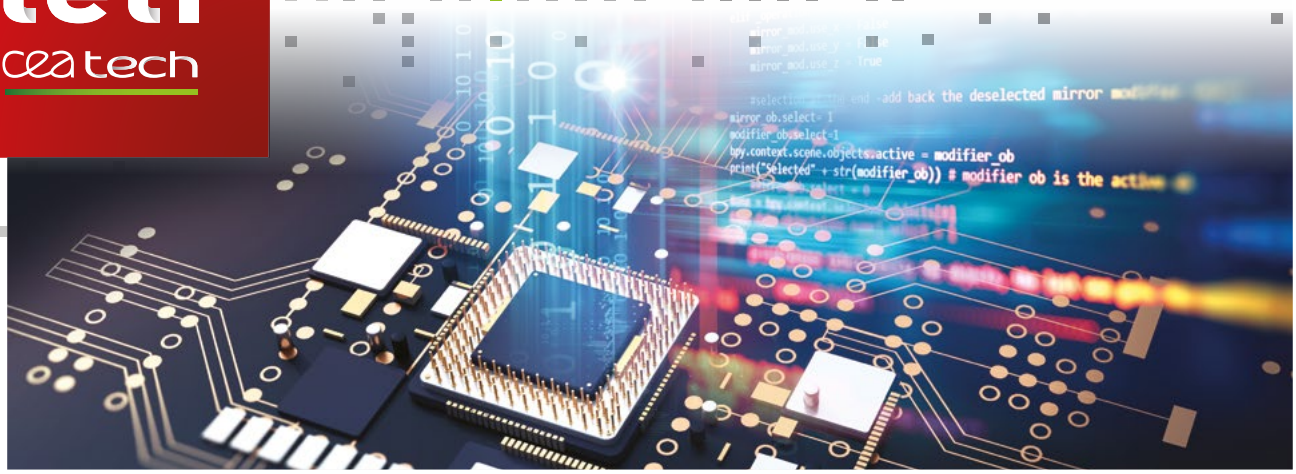
FRANÇAIS ENGLISH



LOKI

SIDE-CHANNEL ATTACKS: TESTING CIRCUIT RELIABILITY

WHAT IS LOKI?

Can we depend on the security of our connected devices? CEA-Leti has developed LOKI, a solution designed to show how quick and easy it is to extract sensitive non-protected data from commercial electronic components.
LOKI demonstrates a side-channel attack during an encryption calculation. The AES encryption implemented in the device is a standardized algorithm used in industry. By design, the memory of the component embeds the encryption key which cannot be accessed via commands to the card's input/output interface.

A side-channel attack is neither invasive nor intrusive; a protective software cannot detect it. The side-channel attack illustrated by LOKI involves picking up the electromagnetic signals emitted by the chip during an encryption operation in order to identify the encryption key used.

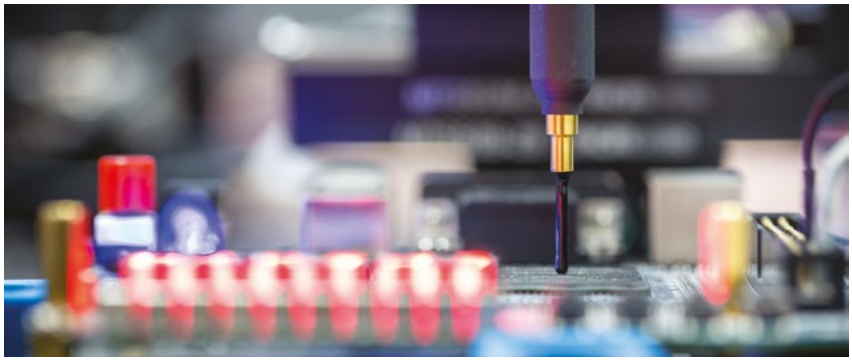
APPLICATIONS

- All types of electronic components that do not take these attacks into account
- Various industries including the medical sector, industrial systems and national security

WHAT'S NEW?

Side-channel attacks have been studied for twenty years in the field of smart cards. The costs involved in these attacks have fallen sharply, as have the size and complexity of the equipment needed. Attacks are now more frequent and more difficult to detect.

CEA-Leti is building on more than 15 years of expertise in protection against side-channel attacks to develop a range of state-of-the-art countermeasures designed for connected devices and their limitations. Working in partnership with the industry, the institute incorporates countermeasures starting at the product design stage, offering the best levels of security while addressing constraints relating to applications, power consumption, size, volume and cost.



WHAT'S NEXT?

The institute is working on a set of technology components to secure processors in cryptography modules, memory and the attack vectors involving the connections between these components.

On the hardware side, developments focus on understanding attacks in the context of new cryptographic algorithms and the patterns of use of IoT devices. The goal is to stay ahead of the hackers by concentrating on the most advanced attacks.

CEA-Leti's experts are developing new cryptography algorithms and new types of processors that IoT components can directly embed. They aim is to achieve memory security and to boost performance (computing power) to make them more suitable for the IoT and its challenges. They are also developing relevant countermeasures in terms of consumption and performance, such as automating countermeasures using dedicated compilers for connected devices.

PUBLICATIONS

- "Binary Edwards Curves For Intrinsically Secure ECC Implementations for the Iot" by A.Loiseau and J.Fournier, secrypt, 2018, springer-verlag, porto, July 2018
- "On The Importance Of Considering Physical Attacks when Implementing Lightweight Cryptography" by A.Adomnicai, B.Lac, A.Canteaut, L.Masson, R.Sirdey, A.Tria and J.Fournier, nist workshop on light weight cryptography, October 2016
- "Backside Shield Against Physical Attacks for Secure ICS" by S.Borel, E.Deschaseaux, J.Charbonnier, P.Médina, S.Anceau, J.Clédière, R.Wacquez, J.Fournier, E.Jalaguier, C.Plantier and G.Simon., Conference and exhibition on device packaging (dpc2017), Arizona, March, 2017
- "Adaptive Masking: a Dynamic Trade-Off Between Energy Consumption & Hardware Security" by M.Montoya, T.Hiscock, S.Bacles Min, A.Molnos & J.Fournier, IEEE ICCD 2019, Abu Dhabi, United Arab Emirates, Nov., 2019

INTERESTED IN THIS TECHNOLOGY?

Contact:
Marie-Sophie Masselot
marie-sophie.masselot@cea.fr
+33 438 783 830

CEA-Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 avenue des Martyrs | 38054 Grenoble Cedex 9 | France
www.leti-cea.com
@CEA_Leti CEALeti CEA-Leti