Constrained Pseudorandom Functions, Revisited

Julian Mouthon, Mario Razafinony

1 Définitions

Fonction pseudo-aléatoire (PRF)

Une fonction pseudo-aléatoire

$$F : \mathcal{K} \times D \to R$$

est une fonction telle que, pour une clé secrète K, la fonction $F(K, \cdot)$ est indiscernable d'une fonction réellement aléatoire $G : D \to R$ pour tout adversaire efficace.

Contrainte

$$C : D \to \{0, 1\}.$$

$C(x) = 1$: « l'entrée est autorisée » $\qquad$ $C(x) = 0$: « l'entrée est interdite ».

CPRF

Une fonction pseudo-aléatoire contrainte (CPRF) est donnée par quatre algorithmes efficaces :

- $\mathsf{Setup}(1^\lambda) \to K$ (clé maître) : génère la clé secrète principale K.
- $\mathsf{Constrain}(K, C) \to K_C$ (clé contrainte) : produit une clé spéciale K_C permettant d'évaluer la fonction uniquement sur les entrées autorisées par C.
- $\mathsf{Eval}(K, x) \to y$: évalue la fonction pseudo-aléatoire sur une entrée x avec la clé maître.
- $\mathsf{EvalC}(K_C, x) \to y$: évalue la fonction sur l'entrée x avec la clé contrainte K_C.

Une CPRF est correcte si, pour toute clé K, toute contrainte C et toute entrée x telle que $C(x) = 1$, on a

$$\mathsf{EvalC}(K_C, x) = \mathsf{Eval}(K, x).$$

Autrement dit, la clé contrainte permet d'évaluer la PRF exactement sur les entrées autorisées.

2 Implémentation de la CPRF de BMO17

La CPRF de BMO17 est basée sur l'itération successive d'une permutation à trappe, qui est une fonction bijective, que l'on notera π.

Génération de la clé maîtresse

La clé maîtresse sera composé des éléments :

- $ST_0 \in \mathbb{Z}_N$
- PK une clé RSA pour avoir la permutation π_{PK}

Évaluation de la CPRF avec la clé maîtresse

Avec la clé maîtresse (ST_0, PK) et une entrée c, on peut évaluer la CPRF sur c :

$$F((PK, ST_0), c) = \pi_{PK}^{-c}(ST_0)$$

Génération de la clé contrainte

À partir de la clé maîtresse (ST_0, PK) et d'un entier n, la clé contrainte calculée sera composée des éléments :

- PK
- $ST_n = \pi_{PK}^{-n}(ST_0)$
- n

Évaluation de la CPRF avec la clé contrainte

Avec la clé contrainte (PK, ST_n, n) et une entrée c, on peut évaluer la CPRF si $c < n$:

$$F.Eval((PK, ST_n, n), c) = \pi_{PK}^{n-c}(ST_c)$$