MIPSs

What we developed

Thanks to Walloon Region funding, MIPSs proposes:

1. http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau
2. A **framework** that formalizes the counterfeited IP detection problem. This is a very general approach that can easily be instantiated to any situation. Its generic representation allows the evaluator to quickly test different tools.
3. Efficient **tools** for both the extraction procedure and similarity score computation. They correspond to the most recent state of the art in side-channel analysis, and regroup signal processing techniques (for the hash extraction process) and advanced statistical tools (for computing the similarity score).
4. A wide range of **realistic case-studies** that go from 8-bit software implementations to fully parallelized hardware implementations on both ASIC and FPGA platforms. In on our experiments, we reached success rates of almost 100%.
5. A substantial **legal analysis** by law researchers addressing the question of the enforceability of this method in court.

Secure IP Marking

References:
[1] François Durvaux, Benoît Gérard, Stéphanie Kerckhof, François Koeune and François-Xavier Standaert, Intellectual Property Protection for Integrated Systems Using Soft Physical Hash Functions, Published in Information Security Applications - 13th Intl. Workshop, WISA 2012, Jeju Island, Korea, August 16-18, 2012.
[2] Stéphanie Kerckhof, François Durvaux, François-Xavier Standaert and Benoît Gérard, Intellectual property protection for FPGA designs with soft physical hash functions: First experimental results, Published in IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, Austin, TX, USA, June 2-3, 2013.
[3] Ludovic-Henri Gustin, François Durvaux, Stéphanie Kerckhof, François-Xavier Standaert and Michel Verleysen, Support Vector Machines for Improved IP Detection with Soft Physical Hash Functions, Published in Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014.
[4] Stéphanie Kerckhof, François Durvaux, Cédric Hocquet, David Bol and François-Xavier Standaert, Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint, Published in Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012.

Partnership We are looking for partners to produce and exploit this new technology

UCL Crypto Group
Place du Levant, 3 1348 Louvain-la-Neuve
(+32) 10 47 81 41 uclcryptogroup@listes.uclouvain.be

crids CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ
UNIVERSITÉ DE NAMUR
Wallonie
SPW Service public de Wallonie
UCL Université catholique de Louvain

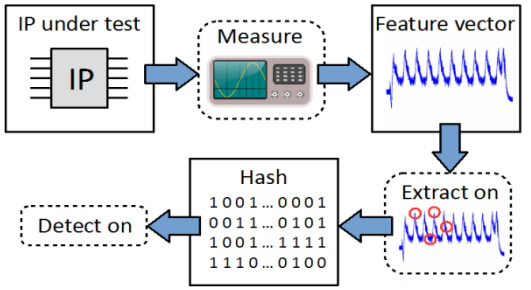
The problem of intellectual property counterfeiting

Over the last three decades, the spread of counterfeit goods has exploded. According to the International Chamber of Commerce, it accounts for up to 7% of the world trade and is worth $600 billion a year. A huge part concerns electronic devices. Counterfeiting is one of the growing challenges the Intellectual Property (IP -- e.g. software, integrated circuits) designers are facing nowadays.

Side-channel attacks

In the late 90's, Paul Kocher and his team introduced Side-Channel Analysis (SCA). They rely on the observation that the internal activity of an implementation (operations and data) is generally reflected in its physical features (e.g. power consumption trace). This unintended leakage is hardly controlled and is usually exploited to attack cryptographic devices.
Why couldn't it be used in a constructive way as well?

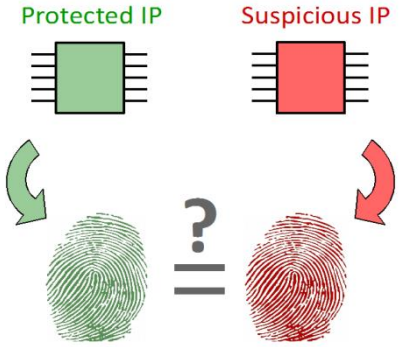
Hashes allow characterizing and distinguishing the implementations



The hash aims to be an accurate characterization of the IP. For this purpose, it first requires an extraction phase using signal processing techniques in order to be robust to minor IP modifications, while still avoiding false positives on different IPs. **MIPs** proposes a wide variety of such extraction tools. Next, the detection is based on a similarity score between the legitimate and suspicious hashes. If the score is above a predefined threshold, the IP is extremely likely to be the same.

MIPSs allows using side-channel emanations of a device to identify its embedded IP, and hence detect counterfeiting

MIPSs proposes a framework and methods to extract a signature, called a hash, identifying the IP thanks to side-channel analysis tools. The legitimate hash can then be compared to those extracted from any suspicious IP in order to detect illegal usage (or copy) of the protected IP.



MIPSs method supports all kinds of implementations

By choosing the appropriate extraction and detection tools provided in the outcome of the **MIPSs** project, the evaluator is able to identify any kind of IP: from 8-bit software implementations to highly parallelized hardware ones (e.g. 128-bit bus).