Problem 2. «Sharing»

Bob is interested in studying mathematical countermeasures to side-channel attacks on block ciphers. He found out that techniques such as special sharings of functions can be applied against such attacks. Now he is thinking about the following mathematical problem in this approach.

Let $\mathcal{F}$ denote the set of **invertible functions** (**permutations**) from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$ and $\mathcal{F}^n$ denote the set of invertible functions from $(\mathbb{F}_2^4)^n$ to $(\mathbb{F}_2^4)^n$. Let $F \in \mathcal{F}^n$ be

$$F(x_1, x_2, \ldots, x_n) = (F_1(x_1, x_2, \ldots, x_n), F_2(x_1, x_2, \ldots, x_n) \ldots, F_n(x_1, x_2, \ldots, x_n)),$$

with component functions $F_i : (\mathbb{F}_2^4)^n \to \mathbb{F}_2^4$, $i = 1, \ldots, n$.

For any $f \in \mathcal{F}$, a function $F \in \mathcal{F}^n$ is called a **sharing** of f if

$$\sum_{i=1}^{n} F_i(x_1, x_2, \ldots, x_n) = f\left(\sum_{i=1}^{n} x_i\right) \quad \text{for all} \quad (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_2^4)^n.$$

Moreover, F is a **non-complete** sharing of f if F is a sharing of f with the additional property that each component function F_i is independent of x_i.

Bob needs your help to study functions for which a non-complete sharing exists. Find answers to the following questions!

Q1 Let $\mathcal{A}$ denote the set of **affine functions** from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$. Two functions $f, g \in \mathcal{F}$ are **affine equivalent** if there exist $a, b \in \mathcal{A}$ such that $g = b \circ f \circ a$.

Let f, g be two functions in the same affine equivalence class of $\mathcal{F}$ and let F be a non-complete sharing of f. Derive from F a non-complete sharing for g.

All functions of the same affine equivalence class have the same degree. It is known [1] that this equivalence relation divides $\mathcal{F}$ into 302 classes: 1 class corresponds to $\mathcal{A}$, 6 classes contain quadratic functions, 295 classes contain cubic functions.

Also, Bob knows that when $n \geqslant 5$, there exists a non-complete sharing for each $f \in \mathcal{F}$ (it can be shown by construction). When $n = 2$ a non-complete sharing exists only for the functions in $\mathcal{A}$. When $n = 3$, non-complete sharings exist for $\mathcal{A}$ and also for 5 out of the 6 equivalence classes containing quadratic functions. When $n = 4$, non-complete sharings exist for $\mathcal{A}$, for all 6 quadratic equivalence classes and for 5 cubic classes.

Q2 **Bonus problem (extra scores, a special prize!)**

Find a concise mathematical property that a function $f \in \mathcal{F}$ must have in order that a non-complete sharing F exists for $n = 3, 4$.

Q3 **Bonus problem (extra scores, a special prize!)**

Generalize to functions over $\mathbb{F}_2^5$, $\mathbb{F}_2^6$.

[1] C. De Canni‘ere. Analysis and Design of Symmetric Encrytption Algorithms, Ph.D. thesis, 2007.