Koeune, Francois; Rouvroy, Gael; Standaert, Francois-Xavier; Quisquater, Jean-Jacques; David, Jean-Pierre; Legat, Jean-Didier

An FPGA implementation of the linear cryptanalysis. (English) Zbl 1020.68734

Summary: This paper deals with cryptographic concepts. It presents a hardware FPGA implementation of linear cryptanalysis of DES. Linear cryptanalysis is the best attack known able to break DES faster than exhaustive search. Matsui’s original attack could not be applied as such, and we had to implement a modified attack to face hardware constraints. The resulting attack is less efficient than Matsui’s attack, but fits in our hardware and breaks a DES key in 12-15 hours on one single FPGA, therefore becoming the first practical implementation to our knowledge. As a comparison, the fastest implementation known so far used the idle time of 18 Intel Pentium III MMX, and broke a DES key in 4.32 days. Our fast implementation made it possible for us to perform practical tests, allowing a comparison with theoretical estimations.

For the entire collection see [Zbl 1010.68847].

MSC:
68U99 Computing methodologies and applications
94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)
94A60 Cryptography

Full Text: Link