UDC 681.3.06:006.354

L. KOVALCHUK, R. OLIYNYKOV, M. RODINKO

SECURITY OF POSEIDON HASH FUNCTION AGAINST NON-BINARY DIFFERENTIAL AND LINEAR ATTACKS[1]

Abstract. In this work we build the security estimations of Poseidon hash function against non-binary linear and differential attacks. We adduce the general parameters for the Poseidon hash function that allow using this hash function in recurrent SNARK-proofs based on MNT-4 and MNT-6 triplets. We also analysed how to choose S-boxes for such function for this choice to be optimal from the point of view of the number of constraints and security. We also showed how many full rounds is sufficient to guarantee security of such hash function against non-binary linear and differential attacks and calculated the number of constraints per bit that is achieved in the proposed realizations demonstrating a considerable gain was demonstrated, as compared to the Pedersen hash function.

Keywords: SNARK, constraints, Poseidon hash function, non-binary linear and differential cryptanalysis.

INTRODUCTION

One of the most important problems arising in construction of SNARK-proofs and STARK-proofs [1–3] is reduction of the number of constraints describing algorithms in the respective SNARK-system. The construction of such proofs begins with the fact that a certain transformation (for example, a hash function) should be described as a system of certain equations of many variables over a finite field, the left part of which contains a polynomial of many second degree variables, and the right part — a polynomial of many variables of the first degree. These equations are called constraints, and their complexity determines the complexity of constructing the appropriate SNARK-proof. Most often SNARK-proofs are used to prove knowledge of the pre-image of some hash function. Therefore, the hash functions used in such blockchains should be designed so that they can be described by as few constraints as possible.

One of the first hash functions convenient for constructing SNARK-proofs was the Pedersen hash function [4, page 134]. It is based on operations in a group of points of an elliptic curve, which, in turn, can be reduced to operations in the corresponding finite field. Since constraints are polynomials just over such a field, the number of constraints required to specify such a hash function is ten times less than for “classical” hash functions that operate with byte and bit operations (about 1.68 constraints per 1 bit of input). This number of constraints is quite acceptable, but the question of reducing it still remains relevant. The Poseidon hash function proposed in [5] appeared to be quite a good construction with respect to the number of constraints. For this function, the number of constraints is up to 15 times smaller than for the Pedersen hash function. Utilization of this function in SNARK-systems requires provision of a full substantiation of its security against the main applicable cryptographic attacks. The Poseidon hash function is based upon the SPONGE construction [6] that uses the HADES block cipher algorithm [7] as the inner permutation. For this reason, the main part of the security substantiation for the Poseidon hash function is to show that the HADES algorithm is indistinguishable from

[1] This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.