

Practical measurements of data path delays for IP authentication & integrity verification

Definition of Hardware Trojan (HT)

A Hardware Trojan is a malicious, undesired and intentional modification of an integrated circuit or design. It can transmit critical information without the knowledge of the user or disable/destroy some components of the circuit.

A HT insertion can be done at any stage during the design of an integrated circuit or during the manufacturing process.

Detection of Hardware Trojan



Detection of a HT can use several techniques. The side channel approach is one of the most studied methods through the power/temperature/electromagnetic emissions analysis.

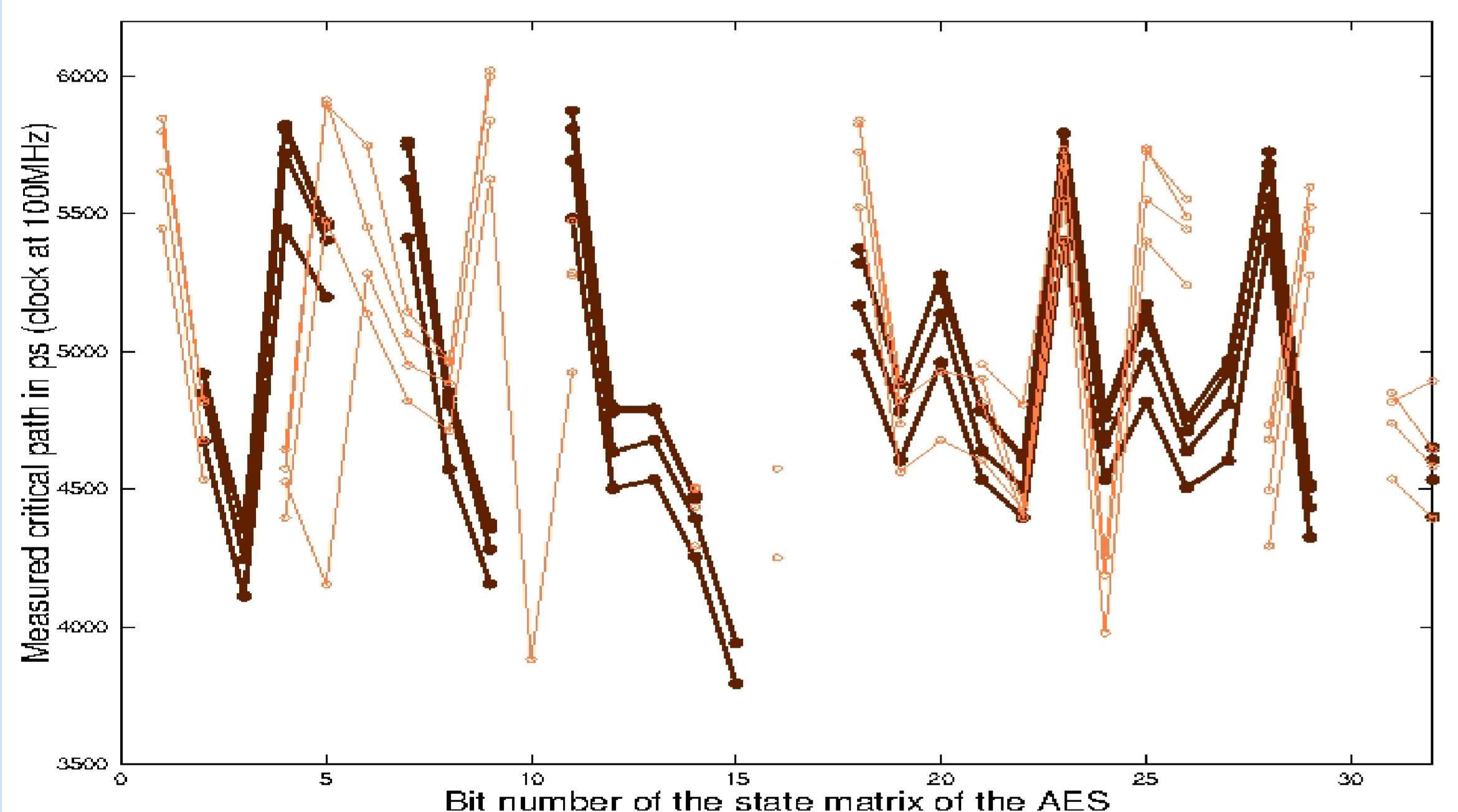


Fig 3. Path delay distributions for the first 32 bits on 4 boards without (thick brown line) & with (thin orange line) HT.

Four measurements were made for an AES without HT, and one with a HT (fig 4) on four different boards. The clock glitch tool is able to detect a significant change in the VHDL code beyond the variations due to inter-die variations (fig 3).

