TRACEA

Unclonable Tags for Low-cost Anti-counterfeiting

Counterfeiting accounts for 7 % of worldwide trade. It becomes particularly crucial when the production is outsourced. The subcontracted producers may realize profits by producing extra quantities outside their license agreement and selling them on the black market.

TRACEA offers a very low-cost solution to prevent both counterfeiting and overproduction

UCL Université catholique de Louvain

RÉGION WALLONNE

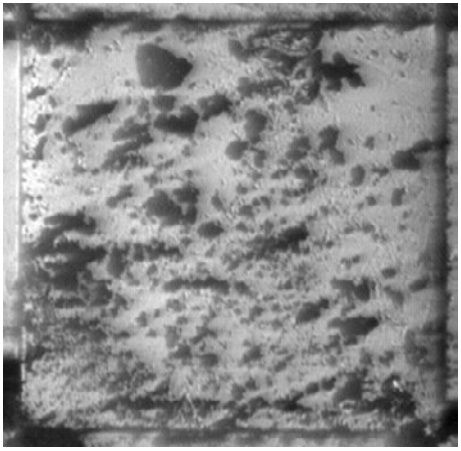
Based on the use of the random unclonable structure of crystallized polymer, TRACEA securely binds the random crystal Physically Unclonable Functions to the product by means of an electronic signature.

PUFs

Physically unclonable functions

Physical objects often bear unpredictable, uncontrollable inherent characteristics making them unique, such as the exact position of paper fibers. These can be seen as a "fingerprint" of the object. In the 90's, researchers suggested to use such objects, named Physically Unclonable Functions (PUFs) as a security component.

TRACEA uses a new type of PUF, based on a random crystal structure formed in a substrate cavity after a process of evaporation and crystallization of a polymer solution in its solvent. The production process is very cheap, and can be implemented wide-scale using industrial equipment



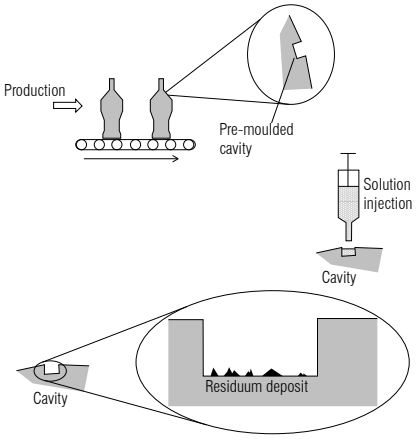
Crystal PUF

Security vs. robustness

One key step of our process is the extraction of an identifier from the PUF. This identifier must sufficiently capture the random characteristics of the PUF, while allowing a stable response among consecutive executions. In other words, it must be both:

- Secure: different PUFs always yield different identifiers
- Robust: multiple querying of the same PUF always yield the same identifier.

These two criteria are opposing, and finding the appropriate security vs. robustness tradeoff is one of the most crucial steps in the design of a PUF-based system.



How does it work?

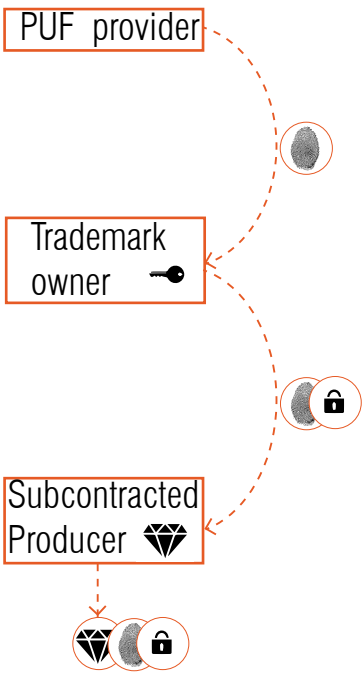
At a glance, our anti-counterfeiting solution works as follows

Producing authentic products

- A specialized PUF provider produces unique security tags
- The trademark owner acquires Crystal PUFs from the PUF provider.
- The trademark owner uses a cryptographic signature to sign the unique identifier extracted of the PUF, together with information on the product, and generates the certificate of authenticity (COA).
- The producer receives the PUF and the certificate of authenticity and attaches them to the product.

Verifying authenticity

- The identifier of the crystal tag is again extracted.
- The information of the product is retrieved.
- The electronic signature is verified. If it matches, the verifier knows for sure that the product is genuine.



The TRACEA solution is very low-cost compared with other anti-counterfeiting systems, e.g. based on Laser-Written PUF (TOMO3D Project) .

Security at a glance

To forge a product , the counterfeiter needs either:

- To produce a new Crystal PUF and generate its COA. Due to the strong security of electronic signature, this is virtually impossible.
- To produce a Crystal PUF yielding the same identifier as one already signed PUF, in order to reuse its COA for a forged product. This is also hardly possible due to unclonability of Crystal PUFs, as was validated by our analysis tool.

What we developed

Thanks to Walloon Region funding, in collaboration with Université de Mons, Wow technology and Serviplast, we developed:

- A prototype to produce and evaluate crystal PUFs at the cost of a few euro cents per tag.
- A prototype to securely extract identifier from crystal PUFs.
- A complete security analysis of the anti-counterfeiting solution.
- A full software prototype to evaluate the security and robustness of the anti-counterfeiting solution.

References:

Saloomeh Shariati, François Koeune, and François-Xavier Standaert. Security Analysis of Image-Based PUFs for Anti-counterfeiting, Volume 7394 of Lecture Notes in Computer Science (LNCS), pages 26-38, Springer, September 2012

Saloomeh Shariati, François-Xavier Standaert, Laurent Jacques, and Benoit Macq. Analysis and experimental evaluation of image-based PUFs, In Journal of Cryptographic Engineering, Volume 2, September 2012

Saloomeh Shariati, Laurent Jacques, François-Xavier Standaert, Benoit Macq, Mohamad Amine Salhi, and Philippe Antoine. Randomly Driven Fuzzy Key Extraction of Uncloneable Images, In The International Conference on Image Processing (ICIP), September 2010

Partnership

We are looking for partners to undertake the production and exploitation of this new technology

UCL Crypto Group

Place du Levant, 3 – 1348 Louvain-la-Neuve
(+32)10 47 8141 – uclcryptogroup@listes.uclouvain.be