Implémentations de Mitaka et MitakaZ

Nguyen Thi Thu Quyen

thi.nguyen@idemia.com

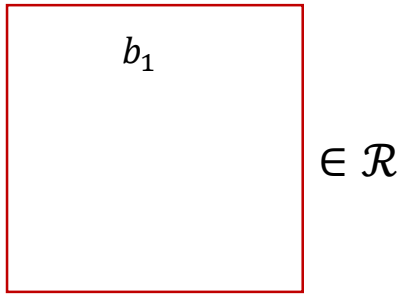
Contenu

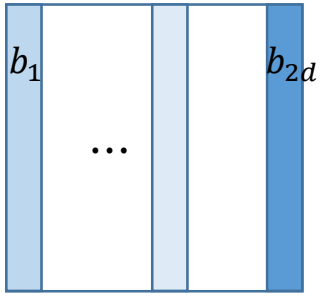
- Rappels de Falcon et Mitaka
- Implémentation existantes:
  - Falcon(python)
  - Mitaka(C)
- Nouvelles Implémentations (Sage)
  - Mitaka: sans FFT
  - MitakaZ
- Résumés

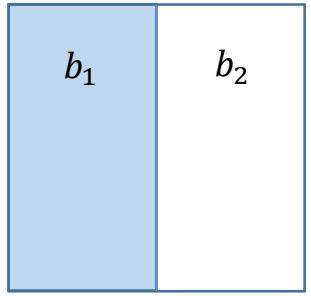
Falcon

Without FFO(Ducas, Prest 15)

Mitaka

$B =$  $\in \mathcal{R}$

$B =$  $\in \mathbb{Z}^{2d \times 2d}$

$B =$  $\in \mathcal{R}^{2\times 2}$

Sampling over ring $\mathcal{R}$

Peikert(m, σ, r):

$$x \hookleftarrow \sigma \cdot \mathcal{N}\left(0, \frac{1}{\sqrt{n}}\right)^d$$

$y \hookleftarrow D_{\mathcal{R},(m-x),r}$

$v = y$

Return $v \sim D_{m,s(\sigma,r)}$

+

Sampling over $\mathcal{L}(\boldsymbol{B}) \subset \mathbb{Z}^{2d}$

Klein$\left(\widetilde{B_Z} = (\widetilde{b_1}, \cdots, \widetilde{b_{2d}}), m, \sigma\right)$:

$v = 0, c = m$

for i $= 2d$ to 1:

$$\sigma_i = \frac{\sigma}{\left\|\widetilde{b_i}\right\|^2}$$

$$t_i = D_{\mathcal{L}, \frac{\langle c, \widetilde{b_i}\rangle}{\left\|\widetilde{b_i}\right\|^2}, \sigma_i}$$

$v = v + t_i b_i$

$c = c - t_i b_i$

Return $v = t_1 b_1 + \cdots t_{2d} b_{2d}$

$\sim D_{\mathcal{L},m,\Sigma_{Klein}}$

=

Sampling over $\boldsymbol{B\mathcal{R}^2} \subset \mathcal{R}^2$

Hybrid$\left(\widetilde{B_{\mathcal{R}}} = \left(\widetilde{b_1}, \widetilde{b_2}\right), m, \sigma, r\right)$:

$v = 0, c = m$

for i $= 2$ to 1:

$$\sigma_i = \sqrt{\frac{\sigma}{\langle \widetilde{b_i}, \widetilde{b_i}\rangle_{\mathcal{R}}} - r^2}$$

$$t_i = \textbf{Peikert}\left(\frac{\langle c, \widetilde{b_i}\rangle_{\mathcal{R}}}{\langle \widetilde{b_i}, \widetilde{b_i}\rangle_{\mathcal{R}}}, \sigma_i, r\right)$$

