Improved meet-in-the-middle attacks on reduced-round Piccolo

Piccolo is a lightweight block cipher that adopts a generalized Feistel network structure with 4 branches, each of which is 16 bit long. The key length is 80 or 128 bit, denoted by Piccolo-80 and Piccolo-128, respectively. In this paper, we mounted meet-in-the-middle attacks on 14-round Piccolo-80 without preand post-whitening keys and 18-round Piccolo-128 with post-whitening keys by exploiting the properties of the key schedule and Maximum Distance Separable (MDS) matrix. For Piccolo-80, we first constructed a 5-round distinguisher. Then 4 rounds and 5 rounds were appended at the beginning and at the end, respectively. Based on this structure, we mounted an attack on 14-round Piccolo-80 from the 5th round to the 18th round. The data, time, and memory complexities were 252 chosen plaintexts, 267.44 encryptions, and 264.91 blocks, respectively. For Piccolo-128, we built a 7-round distinguisher to attack 18-round Piccolo-128 from the 4th round to the 21st round. The data, time, and memory complexities were 252 chosen plaintexts, 2126.63 encryptions, and 2125.29 blocks, respectively. If not considering results on biclique cryptanalysis, these are currently the best public results on this reduced version of the Piccolo block cipher.