

addition, there is often no free access to such countermeasures due to protection conferred by patents. Accordingly, there is a need to provide a new AE scheme in order to overcome at least partially these drawbacks.

Document XP047030081 entitled "Two-Pass Authenticated Encryption
5 Faster Than Generic Composition" (by Stefan Lucks), relates to CCFB
authenticated encryption schemes (with or without associated data H) and
more specifically proposes another two-pass scheme with different separation
of duties between the passes. The first pass is for privacy and "local"
authentication, while the second computes a single "global" authentication tag
10 from the local ones. At each round, only a part (e.g. a 8-bit segment) of the
cryptogram provided by the block cipher algorithm is retained in order to be
successively combined with the message blocks resulting from the division of
the plaintext message into block; the other part (segment) being discarded.

SUMMARY OF THE INVENTION

Instead of providing new countermeasures to protect cryptosystems against DPA attacks, the present invention suggests an improved mode of operation, while keeping DPA attacks in mind. To this end, the present invention refers to a mode of operation, based on the CCFB scheme, which is better suited to mitigate DPA attacks. More particularly, the present invention suggests a block cipher method using round repetition for providing, from a plaintext message, a ciphertext message and a global tag for authenticating said ciphertext message. The plaintext message is converted (in particular dividing and padding if any) into a plurality of ordered plaintext blocks having all the same bit length. Each of these plaintext blocks is successively processed in an orderly manner as a current plaintext block during a round. The method comprising the following actions:

- loading a first data into a register,
- running the round by performing the following steps:
 - a first step for inputting input data into a block cipher algorithm, such input data comprising data of the register and a reproducible data, e.g. a counter data or any other reproducible data series,
 - a second step for computing, within the block cipher algorithm, a cryptogram by encrypting the input data using a single cryptographic key, this cryptogram comprises a first segment and a second segment, the latter being defined as an authentication local tag,
 - a third step for computing a ciphertext block by performing a first operation using as operands: the first segment, the current plaintext block, and the second segment,
 - as long as all the aforementioned plaintext blocks have not been processed in such a round, reloading the register with the last computed