TD3 - MPC-in-the-Head

Responsable : M. Bombar

1 Comportement Malicieux et Évaluation de Circuit

On considère un protocole à 3 joueurs d'évaluation de circuit arithmétique avec sécurité passive (*i.e.*, contre des adversaires semi-honnêtes). Par exemple, BGW ou GMW comme vus dans le cours.

On suppose que les trois joueurs P_1, P_2, P_3 cherchent à calculer $f(x_1, x_2, x_3) \stackrel{\text{def}}{=} x_1 x_2 x_3$.

(Q1) Dérouler le protocole BGW sur le calcul de f sur $\mathbb{F}_5$.

(Q2) Montrer que si P_1 joue un adversaire **actif** (c'est-à-dire que s'il ne respecte pas le protocole entièrement) il peut apprendre x_3.

(Q3) En déduire que BGW à 3 joueurs ne peut pas être sécurisé contre des adversaires malicieux.

2 Syndrome Decoding in the Head

Cet exercice est adapté de [FJR22].

Soit $\mathbb{F}_q$ un corps fini. On rappelle que le poids de Hamming d'un vecteur $\mathbf{v} \in \mathbb{F}_q^n$ est défini comme le nombre de coordonnées non nulles :

$$|\mathbf{v}| \stackrel{\text{def}}{=} |\mathbf{Supp}(\mathbf{v})| = |\{i \mid v_i \neq 0\}|.$$

La sphère de Hamming de rayon w (*i.e.*, l'ensemble des mots de poids w) de l'espace $\mathbb{F}_q^n$ est notée $\mathcal{S}_{n,w}$.

On définit alors le problème de décodage de la façon suivante :

Données Une matrice $\mathbf{H} \leftarrow \mathbb{F}_q^{(n-k)\times n}$, un vecteur $y \in \mathbb{F}_q^{n-k}$ et un entier $w \in \{1, \ldots, n\}$.

Problème Trouver un vecteur $\mathbf{x} \in \mathbb{F}_q^n$ tel que $y = \mathbf{Hx}$ **et** $|\mathbf{y}| = w$.

Pour des paramètres bien choisis, ce problème admet une solution avec très bonne probabilité [1], et est considéré comme extrêmement difficile, y compris pour un adversaire

1. On va supposer qu'il en existe effectivement une

quantique[2]. En particulier, la fonction syndrome

$$\begin{cases} \mathcal{S}_{n,w} & \to & \mathbb{F}_q^{n-k} \\ \mathbf{x} & \mapsto & \mathbf{y} \stackrel{\text{def}}{=} \mathbf{H} \cdot \mathbf{x} \end{cases}$$

est un bon candidat pour définir un schéma de signature de type MPC-in-the-Head. L'objectif de cet exercice est de définir un protocole de MPC à N joueurs permettant de prouver la connaissance d'un tel $\mathbf{x}$. Puisque $\mathbf{z} \mapsto \mathbf{H} \cdot \mathbf{z}$ est linéaire, on peut aisément utiliser un (n, n)-partage de secret linéaire (pour $\mathbf{x}$). La principale difficulté sera alors de prouver la contrainte non linéaire $|\mathbf{x}| \leq w$.

Dans la suite, on se fixe $\mathbb{K}$ une extension de $\mathbb{F}_q$ telle que $N \stackrel{\text{def}}{=} |\mathbb{K}| \geq n$, et soit $\gamma_1, \ldots, \gamma_N$ une énumération des éléments de $\mathbb{K}$. On pose $F \stackrel{\text{def}}{=} \prod_{i=1}^{n}(X - \gamma_i) \in \mathbb{K}[X]$.

(Q4) Soit $\mathbf{x} \in \mathbb{F}_q^n$ et $E \subset \{1, \ldots, n\}$ contenant le support de $\mathbf{x}$. On définit $Q(X) \stackrel{\text{def}}{=} \prod_{i \in E}(X - \gamma_i)$ et soit $S \in \mathbb{K}[X]$ le polynôme interpolateur de Lagrange des x_i en les $(\gamma_i)_{1 \leq i \leq n}$. Montrez que F divise $Q \cdot S$.

