SATURNIN: a suite of lightweight symmetric algorithms for post-quantum security

Changes from Version 1 (March 29, 2019) to Version 1.1 (September 27, 2019)

Anne Canteaut[1], Sébastien Duval[2], Gaëtan Leurent[1], María Naya-Plasencia[1], Léo Perrin[1], Thomas Pornin[3] and André Schrottenloher[1]

[1] Inria, France, {anne.canteaut,gaetan.leurent,maria.naya_plasencia,leo.perrin,andre.schrottenloher}@inria.fr
[2] UCL Crypto Group, Belgium, sebastien.pf.duval@gmail.com
[3] NCC Group, Canada pornin@bolet.org

Changes with Respect to Version 1

- Page 7 in "Security claim for SATURNIN block cipher": changed "$\mathcal{T}/p < 2^{112}$" to "$\mathcal{T}^2/p < 2^{224}$" (the new claim is stronger and matches the probability of success of Grover's algorithm with a reduced number of iterations)
- Page 8 in "Hash function": added $\mathcal{M}_q > 0$ (a quantum adversary uses at least one qubit)
- Correction of typos