Fully homomorphic encryption (FHE) schemes

October 22, 2022

Khanh Nguyen

1 Section 1

Voici le problème direct que nous allons être amenés à résoudre à chaque itération de notre algorithme:

$$\begin{cases} u_t - Lu = \tilde{c}.\chi^{-1}.u + g & (x,t) \in Q \\ u(x,0) = 0 & x \in \Omega \\ Bu = b(x,t) & (x,t) \in S \end{cases} \tag{1}$$

On utilise exactement les mêmes notations que dans Prilepko & Kostin.

2 Section 2

2.1 Section 2.1

On rappelle la définition de l'opérateur A:

$$Ac = l(u_t(x,t,;c)) - L\chi - lg \tag{2}$$

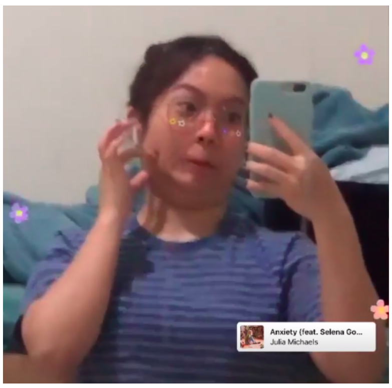

Figure 1: Thao Dien an cut

2.2 Section 2.2

- On initialise les constante Δt, $\delta > 0$ et $T = n * \Delta t$, la variable $i = 0$ et les fonctions $u^0 = 0$, $c(x) < 0$ et $\chi(x) > 0$.
- Tant que $\| lu^n - \chi \|_\infty > \delta$: (on ignore la condition à la première itération)
  - Pour i de 0 à $n - 1$:
    - On calcule u^{i+1} par résolution du problème direct
  - $c \leftarrow Ac$ pour $u = u^n$
- On renvoie la dernière valeur de c.