The cryptographic transformation ThreeCircle

Joan Daemen

Radboud University

Abstract. ThreeCircle is a cryptographic transformation that operates on a state of 160 digits in GF(3). The transformation can be used in modes of use that usually are applied to cryptographic permutations such as the sponge and keyed duplex constructions and Farfalle. The transformation is in general not invertible but the fraction of the states that have no pre-image, or that have multiple pre-images, is negligible.

1 Introduction

2 Specification of ThreeCircle

ThreeCircle has a classical iterated structure: it iterates a round function a number of times to the state. This round function is designed according to the wide trail strategy: it contains a non-linear step, a mixing step, two transposition steps and the addition of a (round-index-dependent) round constant.

A ThreeCircle state a consists of 5 32-digit lanes, we write $a = (a_0, a_1, a_2, a_3, a_4)$.
We list our notational conventions in Table 1.

Table 1: Notational conventions

a_y	Lane y of state a
$a_{y,x}$	Bit x of lane a_z
$a_y \lll v$	Cyclic shift of a_y moving digit in position x to position $x + v$
$a_y + a_{y'}$	Digitwise sum of lanes a_y and $a_{y'}$
$a_y a_{y'}$	Digitwise product of lanes a_y and $a_{y'}$

The permutation consists of 12 rounds $\mathrm{R_i}$ as specified in Algorithm 1.

Algorithm 1 The ThreeCircle round function $\mathrm{R_i}$

for Round index i from -11 to 0 **do**
  $a \leftarrow \mathrm{R_i}(a)$

Here $\mathrm{R_i}$ is specified by the following sequence of steps:

$$
\begin{aligned}
\chi : b_y &\leftarrow a_y + a_{y+1}a_{y+1} \lll 1 \text{ for all } y \\
a &\leftarrow b \\
\theta : p &\leftarrow a_0 + a_1 + a_2 + a_3 + a_4 \\
e &\leftarrow p \lll 12 + p \lll 17 \\
a_y &\leftarrow a_y + e \text{ for all } y \\
\pi : b_y &\leftarrow a_{y+1} \text{ for all } y \\
a &\leftarrow b \\
\iota \quad a_0 &\leftarrow a_0 + c_j \\
\rho : a_i &\leftarrow a_y \lll r_y \text{ for all } y \text{ with } r = (0, 2, 6, 11, 19)
\end{aligned}
$$

The round constants c_j are 32-digit lanes and we specify them currently as all-zero.