Indistinguabilité

Soit $\mathbf{G}$ un groupe cyclique d'ordre q premier engendré par g. Soit $\mathcal{P}$ la distribution uniforme sur $(\mathbb{Z}_q, \mathbf{G})$. Soit $\mathcal{P}_{DL}$ la distribution uniforme sur l'ensemble $\{(r, g^r), r \in \mathbb{Z}_q\}$. Soit $\mathcal{P}_{NDL}$ la distribution uniforme sur l'ensemble $\{(r, g^{r'}), r \neq r' \in \mathbb{Z}_q\}$. On rappelle l'expression de la distance statistique entre deux variables aléatoires discrètes sur un ensemble A dénombrable :

$$\Delta(X, Y) = \frac{1}{2} \sum_{a \in A} |\Pr[X = a] - \Pr[Y = a]| \quad .$$

Question 1. *$\mathcal{P}_{NDL}$ et $\mathcal{P}$ sont-elles calculatoirement indistinguables ? Statistiquement indistinguables ? Les deux ?*

Question 2. *$\mathcal{P}_{DL}$ et $\mathcal{P}$ sont-elles calculatoirement indistinguables ? Statistiquement indistinguables ? Les deux ?*

Cryptosystème de Okamoto-Uchiyama

Cryptosystème de Okamoto-Uchiyama

$\mathsf{KeyGen}(1^n)$:

- Choisir deux entiers premiers p, q tels que $p \mid (q-1)$.
- Définir $N = p^2 q$.
- Choisir un générateur $g \in \mathbb{Z}_N^*$ tel que $g^{p-1} \neq 1 \mod p^2$
- Définir $h = g^N \bmod N$.
- Clé publique : $\mathsf{pk} = (N, g, h)$; clé privée : $\mathsf{sk} = (p, q)$

$\mathsf{Enc}(\mathsf{pk}, m)$ $(m < p)$:

- $r \leftarrow U(\mathbb{Z}_N^*)$
- $c := g^m \cdot h^r \mod N$
- Renvoyer c

Dec ...

Soit $\Gamma = \{x \in \mathbb{Z}_{p^2}^*, x = 1 \mod p\}$.

Question 3. *Montrer que Γ est un sous-groupe de $(\mathbb{Z}_{p^2})^*$ d'ordre p.*

Soit la fonction $L : \mathbb{Z}_{p^2}^* \to \mathbb{Z}_p$ définie par :

$$L(x) := \frac{x-1}{p} \mod p.$$

Question 4. *Montrer que L est un isomorphisme entre Γ et le groupe additif $\mathbb{Z}_p$. En déduire que le problème du logarithme discret est facile dans Γ : sur une entrée $(x, y) \in \Gamma$ avec $L(x) \neq 0$ et $y = x^m \mod p^2$, on peut calculer efficacement m.*

Question 5. *Montrer que $(h^r)^{p-1} = 1 \mod p^2$. En déduire l'algorithme de déchiffrement.*

On va montrer la sécurité IND-CPA sous l'hypothèse :

> Pour $h = g^N \mod N$, la distribution $\{h^r \mod N, r \leftarrow U(\mathbb{Z}_N)\}$ (SUBGROUP) et la distribution $\{gh^{r'} \mod N, r' \leftarrow U(\mathbb{Z}_N)\}$ (RANDOM) sont calculatoirement indistinguables.

En d'autres termes, cette hypothèse suppose que le chiffrement de 0 et 1 sont indistinguables.

Question 6. *Montrer qu'étant donné une paire de messages* (m_0, m_1) *et* $c = \mathsf{Enc}(\mathsf{pk}, b)$ *où* b *est un bit inconnu, on peut facilement calculer un chiffré* $c^* = \mathsf{Enc}(\mathsf{pk}, m_b)$ *aléatoire valide.*

Question 7. *Montrer la sécurité IND-CPA.*

Montgomery power ladder

On considère l'agorithme suivant (*Montgomery power ladder*).

Entrée : x, N, $e = \sum_{i=0}^{k-1} e_i 2^i$

Sortie : $x^e \mod N$

$R_0 \leftarrow 1, R_1 \leftarrow x$
for $i = k-1, k-2, \ldots, 0$ **do**
    if $e_i = 1$ **then**
        $R_0 \leftarrow R_0 \cdot R_1 \mod N$
        $R_1 \leftarrow R_1 \cdot R_1 \mod N$
    else
        $R_1 \leftarrow R_1 \cdot R_0 \mod N$
        $R_0 \leftarrow R_0 \cdot R_0 \mod N$
    end if
end for
Return R_0

Question 8. *Montrer que l'algorithme est correct. Quel est son intérêt ?*