Measurements of data path delay

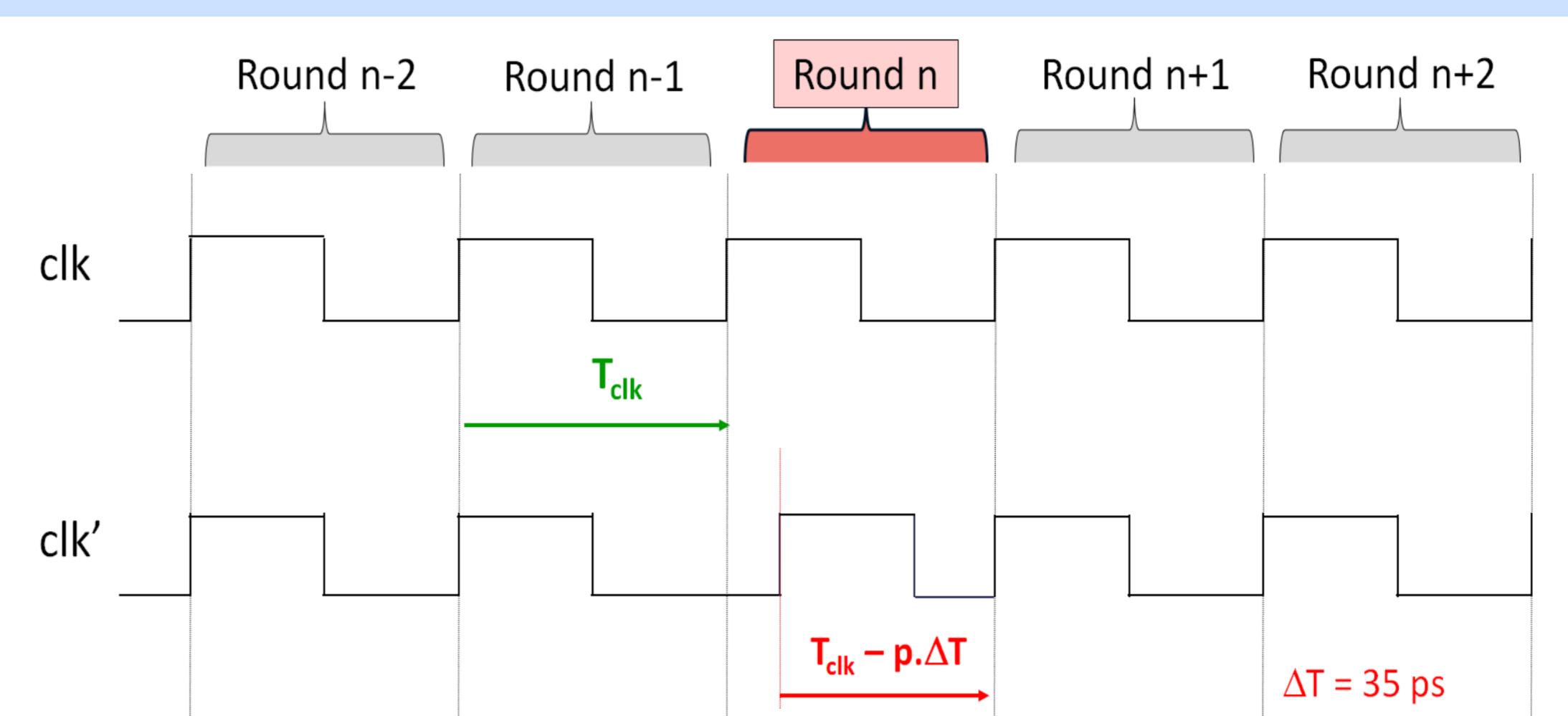


Fig 1. Clock glitch effect.

The clock glitch (fig 1) is achieved by progressively reducing the clock period, until a setup time violation occurs.

The choice of the injection's cycle is possible.

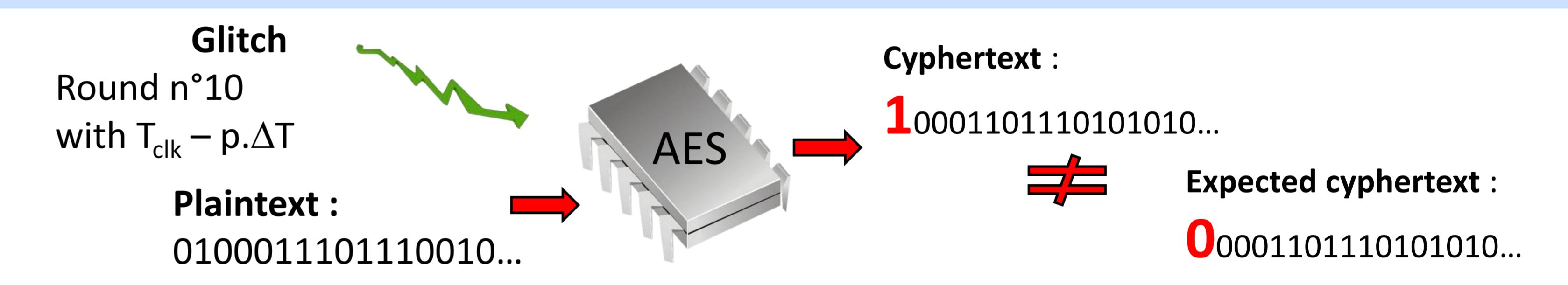


Fig 2. Measurement of path delay for the first bit of the AES.

