Représentation de Nombres pour les Algorithmes

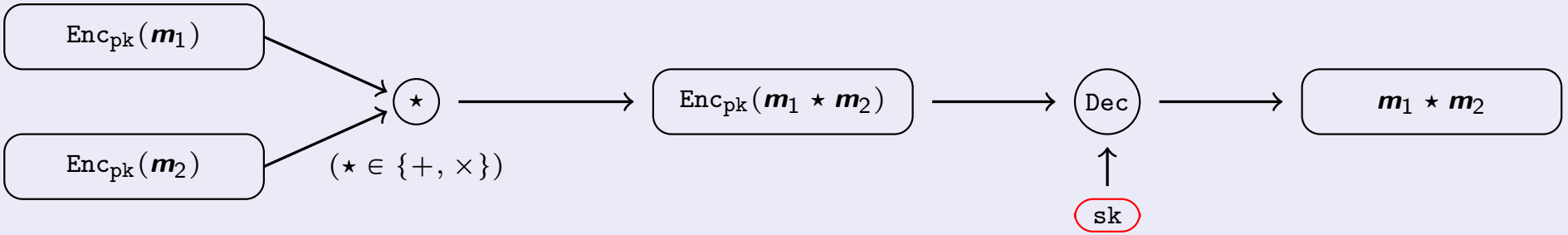
Présentation du Schéma de Chiffrement Somewhat Homomorphe de Fan and Vercauteren

Vincent Zucca

Année 2016-2017

Contexte

Chiffrement Homomorphe:



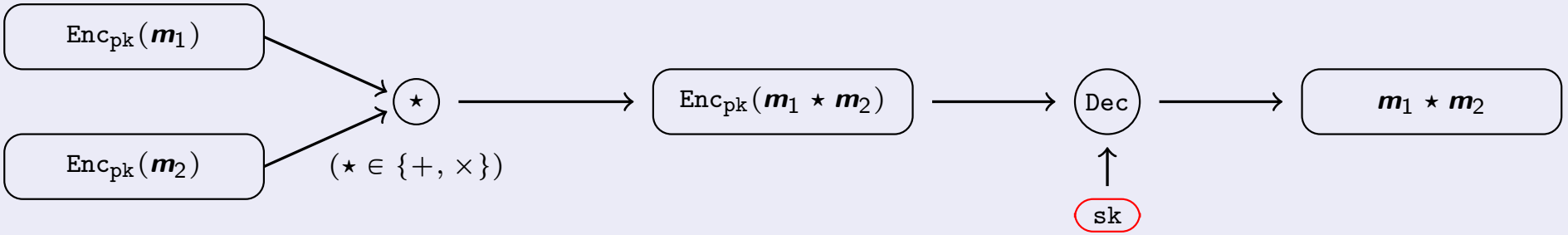
"Chiffrement Bruité"

- Chaque chiffré contient un bruit.
- Après chaque opération homomorphique le bruit grandit.
- Le déchiffrement reste correct tant que le bruit ne dépasse pas une certaine borne.
  $\Longrightarrow$ Nombre limité d'opérations.
  $\Longrightarrow$ Chiffrement "Somewhat" Homomorphe.

Problème : pas très efficace en pratique.

Contexte

Chiffrement Homomorphe:



"Chiffrement Bruité"

- Chaque chiffré contient un bruit.
- Après chaque opération homomorphique le bruit grandit.
- Le déchiffrement reste correct tant que le bruit ne dépasse pas une certaine borne.
  $\Longrightarrow$ Nombre limité d'opérations.
  $\Longrightarrow$ Chiffrement "Somewhat" Homomorphe.

But : accélérer l'arithmétique en utilisant des représentations adaptées.

