

ABSTRACT**Low-complexity electronic circuit protected by customized masking**

5

The subject of the invention is a cryptography circuit protected by masking, said circuit comprising means for encrypting binary words using at least one key k_r^c , means for applying linear processing operations (216) and nonlinear processing operations (226) to said words and means for masking said words. The binary words are unmasked (214) upstream of the nonlinear processing operations by using a mask k_r^i and masked (215) downstream of said processing operations by using a mask k_{r+1}^i , the masks k_r^i and k_{r+1}^i being chosen from a set of masks that is specific to each instance of the circuit.

15

Reference: Figure 2



162162



G00002