# 9. Etude d'un schéma de chiffrement

## 9.1 Les courbes elliptiques et les couplages

Sur certaines courbes elliptiques (dont on notera $(\mathbb{G}, +)$ un sous-groupe d'ordre premier $q$, engendré par $P$), il existe une application $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, où $\mathbb{G}_T$ est un sous-groupe du groupe multiplicatif (d'ordre $q$) d'une extension finie d'un corps fini, telle que :

— $e$ est efficacement calculable (en temps $t_e$) ;

— $e$ est bilinéaire dans $(\mathbb{G}_T, \times)$, ce qui signifie que pour tous $P, Q \in \mathbb{G}$ et $a, b \in \mathbb{Z}_q$, alors $e(a \cdot P, b \cdot Q) = e(P, Q)^{ab} \in \mathbb{G}_T$.

— $e$ est non-dégénérée, ce qui signifie que $e(P, P)$ est un générateur de $\mathbb{G}_T$.

On peut alors définir les problèmes Diffie-Hellman usuels :

— le problème Diffie-Hellman calculatoire dans le groupe $\mathbb{G} = \langle P \rangle$ —noté $\mathsf{CDH}_{\mathbb{G},P}$— qui consiste à calculer $ab \cdot P$, à partir de $P_a = a \cdot P, P_b = b \cdot P \in \mathbb{G}$. On mesure le succès d'un attaquant $\mathcal{A}$ par

$$\mathsf{Succ}^{\mathsf{cdh}}_{\mathbb{G},P}(\mathcal{A}) = \Pr_{a,b \in \mathbb{Z}_q}[\mathcal{A}(a \cdot P, b \cdot P) = ab \cdot P].$$

— le problème Diffie-Hellman décisionnel dans le groupe $\mathbb{G} = \langle P \rangle$ —noté $\mathsf{DDH}_{\mathbb{G},P}$— qui consiste à décider si un élément $Q$ donné est le $\mathsf{CDH}_{\mathbb{G},P}$ de $(P_a, P_b)$, ou non. On mesure l'avantage d'un distingueur $\mathcal{A}$ par

$$\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G},P}(\mathcal{A}) = \left| \Pr_{a,b \in \mathbb{Z}_q}[\mathcal{A}(a \cdot P, b \cdot P, ab \cdot P) = 1] - \Pr_{a,b,c \in \mathbb{Z}_q}[\mathcal{A}(a \cdot P, b \cdot P, c \cdot P) = 1] \right|.$$

Pour toutes les mesures de succès ou d'avantages ci-dessus (et à venir), on définit par $\mathsf{Succ}(t)$ ou $\mathsf{Adv}(t)$, les valeurs maximales atteintes pour des attaquants qui fonctionnent en temps borné par $t$.

**Q-1.** Il existe de tels contextes $(\mathbb{G} = \langle P \rangle, \mathbb{G}_T, e)$ pour lesquels on peut admettre la difficulté du problème Diffie-Hellman calculatoire sur $\mathbb{G}$ (pour tout temps $t$ raisonnable, $\mathsf{Succ}^{\mathsf{cdh}}_{\mathbb{G},P}(t)$ est très petit). Montrer cependant qu'il n'est pas raisonnable de supposer la difficulté du problème Diffie-Hellman décisionnel sur $\mathbb{G}$.

On définit alors les problèmes décisionnels suivants :

— le problème Diffie-Hellman décisionnel bilinéaire dans $\mathbb{G} = \langle P \rangle$ —noté $\mathsf{DBDH}_{\mathbb{G},P}$— qui consiste à décider, étant donné $(P_a = a \cdot P, P_b = b \cdot P, P_c = c \cdot P) \in \mathbb{G}^3$ et $Q \in \mathbb{G}$, si $Q = abc \cdot P$ ou non. On mesure l'avantage d'un distingueur $\mathcal{A}$ par

$$\mathsf{Adv}^{\mathsf{dbdh}}_{\mathbb{G},P}(\mathcal{A}) = \left| \begin{array}{l} \Pr_{a,b,c \in \mathbb{Z}_q}[\mathcal{A}(a \cdot P, b \cdot P, c \cdot P, abc \cdot P) = 1] \\ \quad - \Pr_{a,b,c,d \in \mathbb{Z}_q}[\mathcal{A}(a \cdot P, b \cdot P, c \cdot P, d \cdot P) = 1] \end{array} \right|.$$

— le problème Diffie-Hellman décisionnel bilinéaire dans $\mathbb{G} = \langle P \rangle$ et $\mathbb{G}_T$ —noté $\mathsf{DBDH}_{\mathbb{G},\mathbb{G}_T,P}$— qui consiste à décider, étant donné $(P_a = a \cdot P, P_b = b \cdot P, P_c = c \cdot P) \in \mathbb{G}^3$ et $\alpha \in \mathbb{G}_T$, si $\alpha = e(P, P)^{abc}$ ou non. On mesure l'avantage d'un distingueur $\mathcal{A}$ par

$$\mathsf{Adv}^{\mathsf{dbdh}}_{\mathbb{G},\mathbb{G}_T,P}(\mathcal{A}) = \left| \begin{array}{l} \Pr[\mathcal{A}(a \cdot P, b \cdot P, c \cdot P, e(P, P)^{abc}) = 1] \\ \quad - \Pr[\mathcal{A}(a \cdot P, b \cdot P, c \cdot P, e(P, P)^{d}) = 1] \end{array} \right|.$$

