

ABSTRACT**METHOD FOR TESTING CRYPTOGRAPHIC CIRCUITS,
SECURED CRYPTOGRAPHIC CIRCUIT CAPABLE OF BEING TESTED,
AND METHOD FOR WIRING SUCH CIRCUIT**

The present invention relates to a method for testing cryptography circuits. It also relates to a secure cryptography circuit capable of being tested.

The cryptography circuit comprising registers and logic gates (211, 212, 213, 5 214), a test according to the invention performs a differential power analysis (DPA) on the registers of the circuit.

A cryptography circuit being secure and comprising a first half-circuit (211, 214) associated with a second half-circuit (212, 213) operating in complementary logic, the electric power supply (Vdd1, 23, 25) of the first half- 10 circuit is separated from the electric power supply (Vdd2, 24) of the second half-circuit, the differential power analysis being carried out in parallel on each half-circuit, the two power supplies being combined into one and the same electric power supply after the test.

15 Figure 3