OTHER CYCLING TESTS FOR DES

Jean-Jacques Quisquater & Jean-Paul Delescaille

Philips Research Laboratory Brussels
Avenue Van Becelaere, 2
B-1170 Brussels, Belgium

Abstract

A very preliminary presentation of this paper was done at the rump session of CRYPTO '86 and kindly played by Gus Simmons (Sandia). The full paper will be complete description of some cycling experiments applied to DES using only very fast software for the computations. Using only software permitted many measures and tests.

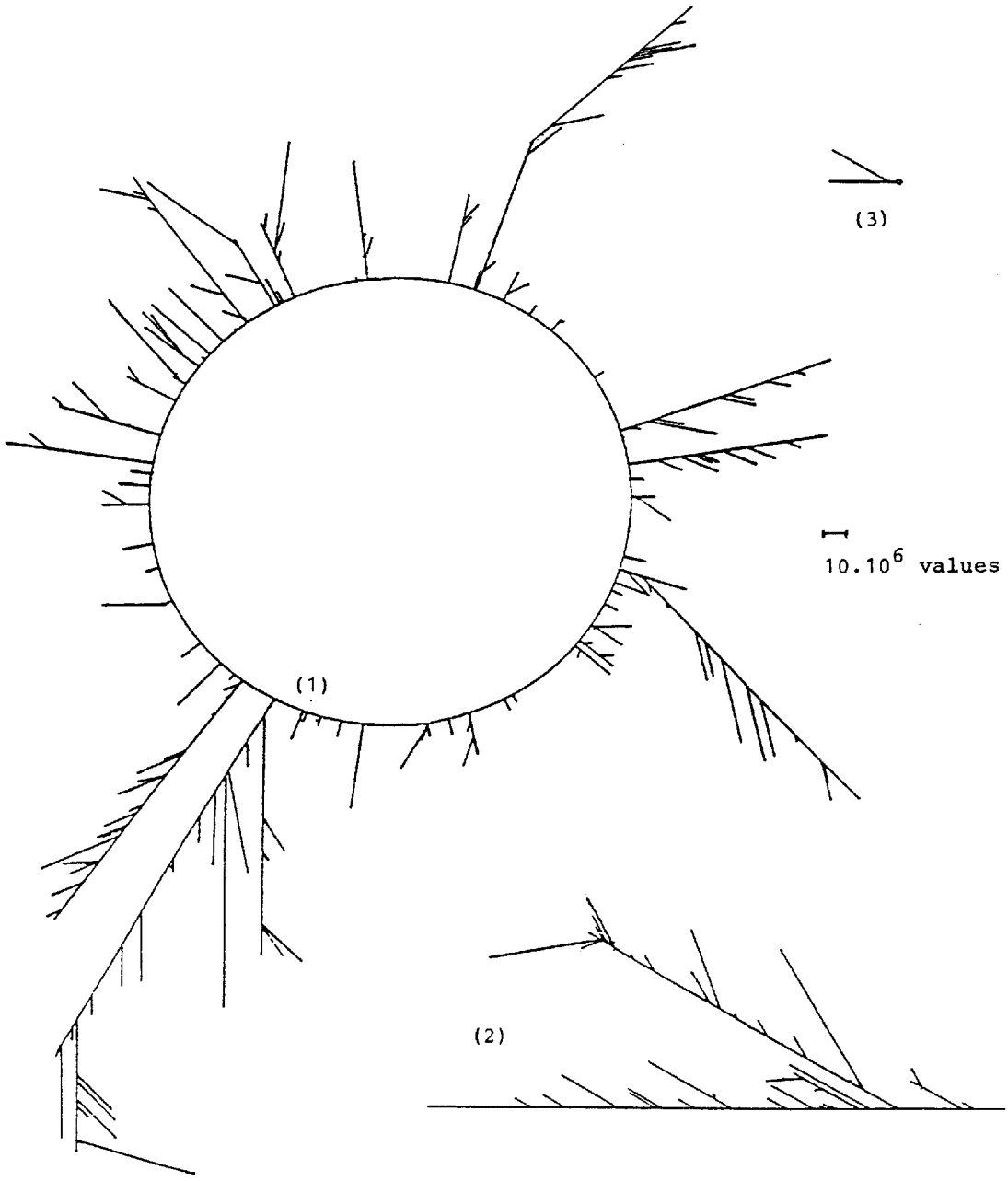
The used version of DES has a speed of about 2 Mbits/sec for a given key and a speed of about 600 kbits/sec for a change of key and an encryption (this version is not fully optimized due to some problems with the cache of the computer). For these experiments we used the idle time of an IBM 3090 and a total of 2^{34} encryptions were performed. Many techniques were used in order to avoid duplicate computations and big files.

The cycling test we done is the following one: Given a "random" key and a fixed message, what is the cycle structure if the output is next used as key after some fixed transformation? For a given configuration, 3 cycles were found, the smallest having only about 60.000 elements. Many statistical tests were done (distribution of "distances" between typical points, cumulative distributions, lengths of tails before collision, etc). A total of 1900 initial points were tested. Each initial point belongs to one of the three found cycles: A very fast technique was used to identify the related cycle. The three cycles were drawn giving more visual informations about random mappings (see next page).

New techniques to find large cycles and collisions of tails were elabored using the notion of *distinguished point* (an output of DES with some quickly tested property), a related concept for the use of an hashing function and a clever time-memory trade-off.

From a theoretical point of view, the relation with the theory of random mappings and the use of DES to obtain random numbers (see J. Gait) was done and a better view of "drainage" (see Reyneri and Hellman) was obtained. The use of distinguished points is also possible for the study of exhaustive machines (Hellman)

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 255-256, 1988.


(3)
10.10^6 values
(1)
(2)