KANE Seyni

Master 2 ACC / Paris 8
DM 2 Interaction Codes-Cryptographie
Prof: Borello Martino
15 Novembre 2022

DM 2: Attaque de Sidelnikov et Shestakov sur le cryptosystème de McEliece

---

Dans ce DM ils nous est donné d'étudier et d'implémenter l'attaque de Sidelnikov et Shestakov sur une variation du cryptosystème de McEliece employant des codes de Reed-Solomon généralisés.

Un code de Reed-Solomon généralisé peut être définit comme suit.

Definition Un code de Reed-Solomon généralisé de longueur n et dimension k, associé à α et β, est donnée par

$$GRS_{n,k}(\alpha, \beta) \overset{\text{def}}{=} \{(\beta_1 p(\alpha_1), \ldots, \beta_n p(\alpha_n)) | p(x) \in \mathbb{F}_q[x], deg(p(x)) < k\}.$$

Maintenant nous allons expliquer le principe de l'attaque.

Principe de l'attaque En résumé l'attaque est étant donné une matrice "brouillée" G' (avec $G' = SGP$, S un matrice inversible et P une matrice de permutation) retrouver α et β.
Plus précisément, on veut récupérer des permutés $\alpha' = \alpha P$ et $\beta' = \beta P$, de manière que GP soit la matrice génératrice canonique de $GRS_{n,k}(\alpha', \alpha')$.

On peut supposer $\alpha'_1 = 0, \alpha'_2 = 1$.

Pour calculer les α'. on a que $G' = [A|B]$ avec A une matrice $k \times k$ inversible. On multiplie par A^{-1} et on obtient

Chaque ligne $b_1, \ldots, b_k$ de B correspond à un polynôme $p_{b_i}(x)$ dans $\mathbb{F}_q[x]$ de degré au plus $k - 1$. De plus, puisque la matrice est en forme systématique, on a $p_{b_i}(\alpha'_j) = 0$ pour tout $j \in \{1, dots, k\}$, $j \neq i$, de manière que

$$p_{b_i}(x) = c_{b_i} \textstyle\prod_{j=1, j \neq i}^{k} (x - \alpha'_j), c_{b_i} \in \mathbb{F}_q$$

Puisque le code est MDS, on a $b_{i,j} \neq 0$ pour tout $k + 1 \leq j \leq n$ et tout $2 \leq i \leq k$, de manière que la quantité suivante soit bien définit

$$\mu_{i,j} \overset{\text{def}}{=} \tfrac{b_{1,j}}{b_{i,j}} = \tfrac{c_{b_1}(\alpha'_j - \alpha'_i)}{c_{b_i}\alpha'_j}.$$

On pose $\lambda_i \overset{\text{def}}{=} \frac{c_{b_1}}{c_{b_i}}$, on a

$$\mu_{2,j} = \lambda_2(1 - (\alpha'_j) - 1)$$

donc

$$\alpha'_j = \tfrac{\lambda_2}{\lambda_2 - \mu_{2,j}} \ (*) \text{ pour tout } k + 1 \leq j \leq n$$

KANE Seyni
kaneseyni.sn@gmail.com

Pour les autres indices, on a,

$$\mu_{i,k+1}\alpha'_{k+1} = \lambda_i(\alpha_k + 1 - \alpha'_i)\mu_{i,k+2}\alpha'_{k+2} = \lambda_i(\alpha_k + 2 - \alpha'_i)$$

$$\begin{cases} \mu_{i,k+1}\alpha'_{k+1} = \lambda_i(\alpha_k + 1 - \alpha'_i) \\ \mu_{i,k+2}\alpha'_{k+2} = \lambda_i(\alpha_k + 2 - \alpha'_i) \end{cases}$$

on obtient

$$\alpha'_i = \frac{\alpha_{k+1}\alpha_{k+2}(\mu_{i,k+1} - \mu_{i,k+2})}{\mu_{i,k+1}\alpha_{k+1} - \mu_{i,k+2}\alpha_{k+2}} \quad (**)$$

pour tout $3 \leq i \leq k$.

Ici on aura pas besoin de calculer le β', car on a $\beta = (1...1)$.

Problème Vue que la quantité lam_2 est a deviné dans $\mathbb{F}_q$. Ce qui pose parfois problème est qu'on peut tomber sur mauvaise valeur.

En effet dans la formule $(*)$ λ_2 doit être différent de $\mu_{2,j}$ pour tout $k+1 \leq j \leq n$, et de plus la valeur de lam_2 choisit doit être de sorte que $\forall i \neq j \alpha_i \neq \alpha_j$.

References :

1 Polycopié Borello Martino https://www.math.univ-paris13.fr/~borello/interactionscodescrypto/20222023/interactions-codes-crypto.html