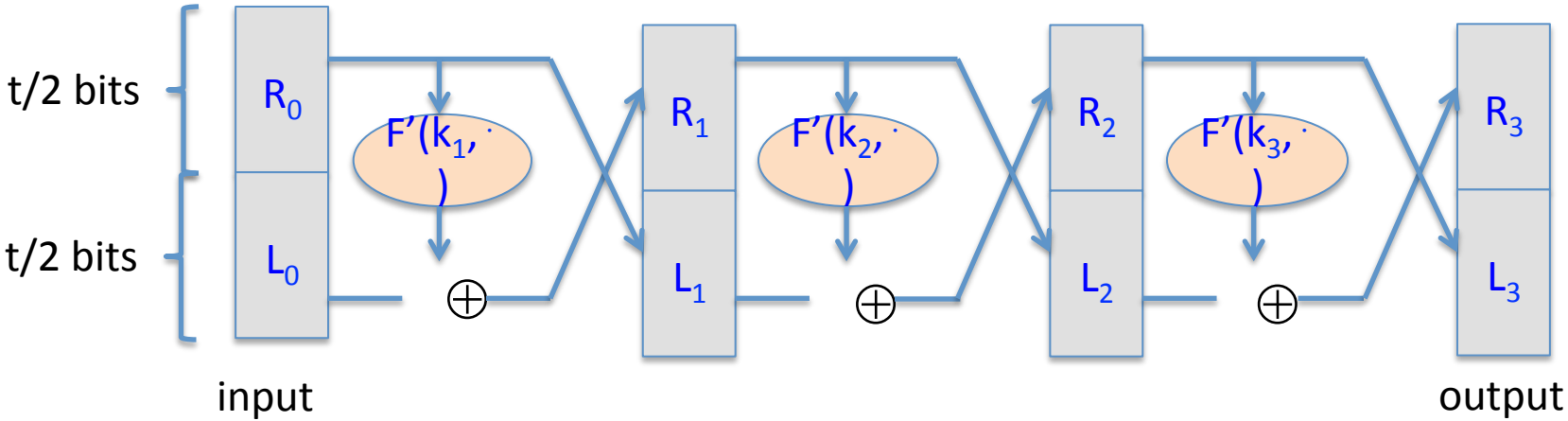
Step 1: from $\{0,1\}^n$ to $\{0,1\}^t$ (t<n)

Want PRP on **{0,…,s-1}** . Let t be such that $2^{t-1} < s \le 2^t$.

Method: Luby-Rackoff with **F': $K \times \{0,1\}^{t/2} \longrightarrow \{0,1\}^{t/2}$** (truncate F)



(better to use 7 rounds a la Patarin, Crypto'03)