

Constrained Pseudorandom Functions, Revisited

Julian Mouthon, Mario Razafinony

January 23, 2026

Introduction

Ce projet s'inscrit dans le cadre de l'étude des fonctions pseudo-aléatoires contraintes (*Constrained Pseudorandom Functions*, CPRF), une extension des fonctions pseudo-aléatoires classiques permettant de restreindre les évaluations à un sous-ensemble d'entrées défini par une contrainte.

Dans un premier temps, nous présentons les notions fondamentales liées aux fonctions pseudo-aléatoires et aux CPRFs, ainsi que la construction proposée par Bost, Minaud et Ohrimenko en 2017 (BMO17).

Dans un second temps, nous nous intéressons aux travaux récents de Cheng et Jaeger en 2025 (CJ25), qui mettent en évidence une attaque contre cette CPRF et proposent une variante hachée assurant la sécurité dans un nouveau modèle.

Contents

1 Définitions	3
2 Construction de la CPRF de BMO17	3

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.

2 Construction de la CPRF de BMO17

La CPRF de BMO17 est basée sur l'itération successive d'une permutation à trappe, c'est-à-dire une fonction bijective facile à calculer mais difficile à inverser sans information secrète. On note cette permutation π .

Génération de la clé maîtresse

La clé maîtresse est composée des éléments suivants :

- $ST_0 \in \mathbb{Z}_N$, un état initial secret choisi aléatoirement
- SK , une clé secrète RSA définissant la permutation à trappe π_{SK}

La clé publique associée PK permet uniquement de calculer la permutation directe π .

Évaluation de la CPRF avec la clé maîtresse

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

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

L'évaluation consiste à appliquer c fois l'inverse de la permutation à partir de l'état initial ST_0 .

Génération de la clé contrainte

À partir de la clé maîtresse (ST_0, SK) et d'un entier n , correspondant à la contrainte $C(c) = [c < n]$, la clé contrainte est composée des éléments suivants :

- PK , la clé publique associée à la permutation π
- $ST_n = \pi_{SK}^{-n}(ST_0)$
- n

La clé secrète SK n'est pas incluse dans la clé contrainte.

Évaluation de la CPRF avec la clé contrainte

Avec la clé contrainte (PK, ST_n, n) et une entrée c , l'évaluation est possible uniquement si $c < n$. Dans ce cas, la valeur de la CPRF est calculée comme suit :

$$\text{EvalC}((PK, ST_n, n), c) = \pi_{PK}^{n-c}(ST_n)$$

Cette valeur est égale à $F((SK, ST_0), c)$ par construction, ce qui assure la correction du schéma.