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Représentation des données dans (FV)

Espace ambiant : $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$ avec $n = 2^h \geqslant 2$

$\Longrightarrow$ polynômes de degré inférieur à n à coefficients entiers

- t: le module des **clairs**, $\boldsymbol{m} \in \mathcal{R}_t = \mathcal{R}/t\mathcal{R}$ (coeff. modulo t)
- q: le module des **chiffrés** ($q >> t$), $\boldsymbol{c} \in \mathcal{R}_q \times \mathcal{R}_q$ (coeff. modulo q)

Probabilités sur $\mathcal{R}_q$

- $\mathcal{U}$ coeff. entiers tirés indép. et uniformément dans [-q/2,q/2[.
- χ_{key} coeff. uniforme et indép. dans un ensemble "étroit" ($\{-1, 0, 1\}$)
- χ_{err} coeff. tirés indép. selon un gaussienne discrète centrée en 0.

Notations

- $[x]_q$ est (x mod q) in $[-q/2, q/2[$ (reste centré),
- $|x|_q$ est (x mod q) in $[0, q[$ (reste de la division euclidienne).

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Génération des clés

1. tirer $\boldsymbol{s} \leftarrow \chi_{key}$
2. tirer $(\boldsymbol{a}, \boldsymbol{e}) \leftarrow \mathcal{U} \times \chi_{err}$
3. retourner
   - $\mathbf{pk} = (\boldsymbol{p_0}, \boldsymbol{p_1}) = ([-(\boldsymbol{as} + \boldsymbol{e})]_q, \boldsymbol{a})$ (Échantillon RLWE)
   - $\mathbf{sk} = \boldsymbol{s}$

Chiffrement

Données : $[\boldsymbol{m}]_t \in \mathcal{R}_t$ à chiffrer, clé publique $\mathbf{pk}$,

1. tirer $(\boldsymbol{e_1}, \boldsymbol{e_2}, \boldsymbol{u}) \leftarrow (\chi_{err})^2 \times \chi_{key}$
2. retourner $(\boldsymbol{c}_0, \boldsymbol{c}_1) = ([\Delta[\boldsymbol{m}]_t + \boldsymbol{p_0 u} + \boldsymbol{e_1}]_q, [\boldsymbol{p_1 u} + \boldsymbol{e_2}]_q)$ $(\Delta = \lfloor \frac{q}{t} \rfloor)$

Propriété : $[\boldsymbol{c}_0 + \boldsymbol{c}_1 \boldsymbol{s}]_q = \Delta[\boldsymbol{m}]_t + \boldsymbol{v} \pmod q$ avec $\boldsymbol{v}$ le "bruit" du chiffré

Remarque

- Un chiffré peut être vu comme un polynôme de degré 1 à coefficients dans $\mathcal{R}_q$. C'est à dire un polynôme dont les coefficients sont des polynômes.
- Évaluer un chiffré en la clé secrète $\boldsymbol{s}$, permet de révéler un multiple du message plus une "petite" erreur.

Application

On considère $\mathcal{R} = \mathbb{Z}[X]/(X^2+1)$, $q = 221$, $t = 2$.
Calculer le chiffré du message $\boldsymbol{m} = -X - 1$, avec $\mathbf{sk} = X - 1$ et $\mathbf{pk} = (83X + 62, 73X - 12)$ et déterminer le bruit v du message.
avec $u = -X$, $e_1 = -3$ et $e_2 = X$

Solution

$\boldsymbol{c} = (49X - 30, 13X + 73)$, $[\boldsymbol{c_0} + \boldsymbol{c_1 s}]_q = 109X + 105$, $v = -X - 5$

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Déchiffrement

Données : $(\boldsymbol{c_0}, \boldsymbol{c_1})$ un chiffré de $[\boldsymbol{m}]_t$, clé secrète $\boldsymbol{s}$.

Renvoie : $\left[\left\lfloor \frac{t}{q}[\boldsymbol{c_0} + \boldsymbol{c_1 s}]_q \right\rceil\right]_t$

Propriété : si le bruit $\boldsymbol{v}$ d'un chiffré $\boldsymbol{c}$ d'un message $[\boldsymbol{m}]_t$ satisfait :

$$\|\boldsymbol{v}\|_\infty \leqslant \frac{\Delta - |q|_t}{2}$$

Alors la fonction de déchiffrement renverra bien $[\boldsymbol{m}]_t$.

Remarque : plus Δ est grand plus la borne est grande.

