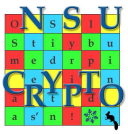

Problem 3. «Quadratic functions»

Alice and Bob are going to use the following pseudorandom binary sequence $u = \{u_i\}$, $u_i \in \mathbb{F}_2$:

- $u_1, \ldots, u_n$ are initial values;
- $u_{i+n} = f(u_i, u_{i+1}, \ldots, u_{i+n-1})$, where

$$f \in Q_n = \{a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1 \le i < j \le n} a_{ij} x_i x_j \mid a_0, a_i, a_{ij} \in \mathbb{F}_2\}.$$

Suppose that you have intercepted the elements $u_t, u_{t+1}, \ldots, u_{t+k-1}$ of a sequence for some t. Is it possible to uniquely reconstruct the elements

$$u_{t+k}, u_{t+k+1}, u_{t+k+2}, \ldots$$

provided $k \leqslant cn$, where c is a constant independent on n?