Insertion of random delay with context-aware dummy instructions generator in a RISC-V processor

Gaëtan Leplus
LETI
CEA
Grenoble, France
gaetan.leplus@cea.fr

Olivier Savry
LETI
CEA
Grenoble, France
olivier.savry@cea.fr

Lilian Bossuet
Laboratoire Hubert Curien
Jean Monnet University
Saint-Etienne, France
lilian.bossuet@univ-st-etienne.fr

***Abstract*—Embedded systems are vulnerable to side channel and fault injection attacks. These two types of attacks can be slightly complicated by using temporal desynchronization methods. In this article we propose a new hardware solution to efficiently insert dummy instructions in run time for a general-purpose processor. The main contribution of this solution is to contextualize these dummy instructions, making them less distinguishable and more variable with a minimal spatial overhead of 2.96% and a 4.27% additional consumption and no code size impact on a CV32E40P RISC V processor. As a result, they bring a significant resistance to resynchronization methods.**

Keywords*—*Side channel attacks, Fault injection attack, countermeasures, random delays

*****This work has been accepted at HOST2022 but is not yet available online*****