**Q-2.** Donner une relation entre $\mathsf{Adv}^{\mathsf{dbdh}}_{\mathbb{G},P}(t)$ et $\mathsf{Adv}^{\mathsf{dbdh}}_{\mathbb{G},\mathbb{G}_T,P}(t')$, où $t$ et $t'$ sont clairement reliés (notamment avec $t_e$, le temps de calcul pour évaluer un couplage $e$).

## 9.2 Un schéma de signature

Considérons le schéma de signature $\mathsf{Sign} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ suivant, dans un contexte $(\mathbb{G}, \mathbb{G}_T, e)$ comme défini ci-dessus, avec $P$ un générateur de $\mathbb{G}$, d'ordre premier $q$. On a également une fonction de hachage $H : \{0,1\}^\star \to \mathbb{G}$.

— $\mathcal{K}(1^k)$ : la clé publique $\mathsf{pk}$ de vérification est définie par un point $X = x \cdot P$ ; la clé de signature $\mathsf{sk}$ consiste en le scalaire $x \in \mathbb{Z}_q$ ;
— $\mathcal{S}(\mathsf{sk}, m)$ : la signature d'un message $m \in \{0,1\}^\star$ est $\sigma = x \cdot H(m) \in \mathbb{G}$ ;
— $\mathcal{V}(\mathsf{pk}, m, \sigma)$ : la vérification d'un couple $(m, \sigma) \in \{0,1\}^\star \times \mathbb{G}$ consiste en le test

$$e(P, \sigma) \stackrel{?}{=} e(X, H(m)).$$

**Q-3.** Montrer que ce schéma est correct (une signature correctement fabriquée sera acceptée).

**Q-4.** Montrer que, dans le modèle de l'oracle aléatoire ($H$ est supposée être une fonction parfaitement aléatoire sur $\mathbb{G}$), ce schéma est infalsifiable à partir de la clé publique (niveau de sécurité $\mathsf{EF} - \mathsf{NMA}$ – pour *Existential Unforgeability under No Message Attacks*).
— On précisera l'hypothèse algorithmique nécessaire.
— On présentera une réduction, puis on conclura avec une borne sur $\mathsf{Succ}^{\mathsf{ef-nma}}_{\mathsf{Sign}}(t)$.
On pourra utiliser $t_m$, le temps d'une multiplication d'un point de $\mathbb{G}$ par un scalaire dans cette relation.

**Rappel :** Le succès $\mathsf{Succ}^{\mathsf{ef-nma}}_{\mathsf{Sign}}(\mathcal{A})$ d'un attaquant $\mathcal{A}$ pour produire une falsification existentielle contre un schéma de signature $\mathsf{Sign} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ est

$$\mathsf{Succ}^{\mathsf{ef-nma}}_{\mathsf{Sign}}(\mathcal{A}) = \Pr\left[\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k), (m, \sigma) \leftarrow \mathcal{A}(\mathsf{pk}) : \mathcal{V}(\mathsf{pk}, m, \sigma) = 1\ \right].$$

**Q-5.** Montrer que, dans le modèle de l'oracle aléatoire, ce schéma est infalsifiable, même selon des attaques à messages choisis (niveau de sécurité $\mathsf{EF} - \mathsf{CMA}$).
— On précisera l'hypothèse algorithmique nécessaire.
— On présentera une réduction, puis on conclura avec une borne sur $\mathsf{Succ}^{\mathsf{ef-cma}}_{\mathsf{Sign}}(t)$.

**Rappel :** Le succès $\mathsf{Succ}^{\mathsf{ef-cma}}_{\mathsf{Sign}}(\mathcal{A})$ d'un attaquant $\mathcal{A}$ pour produire une falsification existentielle selon une attaque à messages choisis contre un schéma de signature $\mathsf{Sign} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ est

$$\mathsf{Succ}^{\mathsf{ef-cma}}_{\mathsf{Sign}}(\mathcal{A}) = \Pr\left[\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k), (m, \sigma) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{pk}) : \mathcal{V}(\mathsf{pk}, m, \sigma) = 1\ \right].$$

On remarque que pendant l'attaque, $\mathcal{A}$ a accès à l'oracle de signature $\mathcal{S}$. Mais bien évidemment, la falsification doit être sur un nouveau message $m$, non demandé à $\mathcal{S}$.

**Q-6.** Sachant que les points du groupe $\mathbb{G}$ peuvent être codés sur moins de 200 bits, commenter les propriétés de ce schéma de signature.

