

Certified and optimizing bit slicing compiler

Darius Mercadier Pierre-Evariste Dagand

February 11, 2017

0.1 Dummy

[1], [2], [3], [4]

Bibliography

- [1] E. Biham, *A fast new DES implementation in software*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 260–272. [Online]. Available: <http://dx.doi.org/10.1007/BFb0052352>
- [2] M. Kwan, “Reducing the gate count of bitslice des,” 2000, mkwan@darkside.com.au 11238 received 8 Oct 2000. [Online]. Available: <http://eprint.iacr.org/2000/051>
- [3] T. Pornin, “Implantation et optimisation des primitives cryptographiques,” *PhD Thesis*, 2001.
- [4] R. Fisher, “General-purpose simd within a register: Parallel processing on consumer microprocessors,” *Ph.D. Thesis Proposal*, 1997.