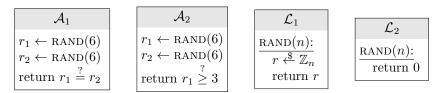
TD 1 Cryptographie

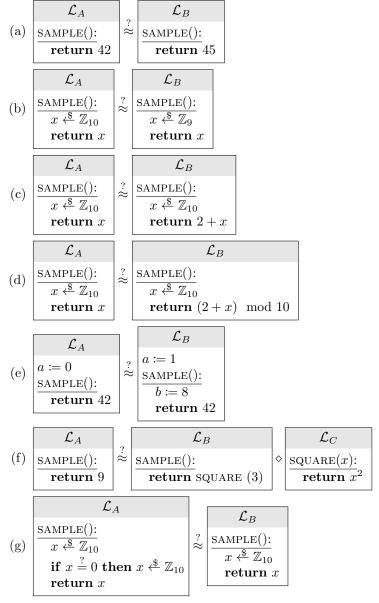
Léo Colisson Palais

Exercice 1: Librairies indistinguables

1. Calculer $\Pr\left[A_1 \diamond \mathcal{L}_1 = \mathsf{true}\right], \Pr\left[A_1 \diamond \mathcal{L}_2 = \mathsf{true}\right], \Pr\left[A_2 \diamond \mathcal{L}_1 = \mathsf{true}\right], \Pr\left[A_2 \diamond \mathcal{L}_2 = \mathsf{true}\right]$ avec



2. Les librairies suivantes sont elles indistinguables ? (si oui, décrivez un distingueur et calculez sa probabilité de succès, exercice à faire sur Moodle en python):



(h) Les librairies de la définition de sécurité IND-CPA avec le chiffrement $\mathsf{Gen}(1^{\lambda})$ qui retourne toujours 0, et $\mathsf{Enc}_k(m) \coloneqq \bar{m}$, où $m \in \{0,1\}^{\lambda}$, \bar{m} inverse m bit à bit (0 devient 1 et 1 devient 0).

- (i) Les librairies de la définition de sécurité IND-CPA avec le chiffrement du One-Time Pad, i.e. $\mathsf{Gen}(1^{\lambda})$ qui retourne une clé aléatoire dans $\{0,1\}^{\lambda}$, et $\mathsf{Enc}_k(m) \coloneqq m \oplus k$.
- (i) Les librairies de la définition de sécurité IND-CPA avec un chiffrement inconnu mais déterministe.

Exercice 2: Fonction négligeable et manipulation de librairie

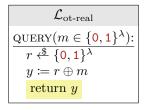
1. Les quelles de ces fonction sont négligeables ? (Prouvez-le, la formule $a^b=2^{b\log a}$ peut-être utile)

$$\frac{1}{2^{\lambda/2}} \qquad \frac{1}{2^{\log(\lambda^2)}} \qquad \frac{1}{\lambda^{\log(\lambda)}} \qquad \frac{1}{\lambda^2} \qquad \frac{1}{2^{\log\lambda^2}} \qquad \frac{1}{\lambda^{1/\lambda}} \qquad \frac{1}{\sqrt{\lambda}} \qquad \frac{1}{2^{\sqrt{\lambda}}}$$

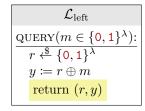
- 2. Montrer que si f et g sont négligeable, alors f+g et fg le sont également.
- 3. Montrer que si $f = poly(\lambda)$ et $g = negl(\lambda)$, alors $fg = negl(\lambda)$.

Exercice 3: Un simple partage de secret

Nous considérons les librairies suivantes :



$$\mathcal{L}_{ ext{ot-rand}}$$
 $ext{QUERY}(m \in \{0,1\}^{\lambda}): \ r \overset{\$}{\leftarrow} \{0,1\}^{\lambda}$ $ext{return } r$



$$\mathcal{L}_{ ext{right}}$$
 $rac{ ext{QUERY}(m \in \{0,1\}^{\lambda}):}{r \overset{\$}{\leftarrow} \{0,1\}^{\lambda}} \ y \coloneqq r \oplus m \ ext{return } (y,r)$

- 1. Montrer que $\mathcal{L}_{ot\text{-real}} \equiv \mathcal{L}_{ot\text{-rand}}$ Indice: utiliser la méthode "calcul des probabilités".
- 2. Utilise cette propriété pour montrer que le OTP est sécurisé en usage unique, i.e. que les deux librairies suivantes sont indistinguables :

$$\begin{array}{|c|} \hline \mathcal{L}_{\text{ots-L}}^{\Sigma} \\ \hline \text{EAVESDROP}(m_L, m_R \in \mathcal{M}) \text{:} \\ \hline k \leftarrow \mathsf{Gen}(1^{\lambda}) \\ \text{return } \mathsf{Enc}_k(m_L) \\ \hline \end{array} \equiv \begin{array}{|c|} \hline \mathcal{L}_{\text{ots-R}}^{\Sigma} \\ \hline \text{EAVESDROP}(m_L, m_R \in \mathcal{M}) \text{:} \\ \hline k \leftarrow \mathsf{Gen}(1^{\lambda}) \\ \text{return } \mathsf{Enc}_k(m_R) \\ \hline \end{array}$$

