Crypto Engineering TP — Generic second preimage attacks on long messages for narrow-pipe Merkle-Damgard hash functions

Barrois. F, Duverney. T

[2018-11-13 mar.]

1 Part one: Preparatory work

2 Part two: The attack