

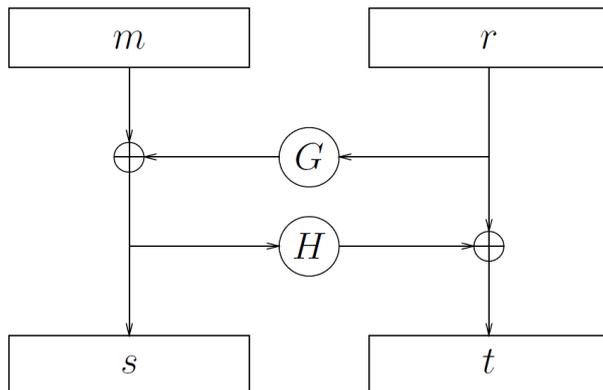
5. OAEP : Optimal Asymmetric Encryption Padding

5.1 Description

En 1994, Bellare et Rogaway ont proposé le padding suivant à appliquer avant l'utilisation d'une permutation à sens-unique à trappe f_{pk} (telle RSA) de $\{0, 1\}^k$, où

$$G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^n \text{ et } H : \{0, 1\}^n \rightarrow \{0, 1\}^{k_0},$$

avec $k = k_0 + n$.



C'est-à-dire que pour chiffrer un message $m \in \{0, 1\}^n$, on applique la construction ci-dessus avec un aléa $r \xleftarrow{R} \{0, 1\}^{k_0}$, pour obtenir le couple $(s, t) = \text{OAEP}(m, r)$. On applique alors la permutation f_{pk} sur l'objet $s||t$ pour obtenir le chiffré $c = \mathcal{E}_{pk}(m; r)$.

Q-1. Décrire l'algorithme de déchiffrement en fonction de g_{sk} , la permutation réciproque de f_{pk} , accessible à qui connaît la trappe sk .

5.2 Sécurité sémantique

Soit $y = f_{pk}(s||t)$, le chiffré du message $m_b = m \in \{m_0, m_1\}$, avec l'aléa r (donc $(s, t) = \text{OAEP}(m_b, r)$ pour $b \in \{0, 1\}$).

Q-2. Montrer que, dans le modèle de l'oracle aléatoire où les fonctions G et H sont modélisées par des fonctions parfaitement aléatoires, sans avoir posé la question $G(r)$, un attaquant a un avantage nul pour deviner b (soit si $m = m_0$ ou si $m = m_1$).

Rappel : L'avantage d'un attaquant contre la sécurité sémantique d'un schéma de chiffrement $\pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ est

$$\text{Adv}_{\pi}^{\text{ind}}(\mathcal{A}) = 2 \times \Pr_{\substack{b \leftarrow \{0, 1\} \\ r \leftarrow \{0, 1\}^{k_0}}} \left[(\text{pk}, \text{sk}) \leftarrow \mathcal{G}(1^k); (m_0, m_1, s) \leftarrow A_1(\text{pk}) \right. \\ \left. c = \mathcal{E}_{\text{pk}}(m_b; r) : A_2(m_0, m_1, s, c) = b \right] - 1.$$

Q-3. Préciser l'avantage d'un attaquant qui n'aurait pas posé la question $H(s)$.

Q-4. En déduire que cette construction conduit à un schéma IND-CPA, dans le modèle de l'oracle aléatoire, sous réserve que f_{pk} soit une permutation à sens-unique à trappe sur $\{0, 1\}^k$.

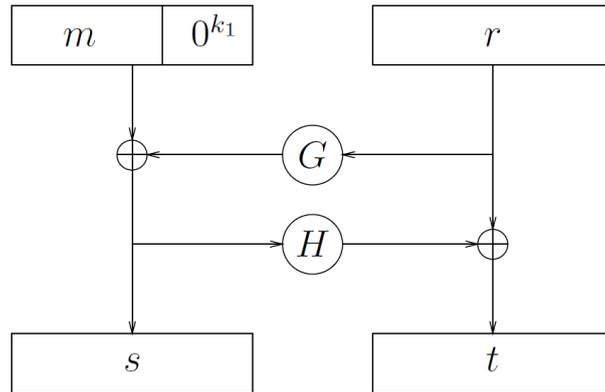
Note : Pour cela, on précisera l'avantage maximal, en temps t , d'un attaquant qui peut poser au plus q_g et q_h questions aux oracles G et H respectivement. On pourra utiliser $\text{Succ}_f^{\text{ow}}(t)$, le maximum pour tout algorithme \mathcal{A} en temps t de

$$\text{Succ}_f^{\text{ow}}(t) = \max_{\mathcal{A}} \left\{ \Pr_{\text{pk}, x} [\mathcal{A}(f_{\text{pk}}(x)) = x] \right\},$$

où pk et x sont choisis selon les distributions convenables : $(\text{pk}, \text{sk}) \leftarrow \mathcal{G}(1^k)$ et $x \leftarrow \{0, 1\}^k$.

5.3 Non-malléabilité

L'objectif initial de OAEP était de conduire à un schéma de chiffrement sûr contre les attaques à chiffrés choisis à partir de toute permutation à sens-unique à trappe. Pour cela, une redondance était nécessaire : $(s, t) = \text{OAEP}'(m, r) = \text{OAEP}(m \| 0^{k_1}, r)$, avec $m \in \{0, 1\}^{n-k_1}$ et $r \in \{0, 1\}^{k_0}$.



Un chiffré est considéré valide si l'inversion de f_{pk} fait bien apparaître cette redondance 0^{k_1} . Et alors, ce qui précède cette série de 0 est retourné en tant que message clair. Dans le cas contraire, le chiffré est refusé.

Considérons une permutation à sens-unique à trappe F_{pk} de $\{0, 1\}^{k_0}$, pour laquelle il existe un algorithme \mathcal{A} qui calcule $F_{\text{pk}}(x \oplus a)$ à partir de pk , a et $y = F_{\text{pk}}(x)$:

$$\mathcal{A}(\text{pk}, a, y = F_{\text{pk}}(x)) = F_{\text{pk}}(x \oplus a).$$

Définissons la fonction de $f_{\text{pk}}(s \| t) = s \| F_{\text{pk}}(t)$, pour $s \in \{0, 1\}^n$ et $t \in \{0, 1\}^{k_0}$.

Q-5. Montrer que f_{pk} est une permutation de $\{0, 1\}^k$ à sens-unique à trappe. Pour cela, on évaluera $\text{Succ}_f^{\text{ow}}(t)$ en fonction de $\text{Succ}_F^{\text{ow}}(t)$.

Q-6. Exprimer $(s', t') = \text{OAEP}'(m \oplus \delta, r)$, pour $\delta \in \{0, 1\}^{n-k_1}$, en fonction de

$$(s, t) = \text{OAEP}'(m, r), \quad \Delta = \delta \| 0^{k_1}, \quad \Gamma = H(s) \oplus H(s').$$

Q-7. En déduite que la construction OAEP' sur la fonction f_{pk} est malléable.

Q-8. Que dire de son niveau de sécurité IND-CCA2 souhaité ?