Application

Vérifier que le chiffré précédent se déchiffre bien correctement. On rappelle que $\boldsymbol{c} = (49X - 30, 13X + 73)$, $\boldsymbol{s} = X - 1$ et $\boldsymbol{m} = -X - 1$.

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Addition

Données : deux messages chiffrés avec $\boldsymbol{pk}$, $\boldsymbol{c}^1 = (\boldsymbol{c}_0^1, \boldsymbol{c}_1^1)$, $\boldsymbol{c}^2 = (\boldsymbol{c}_0^2, \boldsymbol{c}_1^2)$
Renvoie : $\boldsymbol{c_{add}} = (\boldsymbol{c}_0^1 + \boldsymbol{c}_0^2, \boldsymbol{c}_1^1 + \boldsymbol{c}_1^2)$

Propriété : l'algorithme ci-dessus retourne bien un chiffré de $\boldsymbol{m}_1 + \boldsymbol{m}_2$.
Quel impact sur le bruit ?

$$\Longrightarrow \quad \|v_{add}\|_\infty \leqslant \|v_1\|_\infty + \|v_2\|_\infty .$$

Application

Additionner le chiffré précédent avec $\boldsymbol{c}' = (-37X - 31, 19X - 51)$.
Vérifier que la somme des deux chiffrés déchiffre bien en $\boldsymbol{m} = -1$.

Solution

$\boldsymbol{c_{add}} = (12X - 61, 32X + 22)$

$$\left\lfloor \frac{t}{q} \cdot [\boldsymbol{c_{add}}_0 0 + \boldsymbol{c_{add}}_1 \boldsymbol{s}]_q \right\rceil = \left\lfloor \frac{4}{221} \right\rceil \cdot X + \left\lfloor \frac{212}{221} \right\rceil = 1$$

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Multiplication homomorphique de (c_0, c_1) by (c'_0, c'_1)

Version Naïve

1. Calcule le produit $(\tilde{c}_0, \tilde{c}_1, \tilde{c}_2) = (c_0 c'_0, c_0 c'_1 + c'_0 c_1, c_1 c'_1)$ dans $\mathbb{Z}$
2. Normalisation + Arrondi : $\hat{c}_i = \left[\lfloor \frac{t}{q} \cdot \tilde{c}_i \rceil \right]_q$

$$\rightsquigarrow [\hat{c}_0 + \hat{c}_1 s + \hat{c}_2 s^2]_q = \Delta [m_1 m_2]_t + v'' \bmod q$$

3. Relinéarisation: $([\hat{c}_0 + \hat{c}_2 s^2]_q, \hat{c}_1) \to ([\hat{c}_0 + \hat{c}_2(s^2 + e + as)]_q, [\hat{c}_1 - a\hat{c}_2]_q)$

Remarque : on ne peut pas révéler s donc on fournit une clé d'évaluation qui est quasiment un chiffré de s^2 :

$$evk = ([s^2 + e + as]_q, -a) \text{ avec } a \leftarrow \chi_{key} \text{ et } e \leftarrow \chi_{err}.$$

Problème :

- Le terme $\hat{c}_2 \times e$ se rajoute au bruit.
- $\|\hat{c}_2 \times e\|_\infty \leqslant n \|\hat{c}_2\|_\infty \|e\|_\infty \leqslant n \frac{q}{2} \mathcal{B}_{err}$

  $\Longrightarrow$ Le message ne déchiffrera pas correctement.

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Solution : décomposer $\hat{\boldsymbol{c}}_2$ en base $\omega > 2$.

Plus précisemment...