- 3. Montrez que $\mathcal{L}_{left} \equiv \mathcal{L}_{right}$. Pouvez-vous utiliser directement le fait que $\mathcal{L}_{ot\text{-real}} \equiv \mathcal{L}_{ot\text{-rand}}$? Si oui, prouvez-le, sinon, montrez où la preuve naïve échoue.
- 4. Un schéma de partage secret à seuil t sur n (TSSS) consiste en deux algorithmes
 - Share $(m \in \mathcal{M})$ qui produit une séquence $s = (s_1, \ldots, s_n)$ de parts,
 - Reconstruct($\{s_1, \ldots, s_k\}$) qui produit un message $m \in \mathcal{M}$ si $k \geq t$ et \perp sinon.

 tels que :

- Correction: pour tout $m \in \mathcal{M}$ et tout $U \subseteq \{1, \ldots, n\}$ avec $|U| \ge t$, et pour tout $s \leftarrow \mathsf{Share}(m)$, on a Reconstruct $(\{s_i \mid i \in U\}) = m$,
- Sécurité : on a

$$\frac{\mathcal{L}_{tsss-L}}{\begin{array}{c} \underline{SHARE}(m_L, m_R, U):} \\ \underline{sf} \mid U \mid \geq t, \text{ return err} \\ s \leftarrow \underline{SHARE}(m_L) \\ \text{ return } \{s_i \mid i \in U\} \end{array}} \equiv \begin{vmatrix} \mathcal{L}_{tsss-R} \\ \underline{SHARE}(m_L, m_R, U):} \\ \underline{sf} \mid U \mid \geq t, \text{ return err} \\ s \leftarrow \underline{SHARE}(m_R) \\ \text{ return } \{s_i \mid i \in U\} \end{vmatrix} \tag{1}$$

(a) Expliquez pourquoi on appelle cela un "schéma de partage secret".

(b) La construction suivante est-elle sécurisée ? Si oui, prouvez-le, sinon, trouvez un attaquant explicite.

```
\mathcal{M} = \{0, 1\}^{500} 
t = 5
n = 5
Share(m):
split m into <math>m = s_1 \| \cdots \| s_5,
where each <math>|s_i| = 100
return (s_1, \dots, s_5)
return (s_1, \dots, s_5)
```

- (c) On considère un schéma simple de partage secret 2-sur-2, où Share est défini comme la QUERY dans \mathcal{L}_{left} . Décrivez la procédure Reconstruct.
- (d) Prouvez que ce schéma est sécurisé. Ω ap unique ce schéma est sécurisé.
- (e) Pouvez-vous généraliser cette construction pour obtenir un schéma de partage secret 2-sur-k pour un $k \in \mathbb{N}^*$ quelconque et en prouver la sécurité?

Exercice 4: Security of OTP

- 1. Quelqu'un se rend compte que l'OTP révèle le message quand la clé est $0 \dots 0$, et propose de choisir la clé dans $\{0,1\}^{\lambda} \setminus \{0^{\lambda}\}$ au lieu de $\{0,1\}^{\lambda}$. Est-ce plus (ou moins) sécurisé ? Si oui, prouvez-le, sinon trouvez un attaquant cassant la one-time security du schéma (c'est-à-dire un adversaire qui distingue $\mathcal{L}_{\text{ots-L}}^{\Sigma}$ de $\mathcal{L}_{\text{ots-R}}^{\Sigma}$).
- 2. Pour obtenir une sécurité supplémentaire, Alice décide de chiffrer deux fois le message avec OTP. Quels sont les impacts réels en termes de sécurité (i) si Alice utilise la même clé k pour les deux chiffrages (ii) si Alice utilise des clés différentes ?
- 3. Qu'y a-t-il de particulier avec la fonction XOR de l'OTP ? Est-ce que cela fonctionnerait correctement et/ou serait sécurisé avec, par exemple, un AND au lieu d'un XOR ? Est-ce que ça marcherait si on interprète les chaînes comme des entiers modulo 2^{λ} et remplace le XOR par une addition modulaire ? (prouvez formellement vos affirmations)
- 4. Montrez que le schéma de chiffrement suivant n'a pas de secret one-time, en construisant un programme qui distingue les deux bibliothèques pertinentes de la définition de one-time security.

$$\mathcal{K} = \{1, \dots, 9\}$$

$$\mathcal{M} = \{1, \dots, 9\}$$

$$\mathcal{C} = \mathbb{Z}_{10}$$

$$\frac{\mathsf{Gen:}}{k \leftarrow \{1, \dots, 9\}}$$

$$\frac{\mathsf{Enc}(k, m):}{\mathsf{return } k} \times m\%10$$

5. Toi (Eve), tu as intercepté deux textes chiffrés :

```
c_1 = 1111100101111001110011000001011110000110
c_2 = 1111101001100111111011101000100110001000
```

Tu sais que les deux sont des chiffrés OTP, encryptés avec la même clé. Tu sais que soit (i) c_1 est le chiffré de alpha et c_2 est le chiffré de bravo, soit (ii) c_1 est le chiffré de delta et c_2 est le chiffré de gamma (tous convertis en binaire à partir de l'ASCII de manière standard, c'est-à-dire a=97,b=98...). Quelle de ces deux possibilités est correcte, et pourquoi ? Peux-tu retrouver la clé ?