The goal of the Advanced Encryption Standard (AES) is to achieve secure communication. The use of AES does not, however, guarantee reliable communications. Faults must be detected before sending to avoid the transmission and use of erroneous encrypted/decrypted data. Concurrent fault detection is important not only to protect the encryption/decryption process from random faults. It will also protect the encryption/decryption circuitry from an attacker who may maliciously inject faults in order to find the encryption secret key. We first describe some studies of the effects that faults may have on a hardware implementation of AES, by analyzing the propagation of such faults to the outputs. We then present a fault detection scheme based on error detection code.

Industrial Days
Giornate di Matematica per l'Industria
Milan, 1 December 2003