avec le premier type de séquences, même un attaquant tout-puissant ne peut que nous aider à atteindre notre objectif.

## 2.3 Méthode des hybrides

Considérons deux distributions $\Delta_0$ et $\Delta_1$ sur un même ensemble $\mathcal{S}$. Un distingueur entre ces deux distributions est un algorithme capable d'avoir un comportement différent selon qu'il travaille sur une instance provenant de $\Delta_0$ ou de $\Delta_1$. Plus précisément, un $(\varepsilon, t)$-distingueur des distributions $\Delta_0$ et $\Delta_1$ est un algorithme $\mathcal{D}$ qui fonctionne en temps $t$, et possède un avantage $\mathsf{Adv}^{\Delta}(\mathcal{D})$ supérieur à $\varepsilon$ où

$$\mathsf{Adv}^{\Delta}(\mathcal{D}) = \Pr_{\delta\in\Delta_0}[\mathcal{D}(\delta)=1] - \Pr_{\delta\in\Delta_1}[\mathcal{D}(\delta)=1].$$

**Q-6.** Montrer que s'il existe un distingueur $\mathcal{D}'$ entre $\Delta_0^n$ et $\Delta_1^n$ en temps $t$ avec un avantage $\varepsilon$, alors il existe un distingueur $\mathcal{D}$ entre les distributions $\Delta_0$ et $\Delta_1$ avec un avantage supérieur à $\varepsilon/n$.

En déduire l'avantage maximal en temps $t$ entre $\Delta_0^n$ et $\Delta_1^n$ (noté $\mathsf{Adv}^{\Delta^n}(t)$) en fonction de l'avantage maximal en temps $t$ entre $\Delta_0$ et $\Delta_1$ (noté $\mathsf{Adv}^{\Delta}(t)$).

Considérons à nouveau le problème Diffie-Hellman. Comme on vient de le voir, le problème Diffie-Hellman (calculatoire) dans $\mathcal{G}$, en la base $g$, consiste à calculer, sur les entrées $X = g^x$ et $Y = g^y$, la valeur $Z = g^{xy}$. Il en existe une variante, appelée problème Diffie-Hellman décisionnel, qui consiste pour un algorithme (distingueur) de décider si, pour un triplet $(X, Y, Z)$ dans $\mathcal{G}$, $Z$ est effectivement la solution au problème Diffie-Hellman calculatoire ou non. On dit que $\mathcal{D}$ est un $(\varepsilon, t)$-distingueur contre le problème Diffie-Hellman décisionnel dans $\mathcal{G}$, en la base $g$, s'il fonctionne en temps $t$, et possède un avantage $\mathsf{Adv}^{\mathsf{ddh}}\mathcal{G}, g(\mathcal{D})$ supérieur à $\varepsilon$ où

$$\mathsf{Adv}^{\mathsf{ddh}}\mathcal{G}, g(\mathcal{D}) = \Pr_{x,y\in\mathbb{Z}_q^\star}[\mathcal{D}(\mathcal{G}, g, g^x, g^y, g^{xy})=1] - \Pr_{x,y,z\in\mathbb{Z}_q^\star}[\mathcal{D}(\mathcal{G}, g, g^x, g^y, g^z)=1].$$

En d'autres termes, si l'on considère les distributions suivantes :

$$\begin{aligned}\mathcal{DH}(\mathcal{G}, g) &= \{\mathcal{I} = (g^x, g^y, g^{xy}) \,|\, x, y \in \mathbb{Z}_q^\star\}\\ \mathcal{R}and(\mathcal{G}, g) &= \{\mathcal{I} = (g^x, g^y, g^z) \,|\, x, y, z \in \mathbb{Z}_q^\star\}\end{aligned}$$

$$\mathsf{Adv}^{\mathsf{ddh}}\mathcal{G}, g(\mathcal{D}) = \Pr_{\mathcal{I}\in\mathcal{DH}(\mathcal{G},g)}[\mathcal{D}(\mathcal{G}, g, \mathcal{I})=1] - \Pr_{\mathcal{I}\in\mathcal{R}and(\mathcal{G},g)}[\mathcal{D}(\mathcal{G}, g, \mathcal{I})=1].$$

**Q-7.** Montrer que s'il existe un distingueur $\mathcal{D}'$ entre $\mathcal{DH}(\mathcal{G}, g)^n$ et $\mathcal{R}and(\mathcal{G}, g)^n$ en temps $t$ avec un avantage $\varepsilon$, alors il existe un distingueur $\mathcal{D}$ contre le problème Diffie-Hellman décisionnel avec un avantage supérieur à $\varepsilon$, en un temps $t' \leq t + \mathcal{O}(n)$.