(Q5) Soit $\mathbf{x} \in \mathbb{F}_q^n$ de poids $|\mathbf{x}| \leq w$. En déduire qu'il existe un polynôme P de degré au plus $w - 1$ et un polynôme Q de degré w tels que

$$Q \cdot S = P \cdot F. \tag{1}$$

(Q6) Soit $\mathbb{L}$ une extension finie de $\mathbb{K}$. Montrez que si l'Équation 1 n'est pas vérifiée, alors

$$\mathbb{P}_{r \leftarrow \mathbb{L}}\left(Q(r) \cdot S(r) = P(r) \cdot F(r)\right) \leq \frac{n + w - 1}{|\mathbb{L}|}.$$

Remarque 1. *La propriété démontrée dans la question précédente permet de tester une égalité de polynômes en l'évaluant en un* ***unique*** *point, tiré uniformément sur un domaine suffisamment grand. Elle se généralise à des polynômes multivariés sous le nom de Lemme de Schwartz-Zippel.*

Partage d'un Polynôme Soit $M \in \mathbb{K}[X]$ un polynôme de degré au plus d. Un partage de secret de M est simplement la donnée de polynômes $[\![M]\!]_i$ de degré au plus d, et uniformément distribués, conditionnés à la relation

$$M = \sum_{i=1}^{N} [\![M]\!]_i.$$

2. Je vous renvoie à votre cours de cryptographie post-quantique

(Q7) On suppose que les parties $\mathcal{P}_1, \ldots, \mathcal{P}_N$ ont obtenu un partage linéaire $[\![\mathbf{x}]\!]_i$ de l'entrée $\mathbf{x}$. Soit $r \in \mathbb{L}$. Montrer que $\mathcal{P}_i$ peut **localement** calculer sa part $[\![S(r)]\!]_i$, où S est le polynôme défini précédemment.

(Q8) On suppose que le joueur $\mathcal{P}_i$ possède des parts $[\![Q]\!]_i$, et $[\![P]\!]_i \in \mathbb{K}[X]$. Soit $r \in \mathbb{L}$. Montrer que $\mathcal{P}_i$ peut calculer localement ses parts $[\![Q(r)]\!]_i$ et $[\![(F \cdot P)(r)]\!]_i$.

On suppose que les joueurs se partagent un triplet de Beaver $(a, b, c \stackrel{\text{def}}{=} a \cdot b)$ et on considère le protocole de MPC suivant [BN20] :

— Les joueurs choisissent ensemble un élément $\varepsilon \leftarrow\!\!\leftarrow \mathbb{L}$ (par exemple donné par une tierce partie).

— Chaque joueur définit localement

$$[\![\alpha]\!] \stackrel{\text{def}}{=} \varepsilon \cdot [\![\mathbf{x}]\!] + [\![a]\!] \quad \text{et} \quad [\![\beta]\!] \stackrel{\text{def}}{=} [\![S(r)]\!] + [\![b]\!].$$

— Les joueurs broadcast $[\![\alpha]\!]$ et $[\![\beta]\!]$.

— Les joueurs définissent localement

$$[\![v]\!] \stackrel{\text{def}}{=} \varepsilon \cdot [\![(F \cdot P)(r)]\!] - [\![c]\!] + \alpha \cdot [\![b]\!] + \beta \cdot [\![a]\!] - \alpha \cdot \beta.$$

— Les joueurs broadcast $[\![v]\!]$ et reçoivent alors tous v.

(Q9) Que calcule ce protocole ? Différenciez le cas où l'équation 1 est vraie de celui où elle ne l'est pas.

(Q10) En déduire un protocole π à N parties dans lequel $\mathcal{P}_i$ a une entrée de la forme $([\![x]\!], [\![Q]\!], [\![P]\!])$ et qui permet de déterminer si cette entrée forme bien un partage de secret d'une solution au problème de décodage d'instance (H, y), publique. On pourra supposer que les joueurs disposent en plus d'un triplet de Beaver $([\![a]\!], [\![b]\!], [\![a \cdot b]\!])$ et de deux points r et ε tirés uniformément dans $\mathbb{L}$.

(Q11) Quelle est la probabilité que π accepte si l'entrée est correcte ?

(Q12) Quelle est la probabilité p que π accepte si l'entrée est incorrecte ?

(Q13) En déduire une preuve zero-knowledge de type MPC-in-the-Head dont l'erreur de *soundness* est de la forme $p + (1 - p) \cdot \dfrac{1}{N}$.

Références

[BN20] Carsten Baum et Ariel Nof. "Concretely-Efficient Zero-Knowledge Arguments for Arithmetic Circuits and Their Application to Lattice-Based Cryptography". In : *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part I*. Sous la dir. d'Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden et Vassilis Zikas. T. 12110. Lecture Notes in Computer Science. Springer, 2020, p. 495-526.

[FJR22] Thibauld Feneuil, Antoine Joux et Matthieu Rivain. "Syndrome Decoding in the Head : Shorter Signatures from Zero-Knowledge Proofs". In : *IACR Cryptol. ePrint Arch.* (2022), p. 188.