## 9.3 Chiffrement basé sur l'identité

L'avantage du chiffrement asymétrique, par rapport au chiffrement symétrique, est la possibilité d'envoyer un message chiffré à un interlocuteur avec qui l'on n'a jamais mis de secret en commun : seule sa clé publique est nécessaire. Néanmoins, cette clé publique doit être authentique, et donc, une autorité de certification est nécessaire.

Le chiffrement basé sur l'idendité permet de se passer de cette autorité de certification, puisque la clé publique de chacun est sa propre identité (ou son adresse e-mail), et une autorité se charge de distribuer les clés de déchiffrement associées.

Considérons donc le schéma de chiffrement basé sur l'identité (*Identity-Based Encryption*) $\mathsf{IBE} = (\mathcal{K}, \mathsf{Extract}, \mathcal{E}, \mathcal{D})$ suivant :

- Données communes : le contexte ci-dessus, $(\mathbb{G} = \langle P \rangle, \mathbb{G}_T, e)$, où $P$ est un générateur d'ordre premier $q$. Nous avons également une fonction de hachage $H : \{0,1\}^\star \to \mathbb{G}$.
- $\mathcal{K}(1^k)$ : génération des clés de l'autorité, qui consistent en la clé secrète maître, un scalaire $s \in \mathbb{Z}_q$, et la clé publique maître, $Q = s \cdot P$. La clé $Q$ est connue de tous.
- $\mathsf{Extract}(s, \mathsf{ID})$ : l'algorithme d'extraction fournit, à l'aide de la clé secrète maître $s$, la clé de déchiffrement pour l'utilisateur d'identité $\mathsf{ID}$. Il s'agit de $\mathsf{sk} = s \cdot H(\mathsf{ID})$.
- $\mathcal{E}(\mathsf{ID}, m)$ : pour chiffrer un message $m \in \mathbb{G}_T$ à un individu $\mathsf{ID}$, on génère un aléa $r \in \mathbb{Z}_q$, puis le chiffré consiste en le couple $c = (R = r \cdot P, K \times m)$ où $K = e(H(\mathsf{ID}), Q)^r$.
- $\mathcal{D}(\mathsf{sk}, c)$ : pour déchiffrer un couple $c = (R, C)$, on calcule $K = e(\mathsf{sk}, R)$, puis on démasque $m = C/K$.

**Q-7.** Montrer qu'il est difficile, dans le modèle de l'oracle aléatoire, de générer une clé $\mathsf{sk}$ valide pour une nouvelle identité, sans l'aide de l'autorité, même après plusieurs requêtes d'extraction.

**Q-8.** Montrer que ce schéma est correct (un chiffré sera convenablement déchiffré).

**Q-9.** Montrer que ce schéma satisfait le niveau de sécurité $\mathsf{IND} - \mathsf{CPA}$, sous une hypothèse bien précise. On présentera la réduction.

**Note :** L'avantage $\mathsf{Adv}^{\mathsf{ind-cpa}}_{\mathsf{PKE}}(\mathcal{A})$ d'un attaquant $\mathcal{A}$ contre l'indistingabilité d'un schéma de chiffrement $\mathsf{PKE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ est

$$\mathsf{Adv}^{\mathsf{ind-cpa}}_{\mathsf{PKE}}(\mathcal{A}) = 2 \times \Pr[(s, Q) \leftarrow \mathcal{K}(1^k), (\mathsf{ID}, m_0, m_1) \leftarrow \mathcal{A}_1(Q), c = \mathcal{E}(\mathsf{ID}, m_b) : \mathcal{A}_2(c) = b] - 1.$$

On remarque que la définition est ici classique, puisque l'oracle $\mathsf{Extract}$ n'apparaît pas.

Dans un tel environnement, basé sur l'identité, la notion $\mathsf{IND} - \mathsf{CPA}$ est faible, puisque l'attaquant n'a pas accès à l'oracle $\mathsf{Extract}$.

**Q-10.** Si l'on donne accès à l'attaquant à l'oracle $\mathsf{Extract}$, quelles sont les contraintes à imposer quant à ces requêtes pour que le niveau de sécurité soit accessible ?

**Q-11.** Montrer que ce schéma satisfait ce niveau de sécurité $\mathsf{IND} - \mathsf{ID\text{-}CPA}$ pour « Indistingabilité selon des attaques à clairs et identités choisis » (chiffrement des messages de son choix, et extraction des clés secrètes pour les identités de son choix).

- On précisera l'hypothèse algorithmique nécessaire.
- On présentera une réduction, puis on conclura avec une borne sur $\mathsf{Succ}^{\mathsf{ind-id-cpa}}_{\mathsf{IBE}}(t)$.

**Q-12.** Montrer qu'en masquant avec $H'(K)$, au lieu de $K$, on peut reposer sur une hypothèse algorithmique plus faible, dans le modèle de l'oracle aléatoire.