

ABSTRACT**METHOD FOR DETECTING ABNORMALITIES IN A CRYPTOGRAPHIC CIRCUIT PROTECTED BY DIFFERENTIAL LOGIC, AND CIRCUIT FOR IMPLEMENTING SAID METHOD**

The subject of the present invention is a method for detecting anomalies in a circuit protected by differential logic and which processes logic variables represented by a pair of components (a_i , a_f), a first network of cells (T) carrying out logic functions on the first component of said pairs, a second network of dual cells (F) operating in complementary logic on the second component, the logic functions being carried out by each pair of cells (T, F) in a pre-charge phase (21) placing the variables in a known state on input to the cells and followed by an evaluation phase (22) where a calculation is performed by the cells, said method being characterized in that an anomaly is detected by at least one non-consistent state.

The subject of the invention is also a circuit protected by differential logic comprising means for testing the consistency between the two components of the logic variables during the pre-charge or evaluation phases at the monitored nodes of the circuit.

Figure 3

