PUF-Based Identification Tags and Blockchain for Supply Chain Management

Carmelo Felicetti[1], Antonella Guzzo[1], Antonino Rullo[1], Domenico Saccà[1,2], and Francesco Pasqua[2]

[1] DIMES Dept, Università della Calabria, 87036 Rende, Italy
{firstname.lastname}@unical.it
[2] OKT srl, 87036 Rende, Italy
{domenico.sacca, francesco.pasqua}@relatech.com

Abstract. Device authentication is an important issue in the Internet of Things as smart objects may need to safely demonstrate their identity prior the exchange of sensitive data with other entities. The usage of Physically Unclonable Functions (PUF) as device "digital fingerprint" has attracted great interest. Recently, an identification tag (ID tag) architecture has been proposed, which is based on a novel, highly stable PUF model for the secure storage and generation of cryptographic data for authentication purposes. This paper describes how this ID tag can be coupled with a product item in a supply chain scenario to confer a stable and durable identity for authentication, in order to identify the items, track them and perform anti-counterfeiting controls in a distributed ledger framework.

EXTENDED ABSTRACT

The Internet of Things (IoT) is changing the interactions of people with things in everyday life, since it enables the connection of ubiquitous objects to the Internet, while providing innovative services in emerging scenarios of business and industrial distributed applications. An emerging application scenario arises in the modern supply chains, where a product item (*physical object*) needs to be traced along every step among the involved companies, thus requiring identification by reader devices for collecting their data and storing them into a distributed ledger. In this scenario, the product item is required to be recognizable and distinguishable in order to be traced individually. Authentication mechanisms, therefore, play a crucial role. However, as physical objects such as product items do not have authentication capabilities, an important research issue is to provide an identity to them together with a mechanism to prove it. For these purposes, they can be equipped with an Identification Tag (ID Tag), that is an integrated circuit (IC) which presents some unique features (i.e., a "digital fingerprint"), implements an authentication protocol, and incorporates an Input/Output (I/O) interface for exchanging data. ID Tags can be a viable solution to the problem of conferring an identity to product items that must be traced: they can be temporarily coupled to them and interact with a tag reader by means of the NFC or RFID technology.

The use of a Physically Unclonable Function (PUF) as device digital fingerprint for authentication has attracted great interest due to its cryptography-oriented features such as randomness, uniqueness, unclonability, unpredictability, easiness of evaluation, and for its ability to take part in cryptographic operations with the generation of cryptographic keys and random numbers. A PUF leverages on random process variations as entropy source for secure key generations, which represents a low-cost and more secure alternative with respect to the conventional non-volatile memory-based solutions for key storage.

Some of the authors have proposed a PUF-based, memory-less, integrated circuit for identification tags which implements an Elliptic Curve Cryptography (ECC)-based, one-way authentication protocol, and offers numerous advantages over other state-of-the-art solutions. Major improvements are due to the novel, highly stable PUF model which covers very small chip area, allows for the adoption of a lightweight fault tolerance mechanism which does not need to be programmed with recovery data and, combined with appropriate circuit design choices, can be used to produce unpredictable and uncorrelated true random numbers. The authentication protocol is meant to work without the use of any memory or shared secret, and features message authentication services, thus allowing proof-of-identity authentication of tagged objects. As the authentication is one-way, signature verification is supported at the verifier side only.

In this presentation we show how the identification tag can be coupled with physical objects (product items) with the aim of conferring them a digital fingerprint within a blockchain-based supply chain scenario for traceability and anti-counterfeiting of products. In particular we illustrate how the identification tag presented in can be employed to confer identity to a product item to be tracked along its supply chain. The tag acts as a possession factor that only the object must have, or have access to, in order to perform authentication. Ongoing research work is being devoted to define effective proofs of possessions to mitigate the risk of the tag being stolen and used by an object other than the one used in the enrolment phase. An inherence factor may be used by applying the concept of biometrics for physical object identification (*physimetric identification*) by means of advanced machine learning techniques.