$v = v + t_i b_i$

$c = c - t_i b_i$

Return $v = t_1\, b_1 + t_2 b_2$

$\sim D_{\mathcal{L},m,\Sigma_{Hybrid}}$

Implémentations exitantes

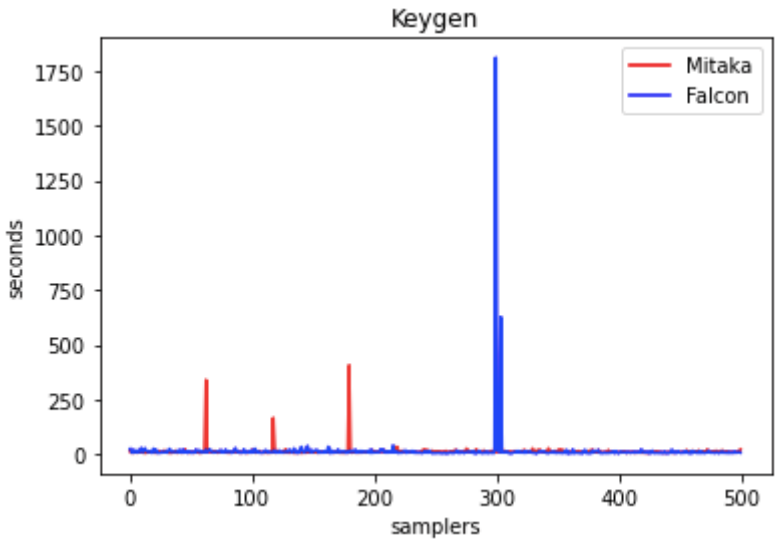
Falcon

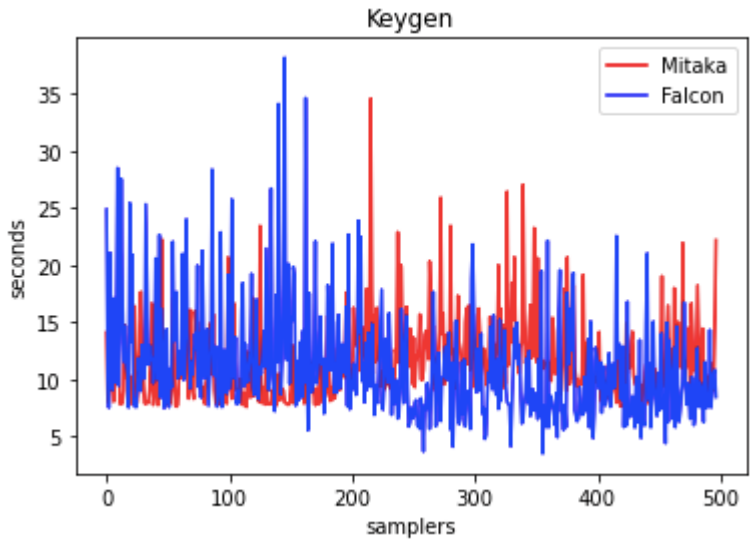
- Keygen
  - python
  - Re-échantilloner après chaque échec
- Sign
  - Python
  - FFO sur tour des anneaux

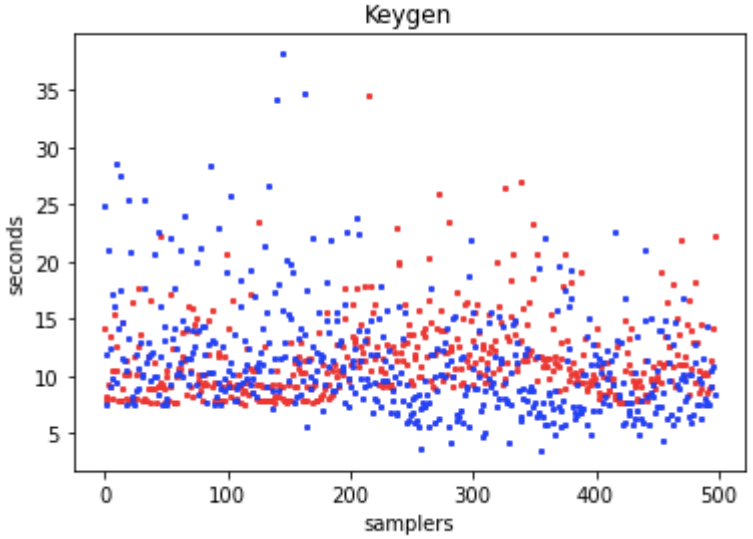
Mitaka

- Keygen
  - Sage
  - Réutiliser les échantillons
- Sign
  - C
  - Hybrid Sampler

Keygen = échantillonner (f,g)+calculer(F,G)







- Mitaka keygen a une borne inférieure visible (8s) mais le taux de succès au premier échantillonage est grand.
- Falcon keygen a une distribution assez étalée. La bore inférieure n'est que 2s => calculer(F,G) est meilleur mais échantillonner(f,g) est pire.

Réutliser des échantillonages est une bonne idée.

Sage en Python

- Taille: ~1GB
- Structures algébriques prédéfinies:
  - Corps cyclotomique
  - FFT
- Echantillonnages discrètes pré-implémenté:
  - Distribution gaussienne discrète sur Z/réseaux euclidien

Nouvelle implémentation de Mitaka

- Hybrid sampler sans FFT (multiplication polynomiale est utilisée)
- Problèmes:
  - Opérations algébriques dans corps quotient de Sage sont couteux.
  - Racine carré, inverse de polynôme nécessitent FFT
  - Sage ne peut pas calculer l'inverse de polynôme dans la grande dimension

Précalcul avec FFT est une bonne idée.

