

# Constrained Pseudorandom Functions, Revisited

Julian Mouthon, Mario Razafinony

## 1 Définitions

### Fonction pseudo-aléatoire (PRF)

Une fonction pseudo-aléatoire

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

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

### Contrainte

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

$$C(x) = 1 : \text{« l'entrée est autorisée »} \quad C(x) = 0 : \text{« l'entrée est interdite »}.$$

### CPRF

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

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

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

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