Generate a fault leads us to measure the bits propagation time knowing the number of ΔT diminution (fig 2).

RTL modifications

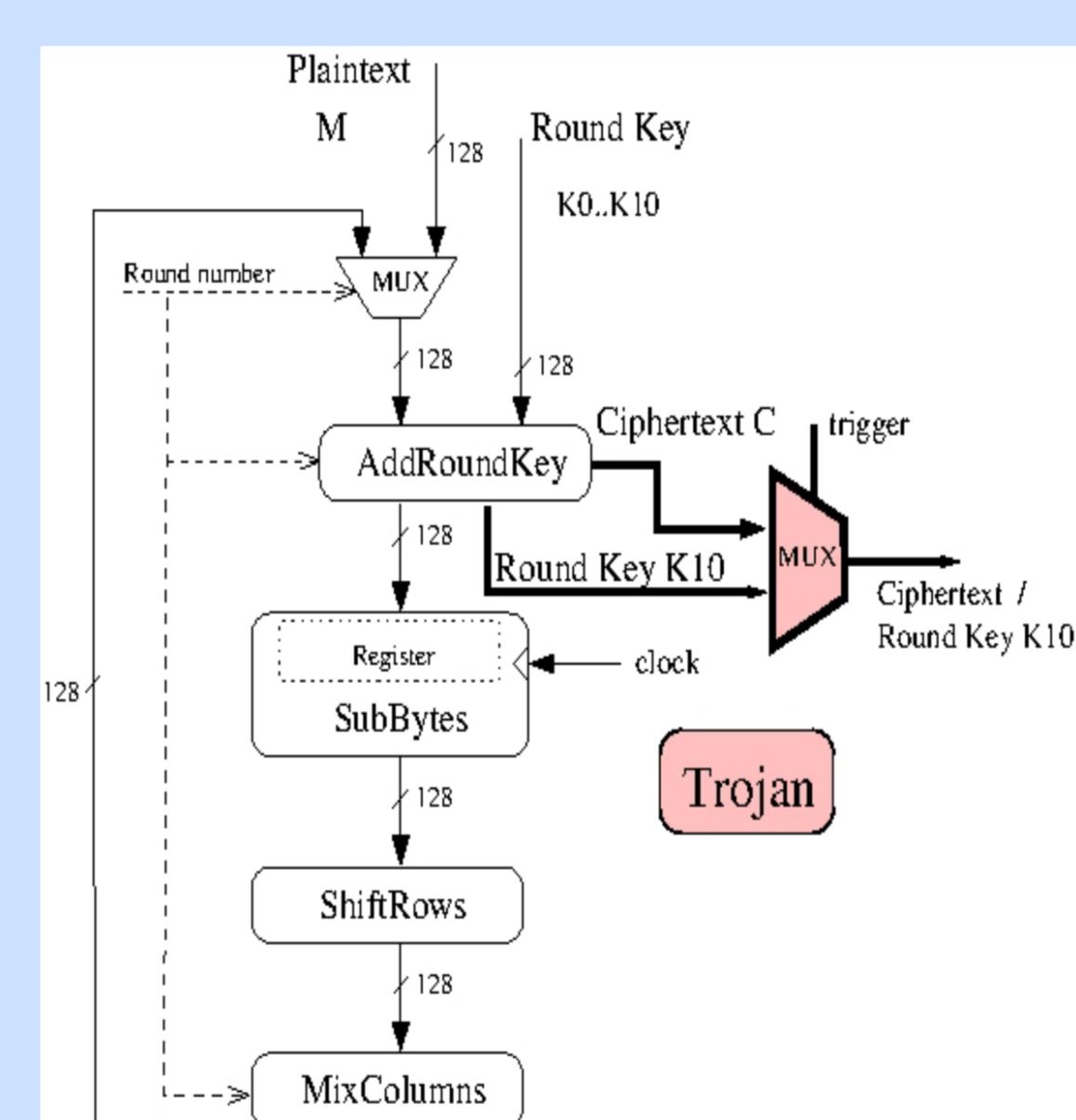


Fig 4. Implemented HT.

