

TABLE SPLITTING FOR CRYPTOGRAPHIC PROCESSES**ABSTRACT**

For a defined cryptographic process including an original substitution table, split masked
5 substitution tables are provided to resist cryptographic attacks. The split masked
substitution tables are defined with reference to a set of random value data words and a
mask value. An entry in the split masked substitution tables is defined by selecting bits
from the corresponding entry in the original masked substitution table, as masked by the
corresponding one of the set of random value data words and by selecting bits from the
10 corresponding one of the set of random value data words as masked by the mask value.
The split masked substitution tables are usable in a modified cryptographic process based
on the defined cryptographic process to permit a masked output to be generated. The split
masked substitution tables are refreshed by each entry in the tables being refreshed upon
access during execution of the modified cryptographic process.

15 (Fig. 1)