

Constrained Pseudorandom Functions, Revisited

Julian Mounthon, Mario Razafinony

January 26, 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
Fonction pseudo-aléatoire	3
Contrainte	3
Fonction pseudo-aléatoire contrainte	3
2 Construction de la CPRF de BMO17	4
2.1 Propriétés	4
Clé maîtresse	4
Evaluation avec clé maîtresse	4
Clé contrainte	4
Évaluation avec clé contrainte	4
2.2 Implémentation	5
2.2.1 Permutation RSA	5
2.2.2 Clé maîtresse	5
2.2.3 Clé contrainte	5
3 L'attaque CJ25	5
3.1 Résumé	5
3.2 Jeu de sécurité	6
3.3 Implémentation	6
4 CPRF hachée de CJ25	6
4.1 Résumé	6
4.2 Implémentation	6
5 Une preuve sur une définition des CPRF	6

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

Une contrainte est un prédictat booléen

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

qui partitionne le domaine D en deux ensembles :

- les entrées *autorisées*, telles que $C(x) = 1$;
- les entrées *interdites* (ou contraintes), telles que $C(x) = 0$.

Intuitivement, la contrainte spécifie l'ensemble des entrées sur lesquelles une clé contrainte est autorisée à évaluer la fonction pseudo-aléatoire.

Ici, nous considérons principalement des contraintes de la forme

$$C_n(x) = [x < n],$$

qui autorisent toutes les entrées strictement inférieures à un seuil $n \in \mathbb{N}$.

Fonction pseudo-aléatoire contrainte (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

2.1 Propriétés

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 .

Evaluation 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.

2.2 Implémentation

Nous utilisons la bibliothèque OpenSSL pour la gestion des grands entiers (**BIGNUM**), les opérations modulaires et le calcul de hachage SHA-256.

L'aléa est sécurisé et est obtenu à partir de `/dev/urandom`, ce qui permet de générer l'état initial ST_0 ainsi que les paramètres RSA de manière sûre.

2.2.1 Permutation RSA

La permutation à trappe utilisée dans BMO17 est défini à l'aide de RSA. Nous implémentons la génération de clés RSA de taille 2048 bits, ainsi que l'évaluation de la permutation dans les deux sens.

Plus précisément, la fonction publique correspond à l'exponentiation modulaire

$$x \mapsto x^e \bmod N,$$

tandis que l'inverse de la permutation est calculé via l'exponentiation privée

$$x \mapsto x^d \bmod N.$$

Afin de limiter les fuites par canaux auxiliaires, l'évaluation privée est réalisée à l'aide de la fonction `BN_mod_exp_mont_consttime` d'OpenSSL, qui garantit un temps d'exécution indépendant des données secrètes.

2.2.2 Clé maîtresse

La clé maîtresse de la CPRF est composée d'un état initial secret ST_0 et d'une clé privée RSA. L'état initial est généré comme un entier aléatoire de 256 bits à partir de `/dev/urandom`.

L'évaluation avec la clé maîtresse consiste à appliquer c fois l'inverse de la permutation RSA à partir de ST_0 .

2.2.3 Clé contrainte

À partir de la clé maîtresse et d'un paramètre de contrainte n , nous dérivons une clé contrainte composée de la clé publique RSA (e, N) et de l'état

$$ST_n = \pi^{-n}(ST_0).$$

Cette clé permet ensuite d'évaluer la CPRF uniquement pour les entrées $c < n$ en appliquant $(n - c)$ fois la permutation publique à partir de ST_n . La clé privée n'est jamais incluse dans la clé contrainte, ce qui garantit que seules les évaluations autorisées sont possibles.

3 L'attaque CJ25

3.1 Résumé

L'attaque CJ25 exploite le fait qu'un attaquant peut recevoir des évaluations et évaluer en parallèle des entrées à partir de clés contraintes.

Plus précisément, l'adversaire commence par obtenir une évaluation de la fonction pseudo-aléatoire contrainte sur une entrée donnée x , c'est-à-dire une valeur $y = F(K, x)$.

Dans un second temps, il peut demander une ou plusieurs clés contraintes K_R telles que l'ensemble de contraintes R inclut l'entrée x . Avec une telle clé contrainte, il peut alors recalculer la valeur $y' = \text{EvalC}(K_R, x)$, et tester si $y' = y$.

Il est donc possible pour un attaquant de discerner les sorties réelles des sorties aléatoires de la CPRF.

3.2 Jeu de sécurité

3.3 Implémentation

4 CPRF hachée de CJ25

4.1 Résumé

4.2 Implémentation

5 Une preuve sur une définition des CPRF