Soit ω un entier plus grand que 2, $\ell_{\omega,q} = \lfloor \log_\omega(q) \rfloor + 1$ et $\boldsymbol{a} \in \mathcal{R}_q$, on définit les fonctions suivantes :

$$\mathcal{D}_{\omega,q}(\boldsymbol{a}) = ([\boldsymbol{a}]_\omega, [\lfloor \boldsymbol{a}\omega^{-1} \rfloor]_\omega, \cdots, [\lfloor \boldsymbol{a}\omega^{-(\ell_{\omega,q}-1)} \rfloor]_\omega) \in \mathcal{R}_q^{\ell_{\omega,q}}$$

$$\mathcal{P}_{\omega,q}(\boldsymbol{a}) = ([\boldsymbol{a}]_q, [\boldsymbol{a}\omega]_q, \cdots, [\boldsymbol{a}\omega^{(\ell_{\omega,q}-1)}]_q) \in \mathcal{R}_q^{\ell_{\omega,q}}$$

Lemme : pour tout $(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{R}_q^2$ on a : $\langle \mathcal{D}_{\omega,q}(\boldsymbol{b}), \mathcal{P}_{\omega,q}(\boldsymbol{b}) \rangle \equiv ab\ [q]$.

Et donc...

- On modifie la clé d'évaluation en :
  $\boldsymbol{evk} = ([\mathcal{P}_{\omega,q}(\boldsymbol{s}^2) + \vec{\boldsymbol{e}} + \vec{\boldsymbol{a}}\,\boldsymbol{s}]_q, -\vec{\boldsymbol{a}})$ avec $(\vec{\boldsymbol{a}}, \vec{\boldsymbol{e}}) \leftarrow \chi_{key}^{\ell_{\omega,q}} \times \chi_{err}^{\ell_{\omega,q}}$.
- On calcule $([\hat{\boldsymbol{c}}_0 + \langle \mathcal{D}_{\omega,q}(\hat{\boldsymbol{c}}_2), \boldsymbol{evk}_0 \rangle]_q, [\hat{\boldsymbol{c}}_1 + \langle \boldsymbol{evk}_1, \mathcal{D}_{\omega,q}(\hat{\boldsymbol{c}}_2) \rangle]_q)$

Remarque : $\| \langle \mathcal{D}_{\omega,q}(\hat{\boldsymbol{c}}_2), \vec{\boldsymbol{e}} \rangle \|_\infty \leqslant n\ell_{\omega,q}\frac{\omega}{2}\mathcal{B}_{err}$.

Schéma de Chiffrement FV (Fan et Vercauteren, 2012)

Application :

On donne $\omega = 4$, $evk_0 = (X - 2, -8X + 1, -32X + 2, 92X)$ et $evk_1 = (-1, 0, X, -X + 1)$. Calculer le produit des chiffrés $\boldsymbol{c} = (49X - 30, 13X + 73)$ et $\boldsymbol{c}' = (-37X - 31, 19X - 51)$.

Solution

- $\hat{\boldsymbol{c}}_{\boldsymbol{mult}} = (-409X + 2743, -6173X - 1183, 724X - 3970)$
- $\left[\left[\frac{t}{q} \cdot \hat{\boldsymbol{c}}_{\boldsymbol{mult}}\right]\right]_q = (-4X + 25, -56X - 11, 7X - 36)$
- $\mathcal{D}_{\omega,q}(7X - 36) = (-X, -2X - 1, X - 2, 0)$
- $\langle \mathcal{D}_{\omega,q}(7X - 36), \boldsymbol{evk}_0 \rangle = 74X + 12$
- $\langle \boldsymbol{evk}_1, \mathcal{D}_{\omega,q}(7X - 36) \rangle = -X - 1$
- $\boldsymbol{c}_{\boldsymbol{mult}} = (70X + 37, -57X - 12)$

Sécurité du Schéma

Pour que le RLWE soit difficile il faut que n et q soit suffisemment grand pour qu'on ne puisse pas attaquer la clé par force brute (i.e. essayer toutes les possibilités).

Paramètres

Voici quelques exemples de paramètres pour 80 bits de sécurité :

- $n = 2048$, $\log_2(q) = 95$, $L = 2$
- $n = 4096$, $\log_2(q) = 190$, $L = 6$
- $n = 8192$, $\log_2(q) = 390$, $L = 13$
- $n = 16384$, $\log_2(q) = 780$, $L = 25$

Les calculs vont devenir très vite très coûteux. Il s'agit de trouver des représentations des éléments du schéma nous permettant de faire les calculs aussi vite que possible.