Problem 4. «Weaknesses of the PHIGFS»

A young cryptographer Philip designs a family of lightweight block ciphers based on a 4-line type-2 Generalized Feistel scheme (GFS) with better diffusion effect.

Its block is divided into four m-bit subblocks, $m \geqslant 1$. For better diffusion effect, Philip decides to use a (4×4)-matrix A over $\mathbb{F}_{2^m}$ instead of a standard subblocks shift register in each round. The family $\text{PHIGFS}_\ell(A, b)$ is parameterized by a non-linear permutation $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, the matrix A and the number of rounds $\ell \geqslant 1$. The one-round keyed transformation of $\text{PHIGFS}_\ell(A, b)$ is a permutation g_k on $\mathbb{F}_{2^m}^4$ defined as:

$$g_k(x_3, x_2, x_1, x_0) = A \cdot (x_3, x_2 \oplus b(x_3 \oplus k_1), x_1, x_0 \oplus b(x_1 \oplus k_0))^T,$$

where $x_0, x_1, x_2, x_3 \in \mathbb{F}_{2^m}$, $k = (k_1, k_0)$ is a $2m$-bit round key, $k_0, k_1 \in \mathbb{F}_{2^m}$.

The ℓ-round encryption function $f_{k^{(1)},\ldots,k^{(\ell)}}\colon \mathbb{F}_{2^m}^4 \to \mathbb{F}_{2^m}^4$ under a key $(k^{(1)}, \ldots, k^{(\ell)}) \in \mathbb{F}_{2^m}^\ell$ is given by

$$f_{k^{(1)},\ldots,k^{(\ell)}}(\mathbf{x}) = g_{k^{(\ell)}} \ldots g_{k^{(1)}}(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{F}_{2^m}^4.$$

For effective implementation and security, Philip chooses two binary matrices A', A'' with the maximum branch number among all binary matrices of size 4, where

$$A' = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad A'' = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

For approval, he shows the cipher to his friend Antony who claims that A', A'' are bad choices because ciphers $\text{PHIGFS}_\ell(A', b)$, $\text{PHIGFS}_\ell(A'', b)$ are insecure against distinguisher attacks for all $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $\ell \geqslant 1$.

Help Philip to analyze the cipher $\text{PHIGFS}_\ell(A, b)$. Namely, for any $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and any $\ell \geqslant 1$, show that $\text{PHIGFS}_\ell(A, b)$ has

(a) ℓ-round differential sets with probability 1;
(b) ℓ-round impossible differential sets;

for the following cases: **Q1** $A = A'$; and **Q2** $A = A''$. In each case, construct these nontrivial differential sets and prove the corresponding property.

Turn to the next page.

Remark. Let us recall the following definitions.

- Let $\delta, \varepsilon \in \mathbb{F}_{2^n}$ be fixed nonzero input and output differences. The *differential probability* of $s\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as
$$p_{\delta,\varepsilon}(s) = 2^{-n} \cdot \left|\{\alpha \in \mathbb{F}_{2^n} | s(\alpha \oplus \delta) \oplus s(\alpha) = \varepsilon\}\right|.$$
- If $s\colon \mathbb{F}_{2^n} \times K \to \mathbb{F}_{2^n}$ depends on a key space K, then the *differential probability* of s is defined as
$$p_{\delta,\varepsilon}(s) = |K|^{-1} \sum_{k \in K} p_{\delta,\varepsilon}(s_k),$$
where $s(x, k) = s_k(x)$, $x \in \mathbb{F}_{2^n}$, $k \in K$.
- Let $\Omega, \Delta \subseteq \mathbb{F}_{2^n} \backslash \{0\}$ and Ω, Δ are nonempty. If $p_{\delta,\varepsilon}(s) = 0$ for any $\delta \in \Omega$, $\varepsilon \in \Delta$, then (Ω, Δ) are *impossible differential sets*. But if
$$\sum_{\delta \in \Omega, \varepsilon \in \Delta} p_{\delta,\varepsilon}(s) = 1,$$
then (Ω, Δ) are *differential sets with probability* 1. We call (Ω, Δ) trivial (impossible) differential sets if $\Omega \in \{\emptyset, \mathbb{F}_{2^n} \backslash \{0\}\}$ or $\Delta \in \{\emptyset, \mathbb{F}_{2^n} \backslash \{0\}\}$.