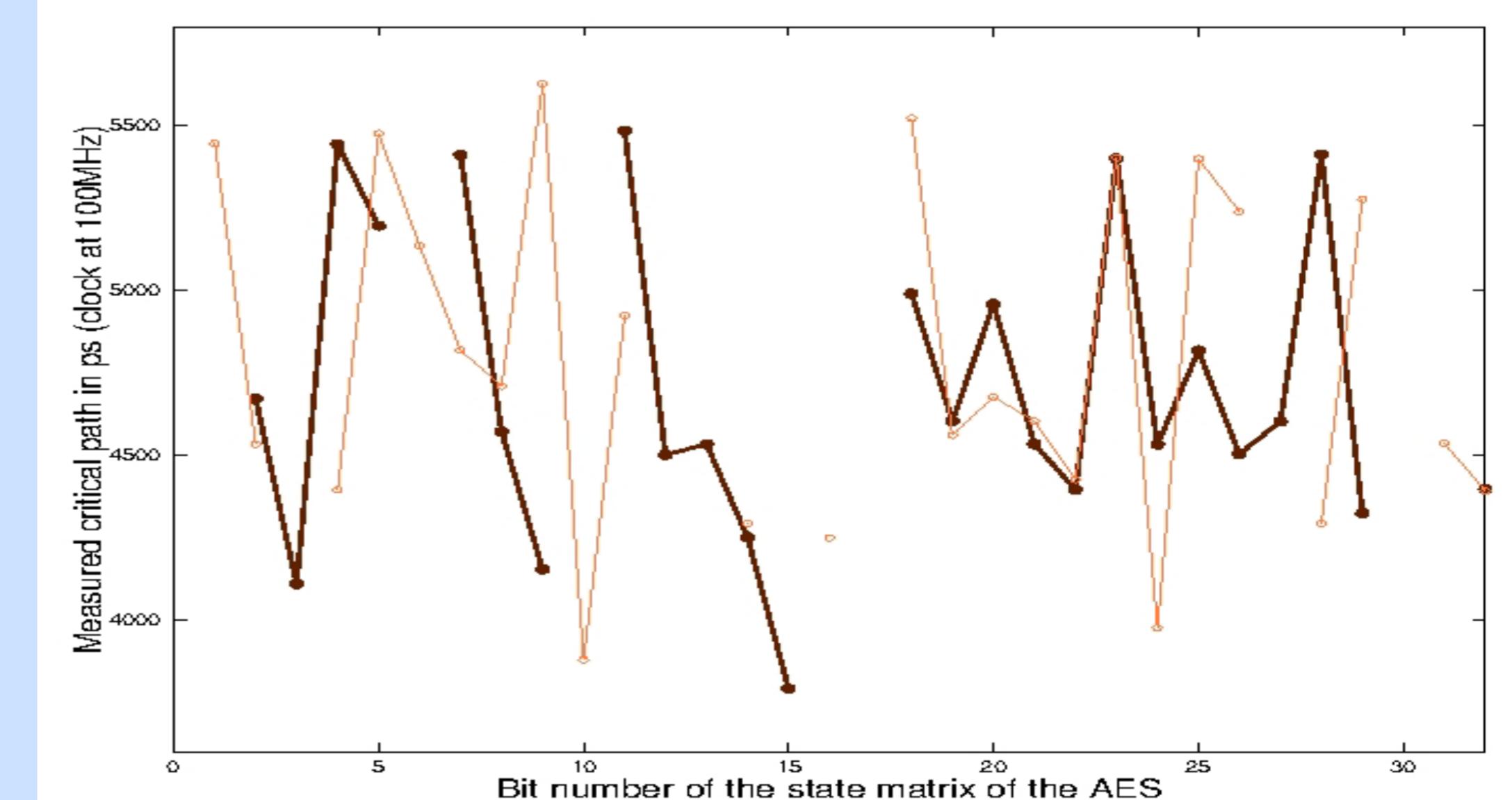


Fig 5. Path delays distributions without (thick brown line) & with (thin orange line) trojan for the first 32 bits of the State matrix.

The measured path delays' distributions of an AES without HT, and one with a HT (fig 4) were done on the same board. The mean path delay associated to each bit has significantly changed. Their "orders of appearances" and the distribution of the "ghost bits" have been changed.

The modifications (fig 5) induced by the HT are significant.

Conclusion

The distribution of those propagation times is a characteristic "fingerprint" of the module, suggesting that this might be a practical means of authenticating an IP and also a method to qualify the integrity of a given IP, without adding any other circuit.

Exurville Ingrid*,‡, Fournier Jacques*, Dutertre Jean Max ‡, Robisson Bruno*, Tria Assia*

*CEA, ‡EMSE

880, route de Mimet, 13541 Gardanne, France