Zorro was lucky to attract the attention of external cryptanalysts who improved our security evaluations and found attacks against the full version of the cipher. In particular, [2] describes an internal differential attack that works for 2^{64} (weak) keys among the 2^{128} possible ones, in approximately 2^{54} time, data and memory. It exploits an equivalent description of the 4-round steps in Zorro (with no round counstants additions between the rounds). Additionally, [3] claims a differential attack with time complexity 2^{108} and data complexity 2^{112}. It is essentially based on an iterated differential characteristic that exploits the property of `MixColumns` that the fourth power of its MDS matrix is the identity matrix. Both attacks suggest that finding the right balance between linear and non-linear components in irregular designs such as Zorro is challenging. For example, avoiding the equivalent description in [2] would require more rounds per steps, and avoiding the iterated differential characteristic in [3] would probably be best achived with a change of linear layer. While these results clearly threaten the instance of cipher proposed, we hope that the design strategy described in [1] (namely, the search for S-boxes with limited number of multiplications, and the use of irregular designs to limit the total number of S-boxes in the cipher) remains interesting, and can potentially be used to obtain ciphers with efficient masked implementations. Note that we have no plans to tweak the design of Zorro in the near future, but may consider it in the mid-term. Feel free to contact us by e-mail if you are willing to collaborate on a Zorro* instance, or to mention additional cryptanalysis results that we should refer.

References

1. Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES*, volume 8086 of *Lecture Notes in Computer Science*, pages 383–399. Springer, 2013.
2. Jian Guo, Ivica Nikolic, Thomas Peyrin, and Lei Wang. Cryptanalysis of zorro. Cryptology ePrint Archive, Report 2013/713, 2013. `http://eprint.iacr.org/`.
3. Zhiyuan Guo Yanfeng Wang, Wenling Wu and Xiaoli Yu. Differential cryptanalysis and linear distinguisher of full-round zorro. Cryptology ePrint Archive, Report 2013/775, 2013. `http://eprint.iacr.org/`.