MitakaZ=HybridU+Offline integral pertubation

$c = (c_1, c_2) \in \mathcal{R}_{\mathbb{Q}}^2$
$U = [(1,0), (u, 1)] \in \mathcal{R}_{\mathbb{Q}}^{2\times 2}$

HybridU(U, c, r):
$z_2 \hookleftarrow \text{RingSampler}_{\mathbb{Z}}(c_2, r)$
$c_1' = c_1 - z_2 u$
$z_1 \hookleftarrow \text{RingSampler}_{\mathbb{Z}}(c_1', r)$
$z = U(z_1, z_2)$
Return $z \sim D_{\mathcal{L}(U),c,r}$

+

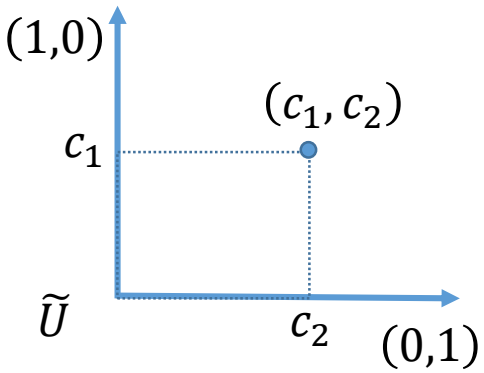
$a \in \mathbb{N}^*$
$A \in \mathcal{R}^{2\times m}, \Sigma = 1/a^2 AA^t + I.$

OffIntPer(A, a, L, r):
$x \hookleftarrow (D_{\mathbb{Z},Lr})^m$
$p' = \frac{1}{aL} Ax$
$p \hookleftarrow D_{\mathcal{R}^2,p',r}$
Return $p \sim D_{\mathcal{R}^2,r^2\Sigma}$

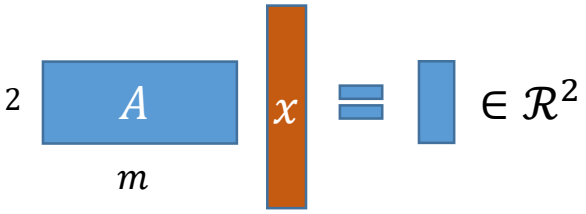
=

$\hat{B}U_{\hat{u}} = B = \tilde{B}U_u, \hat{u} = [u]_a$
$\Sigma_a = s^2 I - \hat{B}\hat{B}^t$
$A = \textbf{IntGram}(a^2(\Sigma_a - I))$

MitakaZ$(\hat{B}, A, c, r)$:
$p =$ **OffIntPer**(A, a, r)
$\hat{c} = \hat{B}^{-1}(c - p)$
$z' =$ **HybridU**$(U_{\hat{u}}, \hat{c}, s)$
$z = \hat{B}z'$
Return $z \sim D_{\mathcal{L}(B),c,rs}$



$\mathcal{R}^2$



Integral pertubation →

$AA^t = a^2(\Sigma_a - I)$

$p \sim D_{\mathcal{R}^2,r^2\Sigma_a}$

$z' \sim D_{\mathcal{L}(U_{\hat{u}}),\hat{c},s)}$

Implémentation de MitakaZ

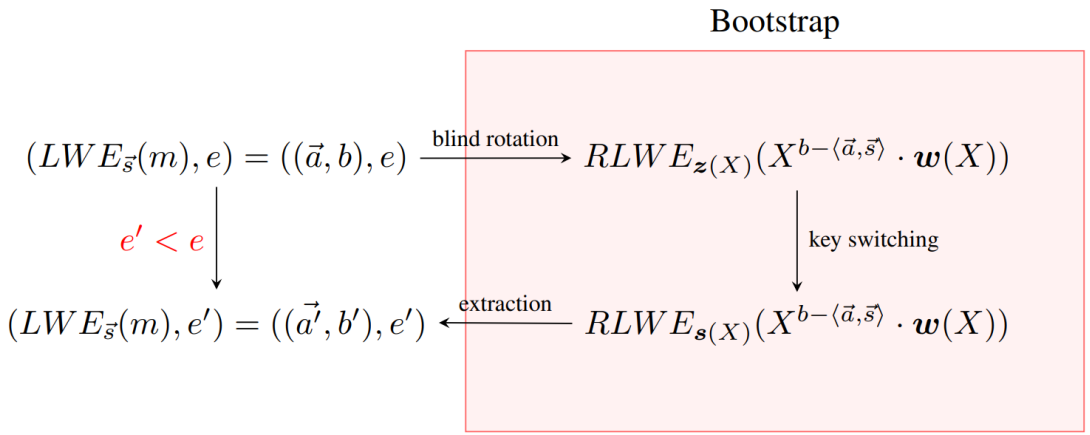
- HybridU sampler sans FFT marche correctement.
- Problèmes:
  - HybridU dans grande dimension est à tester.
  - La généralisation de trouver Matrice de perturbation (IntGram) sur l'anneau n'est pas prête pour l'implémentation.

Précalcul Matrice de perturbation avec FPA?

Résumés

Travaux réalisés

- Implémentations naives sur Sage
- Ecrire le rapport sur HE et le bootstrap (https://hal.archives-ouvertes.fr/hal-03676650)



Travaux à réliser

- Tester implémentations dans plus grande dimension.
- Regarder nouvelles directions pour contourner le IntGram dans MitakaZ.
- Regarder le rôle de q.