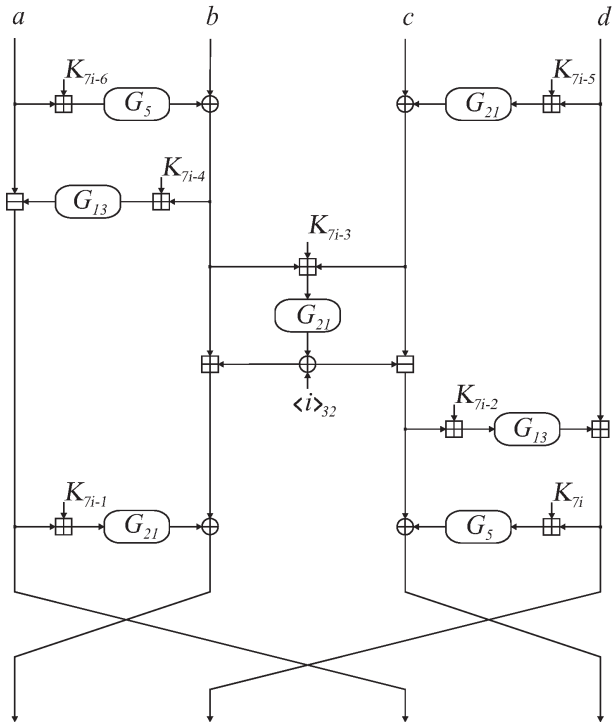
58 Такт Belt

Задача. На i-м такте Belt (СТБ 34.101.31) 128-битовое слово X преобразуется в 128-битовое слово Y. Входы и выходы задаются четырьмя 32-разрядными регистрами a, b, c и d. Преобразование задается семью 32-разрядными тактовыми ключами:



Доказать, что для любой пары (X, Y) найдется ровно 2^{96} наборов тактовых ключей, переводящих X в Y.

Решение. Достаточно доказать, что для любых фиксированных K_{7i-6}, K_{7i-5} и K_{7i-3} найдется единственный способ доопределения тактовых ключей, при котором X перейдет в Y.

Пусть A, B, C, D — 32-разрядные части Y: $Y = A \parallel B \parallel C \parallel D$. Нужное значение C получаем, манипулируя тактовым ключом K_{7i-4}. Нужное значение A — ключом K_{7i-1}, B — ключом K_{7i-2}, D — ключом K_{7i}. Всякий раз будет подходить только один тактовый ключ. □