Cryptographie

26 septembre 2023

1 Prange

$t \in [0, n' - n/q]$

1. Répéter:

$$\pi \leftarrow S_n$$

$$H' \leftarrow \pi(H)$$

$$H'' \leftarrow \textit{Elimination Gaussienne sur les lignes de } H'$$

$H'' = R||Id_{n-t}$, $e'' = \pi(e)$

2. On suppose que $e''_k = 0$