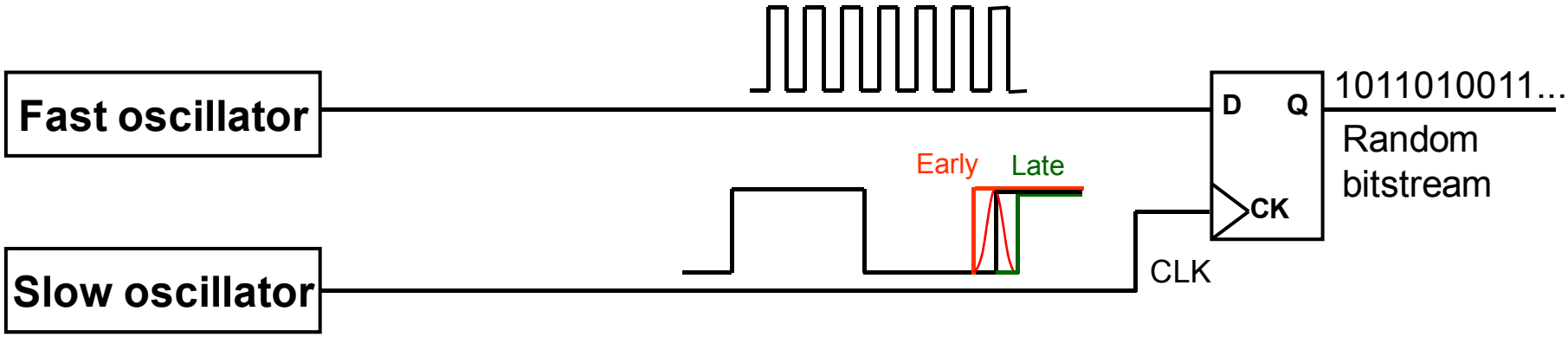
Jitter Amplifier for Oscillator-Based True Random Number Generator (ID:1D-5)

T. Amaki, M. Hashimoto and T. Onoye
Dept. Information Systems Engineering, Osaka University, Japan
JST CREST

Background & Objective

- True random number
  - unpredictable.
  - physically generated.
  - indispensable for security.
- Oscillator-based TRNG[1]
  - 2 oscillators and 1 sampler
  - utilize jitters of oscillators.

- Challenge
  - Jitter amount is insufficient.
  - Low randomness



[1] Benjamin Jun and Paul Kocher, “The Intel random number generator,” cryptography research, inc. white paper for Intel corporation, April 22, 1999.

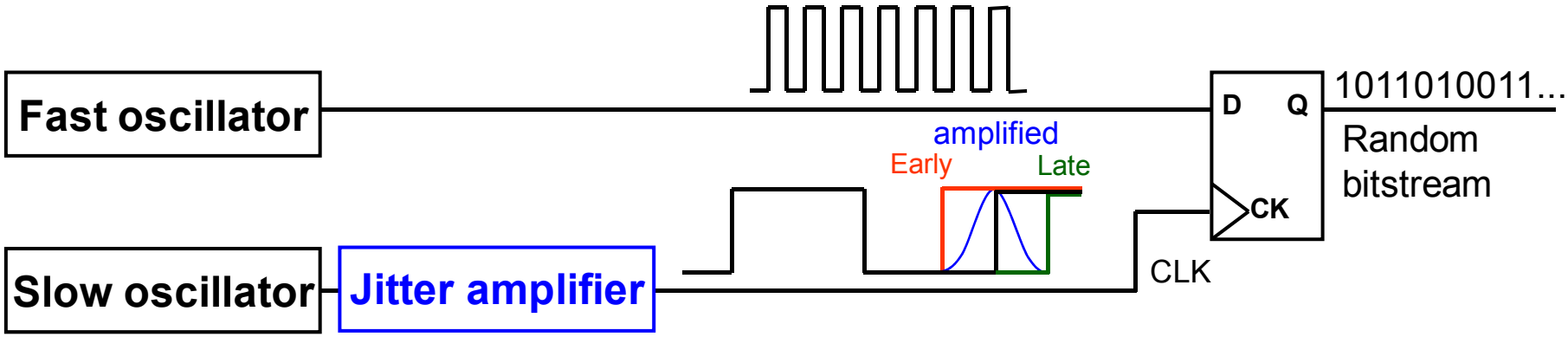
Background & Objective

- True random number
  - unpredictable.
  - physically generated.
  - indispensable for security.
- Oscillator-based TRNG[1]
  - 2 oscillators and 1 sampler
  - utilize jitters of oscillators.

- Challenge
  - Jitter amount is insufficient.
  - Low randomness

↓

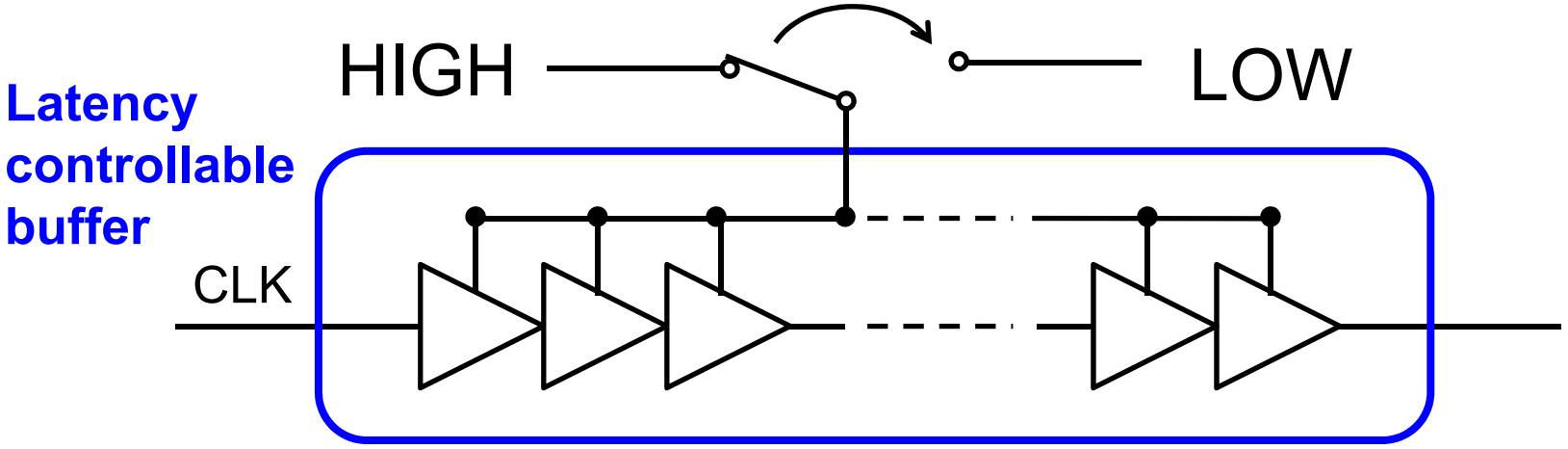
Jitter amplifier is proposed.



[1] Benjamin Jun and Paul Kocher, “The Intel random number generator,” cryptography research, inc. white paper for Intel corporation, April 22, 1999.

Idea of jitter amplifier

- Latency controllable buffer
  - Small latency for early rising edge, and large latency for late rising edge.
  - VDD for buffer is switched from HIGH to LOW.



Early — Small latency — ***Earlier***

Late — Large latency — ***Later***

Efficiency

- Proposed jitter amplifier
  - implemented in 65nm CMOS process.
  - achieved 8.4x gain at 25 ℃.
  - enhanced entropy of random bitstreams.